Council of the European Union

Brussels, 31 May 2021
(OR. en, fr)

Interinstitutional File: 2020/0349(COD)

5527/8/21
REV 8

LIMITE

SIRIS 11
ENFOPOL 27
COPEN 30
SCHENGEN 7
IXIM 27
CODEC 86
IA 11

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	13908/20 + COR 1
No. Cion doc.:	COM(2020) 796 final
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation - Written comments

Delegations will find attached a revised compilation of the Member States' comments regarding the Commission proposal for a Regulation amending Regulation (EU) 2016/794 (Europol Regulation), containing the initial comments received after the LEWP meeting of 11 January 2021 (Annex part 1), the follow-up comments received after the meeting of 25 January 2021 (Annex part 2), additional comments received after the meeting of 8 February 2021 (Annex part 3), comments regarding block 4 received after the meeting of 22 February 2021 (Annex part 4), the follow-up comments and comments regarding block 2 after the meeting on 8 March 2021 (Annex part 5), follow-up comments and comments regarding block 6 after the meeting on 12 April 2021 (Annex part 6), the follow-up comments and comments regarding block 8 after the meeting on 26 April 2021 (Annex part 7) and the latest follow-up comments after meetings on 7 May 2021 (Annex part 8) and 18 May (Annex part 9).

ANNEX

Table of contents

1. GENERAL COMMENTS

AUSTRIA

Austria may present some remarks concerning the Articles 26, 26a and 33a of the draft:

Art. 26 and 26a:

We always supported the enhancement of information exchange between Europol and private parties and we acknowledge that Europol will have the possibility to process data obtained from private parties on the substance, we also welcome that the "resubmission problem" is solved with the new Article 26. We regret that Europol will not be allowed to request personal data directly from private parties. If a procedure of consent from the Member States would be foreseen in the regulation this should be feasible.

We propose to mention Article 26 in Article 18 Purpose of information processing activities.

Art. 33a:

Generally we support this article, regulating the data processing for innovation and research purpose, but we would like to ask you about the deletion of the "old" Article 33 in the Europol Regulation? Will there be a new Article 33? We are of the opinion, that this article, containing regulations concerning developments of technical tools and procedures for lawful data processing still remains very useful.

Two additional remarks:

Austria would strongly prefer if Europol attends the (virtual) meetings.

Europol can support delegations with its know how directly in the discussions if needed.

BELGIUM

Written comments by Belgium

concerning the proposed revision of the Europol Regulation (EU) 2016/794

We welcome the negotiations on the proposed revision of the Europol Regulation (EU) 2016/794, based on the European Commission's document COM(2020)796 as presented in Council document 13908/20. As requested by the Portuguese Presidency we have some general preliminary comments to share as well as some questions, which indicate certain desired clarifications or concerns. Most of these however will require consultations with the European Commission and/or Europol. We thank you for your consideration.

In general, we consider the proposed changes to the Europol Regulation to reflect very well the current concerns and necessities in relation to Europol's support to the MS. For example, we are pleased to note a delicate balance that has been sought in relation to the cooperation with private parties, the processing of large data sets and the request to the MS to initiate investigations. We also welcome the codification of several important existing and emerging tasks, such as concerning EMPACT or in relation to research and innovation.

We would like to focus on the articles to be discussed during the meeting of 25 January 2021. Our preliminary concerns regarding the first building block are the following:

- As for the determining the **private parties** in question we note that there is no definition or limitation to them, we welcome exchanging of views on this extremely important matter. We would like clarifications by the Commission and/or Europol on the intended cooperation with financial institutions. We believe the topic of Europol's cooperation with FIUs is closely linked to the debate on Europol's cooperation with private parties. It is necessary to receive further information about *how* this current proposal will coexist with and not duplicate the way in which FIUs function amongst themselves and cooperate with reporting entities. In this regard we are also very interested to hear about FR's idea during the meeting of 17 December 2020 about including the content of recital 33 in relation to Europol's cooperation with financial intelligence units into article 7. We note that the Commission is not eager to describe in an article what Europol cannot do, but we do find it essential to not interfere with FIU functioning through the rules on Europol's cooperation with private parties. As an alternative it thus seems logical as well as necessary to exclude obliged entities from the private parties Europol can cooperate with directly. Moreover, when it concerns information from financial institutions that is not subjected to FIU reporting (namely non-suspicious activity), how will Europol process such information based on the current proposal? The proposed articles concerning processing information outside Annex II does not seem to allow for this.
- Next to this, regarding the possibility of Europol to request a MS to contact a private party (namely article 26(6a)), we would like to enquire whether this process is also subjected to same reasoning of §2 of article 26 that the concerned MS has/have to resubmit the

information to Europol via their national units. The text of paragraph 6a namely doesn't seem to suggest such a reasoning.
- We would welcome a clarification on the reason for deleting the phrasing concerning "the circumstances allow(ing) a clear presumption of consent" in article 26(5).
- Furthermore, we would welcome clarifications concerning the use of the terminology and the differences between "transmission" and "transfer" throughout the text, namely in article 26(5), taking into account the terminology used in Regulation (EU) 2018/1725.
- We would welcome clarifications on the added value and the intended impact of the proposed changes concerning **terrorist content online**. How does article 4(1)(m) relate to article 4(1)(u)?

Moreover, we already want to highlight certain other aspects concerning the other topics:

- As regards article 18a, namely the possibility of Europol to **process large data files** related to an "investigative case file" we wonder how this phrasing relates to proactive investigations. The definition does not seem to clarify this aspect, which we however consider to be important. Throughout the text we also note other phrasings, such as "specific criminal investigation" (in article 51(3)(g)) and "individual investigation or specific project" (in article 21(8)). We wonder about the meaning of these types of phrasing and how they are linked to the concept of the "investigative case file".
- We note in recital 21 on **giving evidence in proceedings** the condition of taking into account "applicable use restrictions", which we of course welcome. In article 20(5) however we do not see any reference to such restrictions and we wonder whether a reference to for example article 19(2) could be considered.
- We do not consider beneficial to refer in recital 7 concerning **EMPACT** to the certain terminology which is more suited to be flexible and based on Council conclusions. We thus suggest to amend the last sentence as follows: *"Europol should be able to provide administrative, logistical, financial and operational support to such activities, supporting the identification of **cross-cutting** priorities and the implementation of **horizontal** strategic goals in countering serious crime."*

In conclusion, we look forward to fruitful discussions within the LEWP in order to strengthen the Europol mandate where appropriate. As requested by the Portuguese Presidency, we will express our position on the proposed information alert by Europol in the Schengen Information System within the IXIM community before addressing this topic again in the LEWP.

CROATIA

PROPOSAL AMENDMENTS TO THE EUROPOL REGULATION:

1. Enabling Europol to cooperate effectively with private parties
2. Enabling Europol to process large and complex datasets
3. Strengthening Europol's role on research and innovation
4. Enabling Europol to enter data (alarms) in the SIS
5. Strengthening Europol's cooperation with third countries
6. Strengthening Europol's cooperation with the European Public Prosecutor's Office (EPPO)
7. Clarifying Europol's role in initiating investigations
8. Strengthening the data protection framework applicable to Europol

BLOCK 1

Currently, Europol is not allowed to exchange data directly with private parties (this primarily relates to banks, telecommunication operators and ISPs), which results in the lack of exchanges or leads to slow-paced exchanges. This is above all important when obtaining data relating to criminal investigations concerning several Member States. We are therefore of the opinion that amendments should allow for direct exchange.

BLOCK 2

In August 2020, EDPS issued a warning to Europol regarding the processing and analysis of large sets of computer data. The EDPS considers that Europol may not process and analyze all data on criminal offences submitted to Europol by Member States (obtained through court orders), because such data could include data from entities that have no connections to a criminal offense. Europol was given 6 months to align its systems and policies with the EDPS's recommendations. The discussions at LAWP showed that the EC and the Member States consider that the EDPS's opinion and recommendation are illogical and display a misunderstanding of Europol's legal framework, the origin and structure of the data as well as the purposes of data analysis. In this context, the HR representatives underlined that attempts should be made during the remainder time until the EDPS's deadline expires to clarify to the EDPS all the details of the process on which EDPS had given their opinion, since suspending the analysis of large sets of computer data done by the Europol would bring extremely adverse effects for the Member States. At the same time, while we deem Europol's legal framework in this area to be at satisfactory level, we are in favor of its amendments in order to define more clearly the data handling, the implementation of data protection and limits for data storage.

In short, we support the proposed change to the rules (restrictions) of data processing, because, in processing large sets of (computer) data, Europol is not in a position to distinguish immediately whether individual data relate to entities connected to a criminal offence (the only data that may be processed). We also support extending the storage limits of such large datasets to make them available in subsequent judicial proceedings.

BLOCK 3

Proposal is to strengthen the Europol's role in a way that Europol could assist the EC and the Member States in identifying, developing and using new technologies under its mandate. We support these changes.

BLOCK 4

Proposal is to allow Europol to enter data (alarms) in the SIS. These alarms would be based on information received from third countries that do not have signed agreements on cooperation with Europol and would target potential terrorists and sex offenders. We consider it essential, from an operational standpoint, to make relevant data held by third States available to Member States. An alternative to this proposal could be to instruct Member States to use, thoroughly, Interpol databases into which those third countries enter the same data. If the proposal is accepted, it will be imperative to establish a verification system to check how reliable the third country data are and to verify the ownership of such data in terms of possibility of its further use. We are not against, but also not thrilled about this proposal. If an initiative is accepted, we will closely monitor its implementation.

BLOCK 5

With the adoption of the current Europol Regulation, the power to conclude operational agreements on cooperation with third countries was transferred from Europol to the European Commission. Although such move was reasonable, in reality it turned out that the European Commission has not been able conclude a single Europol cooperation agreement with third countries for more than three years. Needs for such agreements exist, and we therefore consider it necessary to modify the rules on the conclusion of operational agreements with third countries within the amendments to the Europol Regulation. In practice, this would suggest reinstating part of the power to conclude an agreement to the Europol Management Board, in which the European Commission would also have the right to vote on this matter. It remains to be seen how this issue will be resolved, but we are supportive of the initiative.

BLOCK 6

We consider it necessary to regulate Europol's cooperation with the EPPO within the Regulation and the Working Arrangement. As regards Europol's obligation to report likely criminal offences to the EPPO, we want to avoid possible overlaps with Member States' obligations, and we are therefore in favor of clear and precise outlines of this obligation through amendments to the Regulation.

BLOCK 7

Currently, Europol may request Member States to initiate an investigation only if there is a cross-border element of the criminal offence. Proposal is to remove this restriction on offences that are detrimental to the interests of the EU. We support this proposal.

BLOCK 8

Proposed are specific changes to the rules on the protection of personal data, the most important being the alignment with the 'police' Directive. We support this proposal.

CZECH REPUBLIC

CZ comments on Revision of Europol Regulation

Please find interim Czech comments on document 13908/20. Further comments may be raised following ongoing scrutiny of the text:

Article 4 (1) (h) – (q), (s) - (u)

These points are superfluous and inconsequential. There is no need to stipulate particular examples of how the Europol supports Member State law enforcement. For example, it is not necessary to legislate that Europol supports cross-border cooperation of special intervention units; on the contrary, it puts in doubt any other support that is not explicitly included. In other cases, there are concrete rules on Europol action in separate instruments, such as TCO draft Regulation. Therefore, these points should be deleted.

Article 4 (4a)

This point diverges too far from the core tasks of Europol in that it mandates Europol to draw up and implement research and innovation programmes.

Article 6

CZ is strictly against such enhanced requests, which go beyond the mandate of Europol and are unnecessary.

Article 18

The stipulation of the extended period of provisional processing of data in paras 5a appears to exclude, in practice, processing of data that typically falls outside the categories in Annex II, such as data from suspicions transactions (cooperation between FIUs). CZ believes it would be better to simply provide for exception from Annex II at least in systematically important cases, similarly to Art. 18a(1).

Article 20a

The application of Art. 21(6), or Art. 19(2)(3), should be unambiguously stipulated to all types of cooperation with EPPO.

Article 25

While CZ supports appropriate strengthening of Europol's ability to transfer personal data to third countries, neither this amendment nor recital 23 provide sufficient explanation of how the approval of category of transfers differs from approval of transfers and when such an approval can be used on case-by-case basis in a specific situation.

Article 26

Council Conclusions 14745/19 should form a basis of this proposal. In certain instances the consent or similar involvement of relevant Member State should be required (e.g. in para 5(a) or (d)). It should be clearly stipulated that cooperation of private parties is voluntary.

Obviously, the para 6a goes too far. The purpose of the Europol is to support the Member States, not the other way around.

Article 26a

This provision should be limited to Europol's obligations under draft TCO Regulation. For example, para 5 goes too far and interferes with the responsibilities of Member States.

(end of file)

FRANCE

NOTE DE COMMENTAIRES DES AUTORITÉS FRANÇAISES

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leurs commentaires écrits suite à la réunion de groupe LEWP du 17 décembre 2020, en particulier sur les aspects liés à l'échange de vues sur la révision du règlement d'Europol.

1. Rappel des éléments portés par la délégation française lors de la réunion du LEWP du 17 décembre 2020.

Remarque générale sur la proposition de révision du règlement de l'agence Europol :

Les autorités françaises souhaitent faire part de leur accueil favorable à ce projet de la Commission qui propose de nombreuses solutions juridiques permettant de répondre aux besoins de l'agence dans son rôle de soutien aux services répressifs des États membres. En effet, l'agence Europol doit être pleinement intégrée dans une architecture de sécurité intérieure européenne solide et contribuer directement au développement d'une meilleure autonomie stratégique de l'Union en matière de sécurité intérieure. Cette proposition pose des bases très encourageantes.

S'agissant de la gestion des données :

Les autorités françaises accueillent favorablement les dispositions permettant à Europol de traiter des données obtenues auprès de parties privées, des données de masse ou des données obtenues dans le cadre d'enquêtes de grande ampleur répondant à des enjeux opérationnels centraux. Elles garantissent la pérennité du modèle de fonctionnement de l'agence dans le cadre des obligations posées par le CEPD, vis-à-vis du règlement 2016/794. Plus particulièrement, les autorités françaises saluent la proposition de la Commission qui prend en compte les risques pesants sur l'articulation efficace avec les cadres nationaux LBC/FT – et par voie de conséquence sur les dispositifs relatifs aux cellules de renseignement financier - en cas d'ouverture sans réserve des échanges entre Europol et les parties privées, par l'insertion d'un considérant spécifique sur ce point (considérant 33) mais qui pourrait être renforcé par une mention dans un article.

Enfin, les autorités françaises font part de leur étonnement sur le fait que le régime d'Europol en matière d'échanges de données avec des États tiers tel que proposé ne soit pas aligné sur celui d'autres agences JAI en utilisant toutes les potentialités prévues par le règlement 2018/1725 (articles 47 et 48 notamment).

Sur le rôle d'Europol en matière d'innovation :

Les autorités françaises marquent leur soutien au rôle octroyé à Europol en matière d'innovation. Le positionnement de l'agence s'en trouve renforcé ce qui permettra de soutenir et d'apporter un appui utile aux services répressifs. À cet égard, et pour placer l'agence dans une perspective plus globale, outre le laboratoire d'innovation, le Hub d'innovation JAI aurait mérité d'être mentionné.

Sur la relation avec le parquet européen :

La relation avec le parquet européen était fortement attendue et correspond au rôle que les États membres ont entendu confier à Europol dans ces **champs de compétence déterminants** pour

l'avenir des forces de sécurité intérieure de l'Union. Une attention particulière demeurera néanmoins sur la rédaction de l'alinéa 4 de l'article 20(a) portant sur les signalements à EPPO de faits susceptibles de relever de sa compétence.

S'agissant de l'inscription de signalements dans le SIS par l'agence :

Les autorités françaises notent la persistance de la proposition de la Commission s'agissant de la possibilité d'octroyer un **rôle à l'agence dans l'incrémentation du SIS en créant une catégorie pour information**. Elles réaffirment leur **opposition** sur ce point et font remarquer **qu'une telle proposition ne répond pas aux difficultés opérationnelles soulevées** lors des précédentes réunions du LEWP mais aussi dans le cadre des débats en TWP sur le protocole d'insertion des CTE dans le SIS et que le coût particulièrement élevé que représente sa mise en œuvre sans réelle plus-value opérationnelle ne plaide pas en sa faveur.

S'agissant de la gouvernance d'Europol :

L'extension des prérogatives d'Europol ne s'accompagne pas d'un renforcement de sa gouvernance au profit des États membres dans le conseil d'administration, qui doit notamment **être impliqué dans les décisions de transfert de données.**

Concernant les aspects financiers :

Les autorités françaises font part de leur **étonnement concernant l'ajout d'une disposition (article 57) permettant aux États membres ou États tiers (ayant signé un accord avec l'UE ou l'agence) de contribuer directement au budget d'Europol.** Cette nouvelle disposition n'a jamais été évoquée auparavant et introduit un mécanisme qui est susceptible de perturber considérablement l'équilibre sur lequel Europol est construite. Les autorités françaises souhaitent donc obtenir des précisions sur ce sujet et notamment sur l'existence de mécanismes similaires dans d'autres agences et sur les fora au cours desquelles cette proposition a été évoquée précédemment.

Concernant l'articulation des compétences de l'Agence avec les compétences des États membres ou d'autres entités européennes :

De nouvelles compétences d'Europol apparaissent telle que la production de l'analyse de la menace, alors que cette tâche est dévolue à l'IntCen. Les autorités françaises sollicitent des précisions sur la plus-value attendue d'Europol sur ce volet.

2. Analyse détaillée de la proposition de la commission (considérants et articles)

De manière plus détaillée, les autorités françaises souhaitent faire part de leurs avis et commentaires concernant les considérants et les articles de la proposition de révision du règlement de l'agence dans le tableau ci-dessous :

Commentaires des autorités françaises sur la proposition de refonte du règlement Europol de la Commission européenne

*I) **CONSIDERANTS***

Proposition de la Commission européenne	*Commentaires des autorités françaises*
Considérant 4: **As Europe faces increasing threats from organised crime groups and terrorist attacks, an effective law enforcement response must include the availability of well-trained interoperable special intervention units specialised in the control of crisis situations. In the Union, the law enforcement units of the Member State cooperate on the basis of Council Decision 2008/617.53 Europol should be able to provide support to these special intervention units, including by providing operational, technical and financial support**	Tout d'abord, les autorités françaises soulignent qu'il convient de définir les termes " **situations de crise**" qui ne recoupent pas les mêmes acceptions d'un Etat membre à un autre. Elles rappellent également qu'il convient d'être prudent sur le soutien que pourrait apporter Europol aux unités spécialisées d'intervention. Les récentes difficultés rencontrées avec le réseau ATLAS doivent impérativement être surmontées avant tout approfondissement du soutien de l'agence à ce type d'unité.
Considérant 6 : High-risk criminals play a leading role in criminal networks and pose a high risk of serious crime to the Union's internal security. To combat high-risk organised crime groups and their leading members, Europol should be able to support Member States in focusing their investigative response on identifying these persons, their criminal activities and the members of their criminal networks.	Le terme de *« high risks criminals »* est à rapprocher du concept de HVT utilisé par Europol. S'agissant d'un article qui doit fixer les missions et objectifs généraux de l'agence, on peut s'interroger sur la pertinence d'intégrer ce niveau de détail qui relève d'un processus de priorisation des dossiers. Cette précision n'a vocation ni à apporter des clarifications légales ni à codifier des tâches existantes. S'agissant de l'utilisation de la notion de risque, le SOP relatif à la sélection des High Value Target renvoie à des prérequis qui relèvent davantage d'une menace concrète que du risque : *"The prerequisite for the initiation of the identification and selection process of the High Value Target is that Europol's criteria for the prioritization of the cases are met and the potential target is:* *- Suspected of planning or preparing of one or more of the offenses defined in Article 3 of the Europol Regulation during the past year; or* *- Suspected to have committed one or more of the offences defined in Article 3 of the Europol Regulation during the past year. "*

	Les critères d'objectivation du niveau de la cible sont également révélateurs de la réalité d'une menace alors que la notion de risque sous-tend une notion de probabilité. **Les autorités françaises proposent donc de supprimer cette référence aux « *high-risks criminals* ».** Toutefois, si la référence à ce niveau de détail devait être maintenue, il serait souhaitable de faire référence à la menace criminelle plutôt qu'au risque et ce en cohérence avec le termes utilisé habituellement « *Threat assessment* » pour l'acronyme SOCTA. **Soit la proposition de rédaction suivante :** *To combat organised crime groups and their leading members, Europol should be able to support Member States in focusing their investigative response on identifying these persons, their criminal activities and the members of their criminal networks.*
Considérant 8: **The Schengen Information System (SIS), established in the field of police cooperation and judicial cooperation in criminal matters by Regulation (EU) 2018/1862 of the European Parliament and of the Council5556, is an essential tool for maintaining a high level of security within the area of freedom, security and justice. Europol, as a hub for information exchange in the Union, receives and holds valuable information from third countries and international organisations on persons suspected to be involved in crimes falling within the scope of Europol's mandate. Following consultation with the Member States, Europol should be able to enter data on these persons in the SIS in order to make it available directly and in real-time to SIS end-users**	Les autorités françaises sont défavorables à ce considérant conformément aux positions déjà exprimées sur cette problématique. Elles tiennent à rappeler qu'Europol doit contribuer à faire en sorte que les États membres inscrivent **eux-mêmes** toutes les données des États tiers dans le SIS. Par ailleurs, un protocole concernant l'inscription des combattants terroristes étrangers dans le SIS a été négocié en TWP.

Considérant 9: **Europol has an important role to play in support of the evaluation and monitoring mechanism to verify the application of the Schengen acquis as established by Council Regulation (EU) No 1053/2013. Given the need to reinforce the Union's internal security, Europol should contribute with its expertise, analysis, reports and other relevant information to the entire evaluation and monitoring process, from programming to on-site visits and the follow-up. Europol should also assist in developing and updating the evaluation and monitoring tools.**	Les autorités françaises s'interrogent sur la plus-value d'une référence à ce règlement ainsi que sur le rôle qu'Europol pourrait prendre dans ce **dispositif déjà prévu dans le règlement 1053/2013**. Le cadre actuel impliquant une évaluation entre « pairs » apparaît satisfaisant et les autorités françaises rappellent que la référence à ce règlement n'a pas été inscrite par le législateur en 2016 lors de l'élaboration du règlement actuel. De même, il convient de s'interroger sur la façon dont ce considérant s'articule avec les objectifs fixés par l'analyse d'impact initiale sur le renforcement du mandat d'Europol.
Considérant 10 : Risk assessments are an essential element of foresight to anticipate new trends and to address new threats in serious crime and terrorism. To support the Commission and the Member States in carrying out effective risk assessments, Europol should provide threats assessment analysis based on the information it holds on criminal phenomena and trends, without prejudice to the EU law provisions on customs risk management.	La proposition de reformulation vise à bien prendre en compte l'évolution de la menace qui vient compléter l'évolution des risques. **Soit la proposition de rédaction suivante** : ***Criminal threat*** *and risk assessments are an essential element of foresight to anticipate new trends and to address new threats in serious crime and terrorism. To support the Commission and the Member States in carrying out effective* ***criminal threat and*** *risk assessments, Europol should provide analysis based on the information it holds on criminal phenomena and trends.*
Considérant 11: **In order to help EU funding for security research to develop its full potential and address the needs of law enforcement, Europol should assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation that are relevant to Europol's objectives.** **When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, it should not receive funding**	Les autorités françaises rappellent que l'agence Europol n'est pas la seule agence de l'UE intervenant dans le domaine de la sécurité intérieure. À ce titre, elles estiment qu'une telle mission pourrait être dévolue au **pôle d'innovation (Hub)** actuellement en cours de création. Cette structure distincte d'Europol – qui n'en assure que le soutien et le secrétariat – apparait comme plus pertinente pour éviter les redondances et mutualiser les efforts. La rédaction de ce considérant devrait donc être adaptée en mettant en avant l'approche globale de mise en relation des agences et réseaux

from that programme in accordance with the conflict of interest principle.	souhaitée par la création du pôle d'innovation. Soit la proposition de rédaction suivante : ***Europol in association with relevant security agencies should assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation that are relevant to Europol's objectives***
<u>Considérant 12:</u> **It is possible for the Union and the Members States to adopt restrictive measures relating to foreign direct investment on the grounds of security or public order. To that end, Regulation (EU) 2019/452 of the European Parliament and of the Council establishes a framework for the screening of foreign direct investments into the Union that provides Member States and the Commission with the means to address risks to security or public order in a comprehensive manner. As part of the assessment of expected implications for security or public order, Europol should support the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes**	Tout d'abord, les autorités françaises rappellent que le règlement 2019/452 cité ne fait pas référence à l'agence Europol ce qui pourrait créer une situation d'insécurité juridique quant à la mise en pratique d'une telle mission. Ensuite, le considérant introduit la notion « **d'ordre public** » pour laquelle l'agence Europol n'est pas compétente. Enfin, un conflit d'intérêt pourrait émerger quand il s'agira pour l'agence d'étudier des investissements directs étrangers qui concernent le développement/l'utilisation de technologies par Europol comme peut le démontrer le développement du Poste de commandement virtuel (VCP) d'Europol. Pour rappel le VCP est une technologie développée par une entreprise dont l'établissement légal se situe hors de l'Union européenne. Les autorités françaises s'interrogent enfin sur la façon dont ce considérant s'articule avec les objectifs fixés par l'analyse d'impact initiale sur le renforcement du mandat d'Europol.

Considérant 13 : **Europol provides specialised expertise for countering serious crime and terrorism. Upon request by a Member State, Europol staff should be able to provide operational support to that Member State's law enforcement authorities on the ground in operations and investigations, in particular by facilitating cross-border information exchange and providing forensic and technical support in operations and investigations, including in the context of joint investigation teams. Upon request by a Member State, Europol staff should be entitled to be present when investigative measures are taken in that Member State and assist in the taking of these investigative measures. Europol staff should not have the power to execute investigative measures.**	Les autorités françaises demeurent attentives à la proposition de la Commission permettant au personnel d'Europol **d'assister les autorités compétentes dans la mise en place de « mesures d'enquête »**. Si ce point n'apparaît pas bloquant en l'état, il importe que la Commission détaille davantage cette disposition et fournisse des cas concrets d'application.
<u>Considérant 14:</u> One of Europol's objectives is to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combatting forms of crime which affect a common interest covered by a Union policy. To strengthen that support, Europol should be able to request the competent authorities of a Member State to initiate, conduct or coordinate a criminal investigation of a crime, which affects a common interest covered by a Union policy, even where the crime concerned is not of a cross-border nature. Europol should inform Eurojust of such requests.	Dans la continuité de la note de commentaire des autorités françaises du 30 octobre 2020, **les autorités françaises sont défavorables à la révision de l'article 6 du règlement Europol actuel**. En effet, cette disposition n'est quasiment pas mise en œuvre et les enquêteurs, en lien avec leurs autorités judiciaires, doivent disposer de la maîtrise de l'ouverture de leurs enquêtes. Les autorités françaises rappellent tout de même que, interrogées sur le sujet, ni la Commission, ni Europol n'ont pu fournir de statistiques concernant le recours à l'article 6 du règlement Europol actuel. Toutefois, les autorités françaises constatent que la nouvelle rédaction de l'article 6 tient compte de certaines réserves exposées et ne prévoit pas de pouvoir d'enquête d'initiative pour l'agence. Elles relèvent enfin que la préservation de l'efficacité des choix des stratégies d'entrave milite en faveur de la maitrise du dialogue entre services enquêteurs et autorités judiciaires.

<u>Considérant 15:</u> **Publishing the identity and certain personal data of suspects or convicted individuals, who are wanted based on a Member State's judicial decision, increases the chances of locating and arresting such individuals. To support Member States in this task, Europol should be able to publish on its website information on Europe's most wanted fugitives for criminal offences in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals.**	Les autorités françaises proposent que ce considérant soit modifié comme suit : "***<u>Upon request from Member States, Europol may provide its support in informing the public about suspects or convicted individuals who are wanted based on a national judicial decision relating to a criminal offence in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals".</u>***
Considérant 18: **To ensure that any data processing is necessary and proportionate, Member States should ensure compliance with national and Union law when they submit an investigative case file to Europol. Europol should verify whether, in order to support a specific criminal investigation, it is necessary and proportionate to process personal data that may not fall into the categories of data subjects whose data may generally be processed under Annex II of Regulation (EU) 2016/794. Europol should document that assessment. Europol should store such data with functional separation from other data and should only process it where necessary for its support to the specific criminal investigation, such as in case of a new lead.**	Les autorités françaises soulignent qu'une telle demande risque de réduire le nombre de contributions nationales à Europol si les outils mis à disposition par l'agence ne facilitent pas la catégorisation des données attendues dans ce considérant. La responsabilité devrait être ainsi partagée entre les États membres responsables des contributions et Europol, en charge de l'administration des outils utilisés par les enquêteurs pour soumette lesdites contributions. Ce considérant pourrait en conséquence être retravaillé en vue de rappeler la responsabilité d'Europol de proposer des outils adaptés aux contraintes pesant sur les États membres. Dès lors, il appartient à Europol de faire évoluer les outils de communication mis à disposition des EM en conséquence. La prise en compte de ces contraintes ne doit pas peser sur les EM. Proposition d'amendement en ce sens : ***To ensure that any data processing is necessary and proportionate, Member States should ensure compliance with national and Union law, provided that Europol delivers adequate tools to Member states when they submit an investigative case file to Europol. Europol should verify whether, in order to support a specific criminal investigation, it is necessary and proportionate to process personal data that may not fall into the categories of data subjects whose data may generally be processed under Annex II of Regulation (EU) 2016/794.***

	Europol should document that assessment
Considérant 19: **To ensure that a Member State can use Europol's analytical reports as part of judicial proceedings following a criminal investigation, Europol should be able to store the related investigative case file upon request of that Member State for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.** **Europol should store such data separately and only for as long as the judicial proceedings related to that criminal investigation are on-going in the Member State.** **There is a need to ensure access of competent judicial authorities as well as the rights of defence, in particular the right of suspects or accused persons or their lawyers of access to the materials of the case.**	Les autorités françaises attirent l'attention sur ce considérant qui semble prévu pour couvrir juridiquement le rôle de soutien d'Europol pour les dossiers impliquant des interceptions de masse telles que celles permises par l'opération EMMA. Concernant le dernier alinéa de ce considérant, il doit être rappelé que la conservation des données ou l'accès au dossier dans ce cadre ne peuvent être autorisés que par l'autorité judiciaire mandante.
Considérant 22: **Europol and the European Public Prosecutor's Office ('EPPO') established by Council Regulation (EU) 2017/193958, should**	Les autorités françaises rappellent qu'au titre de l'article 102 du règlement Parquet européen, Europol fournit un soutien à cet organe pour **les enquêtes** et non pour les poursuites.

put necessary arrangements in place to optimise their operational cooperation, taking due account of their respective tasks and mandates. Europol should work closely with the EPPO and actively support the investigations and prosecutions of the EPPO upon its request, including by providing analytical support and exchanging relevant information, as well as cooperate with it, from the moment a suspected offence is reported to the EPPO until the moment it determines whether to prosecute or otherwise dispose of the case. Europol should, without undue delay, report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence. To enhance operational cooperation between Europol and the EPPO, Europol should enable the EPPO to have access, on the basis of a hit/no hit system, to data available at Europol, in accordance with the safeguards and data protection guarantees provided for in this Regulation. The rules on the transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO. Europol should also be able to support criminal investigations by the EPPO by way of analysis of large and complex datasets.	
<u>Considérant 24:</u> **Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation.**	Les autorités françaises doutent que la modification mineure du **régime dérogatoire** de l'article 25 du règlement Europol puisse résoudre le problème de fond lié à la rigidité du régime juridique applicable aux relations d'Europol avec les parties privées. Pour mémoire, la France soutient « l'option 2 » proposée par la Commission européenne : *ajouter la possibilité, en l'absence d'une coopération opérationnelle structurelle visée à l'option 1, de transférer des données à caractère personnel dans les cas où l'existence de garanties appropriées dans le pays tiers, en ce qui concerne la protection des données à caractère personnel, est prévue dans un instrument juridiquement contraignant (intervention législative).* Les autorités françaises proposent que le régime juridique des relations d'Europol avec les pays

	tiers soit assoupli tout en permettant un **contrôle strict des États membres** et l'assurance du **respect des codes de gestion** dans cet échange de données entre l'agence et les États tiers. **Ces échanges devront impérativement respecter les principes de la règle du tiers service.** Également, les autorités françaises s'interrogent sur la notion « **categories of transfers** » ajoutée par la Commission à l'article 25 paragraphe 5 et souhaiterait disposer d'éclaircissements. Au titre de la gouvernance des EM sur Europol, et au regard de la règle du tiers service/propriété de l'information, ces derniers doivent être impliqués dans le dispositif de validation visant au transfert de données. Proposition d'amendements : **Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries *within the agreement of the management board* while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects.**
Considérant 25: To support Member States in cooperating with private parties providing cross-border services where those private parties hold information relevant for preventing and combatting crime, Europol should be able to receive, and in specific circumstances, exchange personal data with private parties.	Les autorités françaises notent que le considérant 25 ne mentionne que le soutien d'Europol aux États membres pour coopérer avec les **parties privées prestataires de services transfrontaliers**. Les articles modifiés figurant dans la révision du Règlement vont cependant bien au-delà de cet objectif, soulevant un problème de cohérence entre les objectifs et la proposition. Aussi les autorités françaises s'interrogent sur la possibilité de mieux inscrire cet objectif dans les articles liés à l'échange d'information entre Europol et les parties privées (articles 26 et 26a).

Considérant 31: **Member States, third countries, international organisation, including the International Criminal Police Organisation (Interpol), or private parties may share multi-jurisdictional data sets or data sets that cannot be attributed to one or several specific jurisdictions with Europol, where those data sets contain links to personal data held by private parties. Where it is necessary to obtain additional information from such private parties to identify all relevant Member States concerned, Europol should be able to ask Member States, via their national units, to request private parties which are established or have a legal representative in their territory to share personal data with Europol in accordance with those Member States' applicable laws. In many cases, these Member States may not be able to establish a link to their jurisdiction other than the fact that the private party holding the relevant data is established under their jurisdiction. Irrespective of their jurisdiction with regard the specific criminal activity subject to the request, Member States should therefore ensure that their competent national authorities can obtain personal data from private parties for the purpose of supplying Europol with the information necessary for it to fulfil its objectives, in full compliance with procedural guarantees under their national laws.**	La notion d'autorité compétente telle que définie à l'article 2 du Règlement Europol et évoquée au considérant 31 (partie en rouge) de la présente proposition de révision entraine des interrogations sur les autorités effectivement concernées. Les autorités françaises aimeraient obtenir des clarifications sur la nature des autorités compétentes nationales qui devraient pouvoir obtenir des données personnelles des parties privées pour le compte d'Europol. En effet, les échanges d'information entre Europol et certaines autorités publiques font l'objet de dispositions distinctes, notamment concernant les cellules de renseignement financier, celles énoncées par la Directive 2019/1153 fixant les règles facilitant l'utilisation d'informations financières aux fins de la prévention ou de la détection de certaines infractions pénales (dont la transposition doit intervenir au plus tard le 1er aout 2021). Les autorités françaises marquent leur attachement à ce que ces cadres existants soient respectés.
Considérant 33: Any cooperation of Europol with private parties should neither duplicate nor interfere with the activities of the Financial Intelligence Units ('FIUs'), and should only concern information that is not already to be provided to FIUs in accordance with Directive 2015/849 of the European Parliament and of the Council59. Europol should continue to cooperate with FIUs in particular via the national units.	Les autorités françaises saluent la proposition de la Commission qui prend en compte les risques pesant sur l'articulation efficace avec les cadres nationaux LBC/FT – et par voie de conséquence sur les dispositifs relatifs aux cellules de renseignement financier - en cas d'ouverture sans réserve des échanges entre Europol et les parties privées, par l'insertion d'un considérant spécifique sur ce point (considérant 33) mais qui pourrait être renforcé par **une mention dans un article** (cf. proposition sur article 1 (4)).

Considérant 35: **Terrorist attacks trigger the large scale dissemination of terrorist content via online platforms depicting harm to life or physical integrity, or calling for imminent harm to life or physical integrity. To ensure that Member States can effectively prevent the dissemination of such content in the context of such crisis situations stemming from ongoing or recent real-world events, Europol should be able to exchange personal data with private parties, including hashes, IP addresses or URLs related to such content, necessary in order to support Member States in preventing the dissemination of such content, in particular where this content aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.**	Les autorités françaises soulignent la nécessité de clairement définir la notion de « **situation de crise** ». Le passage en situation de crise pourrait être décidé ad-hoc après concertation des États membres (exemple : attentats sur le territoire européen concernant plusieurs États membres)
Considérant 37 : **Given the challenges that the use of new technologies by criminals pose to the Union's security, law enforcement authorities are required to strengthen their technological capacities. To that end, Europol should support Member States in the use of emerging technologies in preventing and countering crimes falling within the scope of Europol's objectives. To explore new approaches and develop common technological solutions for Member States to prevent and counter crimes falling within the scope of Europol's objectives, Europol should be able to conduct research and innovation activities regarding matters covered by this Regulation, including with the processing of personal data where necessary and whilst ensuring full respect for fundamental rights.** **The provisions on the development of new tools by Europol should not constitute a legal basis for their deployment at Union or national level.**	Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation. Elle rappelle que la Commission, dans sa stratégie de sécurité intérieure pour l'Union 2020-2025 évoquait dans la lignée de la révision du règlement Europol *« la création **d'un pôle d'innovation européen** pour la sécurité intérieure qui serait chargé de définir des solutions conjointes à des défis communs en matière de sécurité et face à des opportunités que les États membres ne peuvent exploiter seuls »*. Elle précisait que ce pôle travaillerait avec Frontex, CEPOL, eu-LISA et le Centre commun de recherche (JRC). Afin de mutualiser les moyens humains et financiers, les autorités françaises souhaitent que **l'ensemble des agences JAI** soient impliquées dans le développement d'outils technologiques. Elles ajoutent que le CEPD et la FRA doivent pouvoir être impliquées dans ce processus si nécessaire. Proposition d'amendement : "To that end, Europol should ***in close***

	cooperation with relevant Union bodies support Member States in the use of emerging technologies in preventing and countering crimes falling within the scope of Europol's objectives."
Considérant 38 : **Europol should play a key role in assisting Member States to develop new technological solutions based on artificial intelligence, which would benefit national law enforcement authorities throughout the Union. Europol should play a key role in promoting ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety and fundamental rights.**	Les autorités françaises réitèrent leur commentaire précédent (considérant 37). et propose l'amendement suivant : ***Europol should in close cooperation with relevant Union bodies play a key role in assisting Member States to develop new technological solutions based on artificial intelligence, which would benefit national law enforcement authorities throughout the Union. Europol should play a key role in promoting ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety and fundamental rights.***
Considérant 40: **Providing Europol with additional tools and capabilities requires reinforcing the democratic oversight and accountability of Europol. Joint parliamentary scrutiny constitutes an important element of political monitoring of Europol's activities. To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group with annual information on the use of these tools and capabilities and the result thereof.**	Afin de suivre et d'enrichir les travaux de l'agence, cette information annuelle doit être communiquée aux États-membres. Les autorités françaises proposent de modifier le considérant comme suit : « *To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny* ***Group and the Member States*** *with annual information on its use of these tools and capabilities and the result thereof* ».
Considérant 41: **Europol's services provide added value to Member States and third countries. This includes Member States that do not take part in measures pursuant to Title V of Part Three of the Treaty on the Functioning of the European Union. Member States and third countries may contribute to Europol's budget based on separate agreements.** **Europol should therefore be able to receive contributions from Member States and third**	Les autorités françaises s'étonnent d'une telle proposition et rappellent que l'agence Europol ne peut voir se créer un lien de dépendance plus spécifique avec un État au prétexte qu'il contribuerait davantage à son budget que les autres. Cette situation serait préjudiciable à la fois pour les Etats-membres mais également pour l'image de l'agence et la confiance que les Etats-membres placent en elle. Elles souhaitent donc que la Commission soit interrogée sur l'existence d'un tel mécanisme

countries on the basis of financial agreements within the scope of its objectives and tasks.	dans d'autres agences de l'UE qui concerne non seulement **les États-Membres mais également les États tiers**. L'expérience acquise par les autorités françaises dans d'autres enceintes multilatérales où les États-membres financent les projets au cas par cas leur permet **d'émettre d'importantes réserves sur ce mécanisme**. Celui-ci **créera inévitablement des déséquilibres forts, en matière d'influence, entre les États capables de financer des projets et ceux qui ne le peuvent ou ne le souhaitent pas.** Enfin il doit être redouté que les projets soutenus par les États membres soient systématiquement soumis à des conditions de ressources dans les documents de programmation tandis que ceux portés par la Commission ou Europol seront considérés comme financés *ab initio*.
II) ARTICLES	
<u>Article – 1 (1) (c)</u> (q) investigative case file' means a dataset or multiple datasets that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation, in accordance with procedural requirements and safeguards under the applicable national criminal law, and submitted to Europol in support of that criminal investigation	Les autorités françaises jugent cette disposition restrictive et précise que d'autres agences JAI pourraient également transférer des dossiers d'enquête à Europol.
<u>Article 1 (2) (a) (i)</u> **<u>Tasks</u>** **(h) Support Member States cross-border information exchange activities, operations and investigations, as well as joint investigation teams, and special intervention units, including by providing operational, technical and financial support;**	Les autorités françaises réitèrent leur commentaire précédent sur le considérant 4. De nouvelles tâches sont assignées à Europol, sans articulation avec les compétences des Etats membres ou avec d'autres entités européennes : quid de l'articulation avec l'IntCen ?

Article 1 (2) (a) (iv): (q) support Member States in identifying persons whose involvement in crimes falling within the scope of Europol's mandate, as listed in Annex I, constitute a high risk for security, and facilitate joint, coordinated and prioritised investigations ;	(q) : CF commentaires sur le concept de « high risk ». Soit la proposition de rédaction suivante : (q) support Member States in identifying persons **or groups** whose involvement in crimes falling within the scope of Europol's mandate, as listed in Annex I, constitute a high **criminal threat** for security, and facilitate joint, coordinated and prioritised investigations ;
Article 1 (2) (a) (iv) **Tasks** (r) enter data into the Schengen Information System, in accordance with Regulation (EU) 2018/1862, following consultation with the Member States in accordance with Article 7 of this Regulation, and under authorization by the Europol Executive Director, on the suspected involvement of a third country national in an offence in respect of which Europol is competent and of which it is aware on the basis of information received from third countries or international organizations within the meaning of Article 17(1)(b);	La délégation française notera la persistance de la proposition de la Commission s'agissant de la possibilité d'octroyer un rôle à l'agence dans l'incrémentation du SIS en créant une catégorie pour information. La délégation française réaffirmera son opposition sur ce point et fera remarquer qu'une telle proposition ne répond pas aux difficultés opérationnelles soulevées lors des précédentes réunions du LEWP mais aussi dans le cadre des débats en TWP sur le protocole d'insertion des CTE dans le SIS et que le coût particulièrement élevé que représente sa mise en œuvre sans réelle plus-value opérationnelle ne plaide pas en sa faveur.
Article 1 (2) (a) (iv) **Tasks** (s) support the implementation of the evaluation and monitoring mechanism under Council Regulation (EU) No 1053/2013 within the scope of Europol's objectives as set out in Article 3;	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 9. Pour mémoire : Les autorités françaises s'interrogent sur la plus-value d'une référence à ce règlement ainsi que sur le rôle qu'Europol pourrait prendre dans ce **dispositif déjà prévu dans le règlement 1053/2013**. Le cadre actuel impliquant une évaluation entre « pairs » apparaît satisfaisant et les autorités françaises rappellent que la référence à ce règlement n'a pas été inscrite par le législateur en 2016 lors de l'élaboration du règlement actuel. De même, il convient de s'interroger sur la façon dont ce considérant s'articule avec les objectifs fixés par l'analyse d'impact initiale sur le

	renforcement du mandat d'Europol.
Article 1 (2) (a) (iv) **Tasks** (t) proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States, and implement its research and innovation activities regarding matters covered by this Regulation, including the development, training, testing and validation of algorithms for the development of tools	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 37. Pour mémoire : Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.
Article 1 (2) (d) **Tasks** **4a. Europol shall assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation activities that are relevant to achieve the objectives set out in Article 3. When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, the Agency shall not receive funding from that programme.**	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 37. Pour mémoire : Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.
Article 1 (2) d) **Tasks** **4b. Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council* that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3**	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 12. Pour mémoire : les autorités françaises rappellent que le règlement 2019/452 cité ne fait pas référence à l'agence Europol ce qui pourrait créer une situation d'insécurité juridique quant à la mise en pratique d'une telle mission. Ensuite, le considérant introduit la notion « **d'ordre public** » pour laquelle l'agence Europol n'est pas compétente.

on the expected implications for security.	Enfin, un conflit d'intérêt pourrait émerger quand il s'agira pour l'agence d'étudier des investissements directs étrangers qui concernent le développement/l'utilisation de technologies par Europol comme peut le démontrer le développement du Poste de commandement virtuel (VCP) d'Europol. Pour rappel le VCP est une technologie développée par une entreprise dont l'établissement légal se situe hors de l'Union européenne. Les autorités françaises s'interrogent enfin sur la façon dont ce considérant s'articule avec les objectifs fixés par l'analyse d'impact initiale sur le renforcement du mandat d'Europol.
Article 4 paragraph 5 **Tasks** **Europol staff may assist the competent authorities of the Member States, at their request and in accordance with their national law, in the taking of investigative measures.**	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 13. Pour mémoire : Les autorités françaises demeurent attentives à la proposition de la Commission permettant au personnel d'Europol **d'assister les autorités compétentes dans la mise en place de « mesures d'enquête »**. Si ce point n'apparaît pas bloquant en l'état, il importe que la Commission détaille davantage cette disposition et fournisse des cas concrets d'application.
Article 1 (3) **Request by Europol for the initiation of a criminal investigation** In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation.	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 14. Pour mémoire : Dans la continuité de la note de commentaire des autorités françaises du 30 octobre 2020, **les autorités françaises sont défavorables à la révision de l'article 6 du règlement Europol actuel**. En effet, cette disposition n'est quasiment pas mise en œuvre et les enquêteurs, en lien avec leurs autorités judiciaires, doivent disposer de la maîtrise de l'ouverture de leurs

	enquêtes. Les autorités françaises rappellent tout de même que, interrogées sur le sujet, ni la Commission, ni Europol n'ont pu fournir de statistiques concernant le recours à l'article 6 du règlement Europol actuel. Toutefois, les autorités françaises constatent que la nouvelle rédaction de l'article 6 tient compte de certaines réserves exposées et ne prévoit pas de pouvoir d'enquête d'initiative pour l'agence. Elles relèvent enfin que la préservation de l'efficacité des choix des stratégies d'entrave milite en faveur de la maitrise du dialogue entre services enquêteurs et autorités judiciaires.
Article 1(4) ***Article 7*** **:** "8. Member States shall ensure that their financial intelligence units established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council* are allowed to cooperate with Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and the Council**, in particular via their national unit regarding financial information and analyses, within the limits of their mandate and competence. _____ * Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73). ** Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the	Les autorités françaises suggèrent de modifier à l'article 7 paragraphe 8 la phrase qui indique que les CRF sont autorisées à coopérer avec Europol par la phrase suivante : « les CRF sont habilitées à donner suite aux demandes dûment justifiées présentées par Europol ». Cela permettrait de mieux retranscrire la Directive (UE) 2019/1153 dont est issue cette modification. Soit la proposition de rédaction suivante : *8. Member States shall ensure that their financial intelligence units established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council* are* ***entitled to reply to duly justified requests made by*** *Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and the Council**, in particular via their national unit regarding financial information and analyses, within the limits of their mandate and competence.*

prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ L 186, 11.7.2019, p. 122)."	
Article 1(5) **Purposes of information processing activities** (f) supporting Member States in informing the public about suspects or convicted individuals who are wanted based on a national judicial decision relating to a criminal offence in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals.	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 15. Pour mémoire : Les autorités françaises proposent que ce considérant soit modifié comme suit : "***Upon request from Member States, Europol may provide its support in informing the public about suspects or convicted individuals who are wanted based on a national judicial decision relating to a criminal offence in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals".***
Article 1 (6) **Art 18a** **Information processing in support of a criminal investigation** 1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where: (a) a Member State or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2); and (b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded.	

2. Europol may process personal data contained in an investigative case for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by a Member State or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided.	
3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State. That Member State may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a related criminal investigation are on-going in another Member State. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Such	

personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.	
4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, or the EDPS, reaches the conclusion that there are preliminary	Les autorités françaises s'étonnent de la possibilité offerte à certains États tiers de pouvoir bénéficier du soutien d'Europol dans l'analyse de données. Sur le plan juridique, la mise en œuvre d'une telle proposition nécessiterait de réviser l'ensemble des accords opérationnels de l'agence en prenant en compte ces nouvelles dispositions Par ailleurs, les autorités françaises considèrent que si ces transmissions de données personnelles n'ont pas donné lieu à une ouverture d'enquête par un Etat membre, une telle proposition implique pour Europol la nécessité de soutenir une enquête criminelle menée par un État tiers. Or, Europol est une agence qui soutient **en priorité les États membres** dans leurs enquêtes. Il est donc indispensable que, si les données fournies par un Etat tiers devaient être ainsi exploitées, cela ne devrait se faire qu'au profit d'un ou plusieurs États-membres ayant ouvert une enquête miroir permettant d'exploiter ces données. Les autorités françaises rappellent l'importance de la règle du tiers service/propriété de l'information s'agissant des données communiquées à Europol. Dès lors, les échanges relatifs à des données en provenance des EM doivent strictement respecter ce cadre.
Article 1(8) **Article 20a** **Relations with the European Public Prosecutor's Office**	La relation avec le parquet européen était fortement attendue et correspond au rôle que les États membres ont entendu confier à Europol dans ces champs de compétence déterminants pour l'avenir des forces de sécurité intérieure de l'Union. Une attention particulière demeurera néanmoins sur les conditions d'encadrement de l'alinéa 4 de l'article 20(a) portant sur le

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation. **2. Europol shall actively support the investigations and prosecutions of the EPPO and cooperate with it, in particular through exchanges of information and by providing analytical support.** **3. Europol shall take all appropriate measures to enable the EPPO to have indirect access to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system. Article 21 shall apply mutatis mutandis with the exception of its paragraph 2.** **4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence.**	transfert de données à l'EPPO. Les autorités françaises rappellent les dispositions de l'article 102 du règlement Parquet européen qui disposent que le Parquet européen « *peut également demander à Europol de fournir une aide à l'analyse dans le cadre d'une enquête particulière conduite par le Parquet européen* ». Elles estiment par conséquent que **le terme de « poursuites » doit être retiré de cette proposition d'article.** **Les autorités françaises s'interrogent également sur la compatibilité entre le quatrième alinéa de l'article 20(a) et le principe de propriété de l'information tel que prévu par le règlement Europol.** **Enfin, un cinquième alinéa pourrait être proposé invitant Europol à produire devant le CAE, un rapport annuel sur la relation entre l'agence et l'EPPO.**
<u>Article 1 (11)</u> **<u>Article 25</u>** **Transfer of personal data to third countries and international organisations** (a) In paragraph 5, the introductory phrase is replaced by the following: "By way of derogation from paragraph 1, the Executive Director may authorise the transfer or categories of transfers of personal data to third countries or international organisations on a case-by-case basis if the transfer is, or the related transfers are: **(b) In paragraph 8, the following sentence is deleted :** **Where a transfer is based on paragraph 5,**	Les autorités françaises soulignent que la Commission européenne n'a pas modifié le régime général de l'échange de données par Europol avec les États tiers. Les autorités françaises estiment que l'article 25 ne permet pas de pallier aux rigidités du cadre juridique actuel en la matière. Enfin, elles proposent que le cadre relatif à l'échange de données personnelles entre Europol et les États tiers soit calqué sur celui **d'Eurojust.**

such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.	
Article 1 (12) ***Article 26*** **:** "5. Europol may transmit or transfer personal data to private parties on a case-by-case basis, where it is strictly necessary, and subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67, in the following cases: (a) the transmission or transfer is undoubtedly in the interests of the data subject, and either the data subject has given his or her consent; or (b) the transmission or transfer is absolutely necessary in the interests of preventing the imminent perpetration of a crime, including terrorism, for which Europol is competent; or (c) the transmission or transfer of personal data which are publicly available is strictly necessary for the performance of the task set out in point (m) of Article 4(1) and the following conditions are met: (i) the transmission or transfer concerns an individual and specific case; (ii) no fundamental rights and freedoms of the data subjects concerned override the public interest necessitating the transmission or transfer in the case at hand; or (d) the transmission or transfer of personal data is strictly necessary for Europol to inform that private party that the information received is insufficient to enable Europol to identify the national units concerned, and the following conditions are met: (i) the transmission or transfer follows a receipt of personal data directly from a private party in accordance with paragraph 2 of this Article;	Les autorités françaises s'interrogent sur les conditions mentionnées au paragraphe 5 de l'article 26 et sur la nature cumulative de ces dernières.

(ii) the missing information, which Europol may refer to in these notifications, has a clear link with the information previously shared by that private party; (iii) the missing information, which Europol may refer to in these notifications, is strictly limited to what is necessary for Europol to identify the national units concerned.	
Article 26 **:** 6. With regard to points (a), (b) and (d) of paragraph 5 of this Article, if the private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, the transfer shall only be authorised by the Executive Director if the transfer is: (a) necessary in order to protect the vital interests of the data subject or another person; or (b) necessary in order to safeguard legitimate interests of the data subject; or (c) essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or (d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences for which Europol is competent; or (e) necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence for which Europol is competent. Personal data shall not be transferred if the Executive Director determines that fundamental rights and freedoms of the data subject	Il est précisé à l'article 26, paragraphe 6 (e) que les transferts ne doivent pas être systématiques, massifs ou structurels. Les autorités françaises aimeraient obtenir des clarifications sur ce point et notamment afin de savoir s'il concerne uniquement les demandes d'information d'Europol aux parties privées située hors de l'UE ou dans un pays sans accord en matière de protection des données personnelles ou s'il s'applique à l'ensemble des échanges entre Europol et les parties privées.

concerned override the public interest in the transfer referred to in points (d) and (e). Transfers shall not be systematic, massive or structural."	
Article 1 (20) **Article 34 :** (a) paragraph 1 is replaced by the following: "1. In the event of a personal data breach, Europol shall without undue delay notify the competent authorities of the Member States concerned, of that breach, in accordance with the conditions laid down in Article 7(5), as well as the provider of the data concerned unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."; (b) (b) paragraph 3 is deleted;	La modification de l'article 34 et la suppression de la notification à l'EDPS ne sont pas documentées dans la présentation des modifications apportées à l'actuel règlement. Une réinsertion de cette notification à l'EDPS est donc souhaitable pour l'instant. **Soit la proposition de rédaction suivante :** In the event of a personal data breach, Europol shall without undue delay notify ***the EDPS as well as*** the competent authorities of the Member States concerned, of that breach, in accordance with the conditions laid down in Article 7(5), as well as the provider of the data concerned unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.'';
Article 1 (37) **Article 51** **Joint Parliamentary scrutiny** (h) annual information about the number of cases in which Europol issued alerts in the Schengen Information System in accordance with Article 4(1)(r), and the number of 'hits' these alerts generated, including specific examples of cases demonstrating why these alerts were necessary for Europol to fulfil its objectives and tasks;	Les autorités françaises demandent la suppression de cet article, lequel ne tient pas compte du protocole validé en COSI.
Article 1 (38) **Article 57** **Budget** **4. Europol may benefit from Union funding in the form of contribution agreements or grant agreements in accordance with its financial rules referred to in Article 61 and**	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 41. Pour mémoire : Les autorités françaises s'étonnent d'une telle proposition et rappellent que l'agence Europol ne peut voir se créer un lien de dépendance plus

with the provisions of the relevant instruments supporting the policies of the Union. Contributions may be received from countries with whom Europol or the Union has an agreement providing for financial contributions to Europol within the scope of Europol's objectives and tasks. The amount of the contribution shall be determined in the respective agreement.	spécifique avec un État au prétexte qu'il contribuerait davantage à son budget que les autres. Cette situation serait préjudiciable à la fois pour les Etats-membres mais également pour l'image de l'agence et la confiance que les Etats-membres placent en elle. Elles souhaitent donc que la Commission soit interrogée sur l'existence d'un tel mécanisme dans d'autres agences de l'UE qui concerne non seulement **les États-Membres mais également les États tiers**. L'expérience acquise par les autorités françaises dans d'autres enceintes multilatérales où les États-membres financent les projets au cas par cas leur permet **d'émettre d'importantes réserves sur ce mécanisme**. Celui-ci **créera inévitablement des déséquilibres forts, en matière d'influence, entre les États capables de financer des projets et ceux qui ne le peuvent ou ne le souhaitent pas.** Enfin il doit être redouté que les projets soutenus par les États membres soient systématiquement soumis à des conditions de ressources dans les documents de programmation tandis que ceux portés par la Commission ou Europol seront considérés comme financés *ab initio*. La définition « **countries with whom Europol or the Union has an agreement providing for financial contributions to Europol within the scope of Europol's objectives and tasks" mériterait d'être précisée.**

Article 1 (40) **Article 67** 1. The Europol shall adopt its own security rules that shall be based on the principles and rules laid down **in the Commission's security rules** for protecting European Union classified information (EUCI) and sensitive non-classified information including, inter alia, provisions for the exchange of such information with third countries, and processing and storage of such information as set out in Commission Decisions (EU, Euratom) 2015/443 (44) and (EU, Euratom) 2015/444 (45). A**ny administrative arrangement on the exchange of classified information** with the relevant authorities of a third country or, in the absence of such arrangement, any exceptional ad hoc release of EUCI to those authorities, **shall be subject to the Commission's prior approval**. 2. The Management Board shall adopt the Europol's security rules **following approval by the Commission.** When assessing the proposed security rules, the Commission shall ensure that they are compatible with Decisions (EU, Euratom) 2015/443 and (EU, Euratom) 2015/444.	Les autorités françaises remarquent que, là où les règles de sécurité d'Europol étaient auparavant alignées sur les règles de sécurité du Conseil (décision 2013/488/UE), elles sont désormais basées sur les règles de sécurité de la Commission. En outre, la Commission est dotée d'un pouvoir important, puisqu'elle approuve les règles de l'agence avant qu'elles ne soient adoptées. Pourtant, il nous semble ressortir du règlement Europol que l'agence répond au Conseil, et non à la Commission (c'est notamment le Conseil qui nomme le directeur exécutif, et qui peut lui demander de lui rendre compte). **Les autorités françaises s'interrogent sur les raisons de ce changement envisagé par la proposition de la Commission.**

3. Propositions d'articles additionnels

Afin d'enrichir cette proposition, les autorités françaises souhaitent proposer l'ajout de certains articles.

1) Renforcer la confiance des services opérationnels dans l'agence Europol

a) Permettre aux services opérationnels de demander à Europol de recueillir des données personnelles auprès de parties privées

Les autorités françaises proposent l'ajout d'un article 26 (b) : La création d'un article 26b vise à demander à Europol, sur sollicitation de **deux ou plusieurs États membres enquêtant sur un même dossier**, de recueillir des données personnelles auprès d'une entreprise privée dont le principal établissement légal se trouve sur ou hors du territoire de l'Union européenne. L'agence communiquera ensuite aux Unités nationales les informations captées et pourra elle-même les intégrer dans ses bases de données.

Exemple : dans le cadre d'une enquête commune (ECE) entre la France, la Belgique et les Pays-Pays en matière de trafic de stupéfiants, les États membres travaillant sur un même dossier pourraient exiger d'Europol – via SIENA et un modèle de demande préétabli – que l'agence les représente et puisse exiger des données personnelles détenues par un GAFAM (Google, Apple, Facebook, Amazon, Microsoft).

Justifications : Europol – agence représentant 500 M de citoyens – disposerait d'un poids démographique beaucoup plus important qu'un État membre seul en termes de représentation et de négociation avec des entreprises mondialisées. En outre, elle déchargerait les services opérationnels de demandes chronophages et fastidieuses.

Proposition d'article : Nouvel article 26 (b) : Demande de données personnelles avec les parties privées :

« Dans le cadre d'une enquête relevant des infractions pour lesquelles l'agence est compétente et touchant au moins deux États-membres, Europol peut, à la demande d'un État membres solliciter d'une partie privée, dont le principal établissement légal est établi sur ou en dehors du territoire de l'Union européenne, la communication de données personnelles pertinentes.

Europol peut, dans la mesure où cela est nécessaire à l'accomplissement de ses missions traiter ces données personnelles et les communiquer aux Unités nationales concernées ».

b) Assurer la transparence sur le traitement par Europol des informations transmises par les services opérationnels

Les autorités françaises proposent de modifier l'article 19 du règlement Europol consacré au principe de propriété de l'information transmise à Europol. Elle propose que soit clairement inscrite dans cet article **la notion de propriété de l'information** et souhaite, à l'instar de ce qui se pratique actuellement pour les codes de gestion, que le service contributeur puisse faire savoir à l'agence s'il souhaite que la donnée transmise puisse être ultérieurement transférée aux institutions, agences, et organes de l'Union européenne.

Justification : Cette disposition permettra aux services contributeurs de s'assurer que les informations soient traitées de manière transparente. Cette disposition permettra en outre de renforcer la confiance des enquêteurs dans l'agence et de ce fait d'augmenter leurs contributions.

Proposition : article 19 : détermination des finalités du traitement d'informations par Europol et des limitations en la matière

1. Tout État membre, organe de l'Union, pays tiers ou organisation internationale qui fournit des informations à Europol définit la ou les finalités du traitement de ces données conformément à l'article 18. À défaut, Europol, en accord avec le fournisseur des informations concerné, traite ces informations en vue de déterminer leur pertinence ainsi que la ou les finalités de leur traitement ultérieur. Europol ne peut traiter ces informations à des fins autres que celles pour lesquelles elles ont été fournies que si le fournisseur des informations l'y autorise.

BIS. Tout Etat Membre qui fournit des informations à Europol et qui définit la finalité du traitement de ces données doit au préalable s'assurer de leur propriété sur celles-ci.

2. ***Dans le respect du principe de propriété de l'information*** les États membres, les organes de l'Union, les pays tiers et les organisations internationales peuvent notifier, lors de la fourniture des informations à Europol, toute limitation de l'accès à ces données ou de leur utilisation, en termes généraux ou spécifiques, y compris en ce qui concerne leur transfert, effacement ou destruction. ***Les États membres peuvent notifier dès la fourniture d'information toute limitation de l'accès à ces données ou de leur utilisation, en termes généraux ou spécifiques lorsque ces données sont susceptibles d'être transmises aux institutions, agences et organes de l'Union européenne.*** Lorsque la nécessité d'appliquer ces limitations apparaît après la fourniture des informations, ils en informent Europol. Europol se conforme à ces limitations.

Dans des cas dûment justifiés, Europol peut soumettre les informations extraites auprès de sources accessibles au public à des limitations d'accès ou d'utilisation par les États membres, les organes de l'Union, les pays tiers et les organisations internationales.

2) renforcer le contrôle des États membres sur l'agence

a) Clarifier le nombre d'informations échangées par Europol avec les parties privées et les États tiers

Les autorités françaises proposent un nouvel article 7 (12) consacré aux informations personnelles échangées par Europol avec les États tiers et les parties privées avec l'établissement d'un rapport annuel sur les informations échangées par Europol avec les États membres et les États tiers.

Justification: elles considèrent que les nouvelles missions dévolues à Europol doivent être accompagnées d'un plus grand contrôle des États membres.

Proposition de rédaction de l'article 7 (12) : Informations échangées par Europol avec les États tiers et les parties privées

« *Europol rédige un rapport annuel portant sur la nature et le volume des données personnelles fournies à Europol par les États tiers et les parties privées sur la base des critères d'évaluation quantitatifs et qualitatifs fixés par le conseil d'administration. Ce rapport annuel est transmis au Parlement européen, au Conseil, à la Commission et aux parlements nationaux* **».**

b) Permettre aux États de disposer d'informations claires et précises sur les activités de l'agence

Les autorités françaises proposent de créer un nouvel article 7 (bis) afin de permettre aux États membres de disposer du maximum d'informations pour le bon suivi des travaux de l'agence. A l'instar de ce qui se pratique pour le Groupe parlementaire conjoint de surveillance JPSG, elles proposent la création d'un cadre dédié aux questions des États membres pour lesquelles Europol devra présenter des réponses claires et précises. A l'heure actuelle, les États membres sont confrontés à une agence qui ne répond pas toujours avec précision aux questions posées.

Justification : les autorités françaises considèrent que certaines questions posées par les États membres à l'agence trouvent des réponses insatisfaisantes.

Proposition de rédaction de l'article 7 bis: Contrôle opérationnel et stratégique d'Europol

« *Europol met en place toutes les mesures nécessaires pour permettre à chaque Etat membre de disposer des informations opérationnelles et stratégiques nécessaires au contrôle de l'ensemble de ses activités.*

Le Conseil d'administration, sur proposition du directeur exécutif, adopte des règles internes permettant aux États membres de disposer de ces informations ».

3) Ressources humaines

En mars 2020 Europol nous informait que depuis 2010, **51 contrats à durée indéterminés (CDI)** avaient été accordés (47 TA et 4 CA). Pour la seule année 2019, 18 CDI ont été accordés et se répartissent à des niveaux d'encadrement élevé (AD 07 à AD 10). Les autorités françaises considèrent que la pérennisation d'emplois est une pratique dangereuse quand il s'agit de poste de direction, dit de haut niveau d'encadrement.

Sans préjudice des règles européennes en la matière et suivant une analyse juridique précise qu'il conviendra de mener, les autorités françaises proposent que la question de la « CDIsation » des postes à haut niveau soit discutée et **encadré** dans le règlement Europol.

GERMANY

Please find below Germany's written submission for agenda item 5 – Revision of the Europol Regulation – of the last LEWP meeting:

We would like to thank the Commission for this comprehensive legislative proposal that addresses important and pressing challenges not only for Europol, but also for law enforcement authorities throughout the EU. The assessment of the proposal and the consultations within the federal government are still pending. Therefore, Germany has to enter a general scrutiny reservation and will confine itself to the following initial comments:

For MS it is essential that Europol has the ability to effectively support national law enforcement authorities. This has been demonstrated by the discussion in the LEWP over the past months and years. And this is shown by the fact that the EU Home Affairs Ministers – in their Declaration on the Future of Europol – have jointly and unanimously defined the MS's core ideas for the future development of Europol.

Based on our initial assessment, Germany welcomes the general aim of the proposal insofar as it addresses existing deficits and legal challenges. This includes, in particular, the aims of remedying the EDPS' admonishment regarding the "Europol's big data challenge", improving cooperation with Private Parties and third countries as well as strengthening Europol's ability to support MS in the field of innovation. We still have to check the suitability of the proposals to achieve these objectives in detail. As for the further discussion of the proposal in the LEWP, we think it is urgent to reach first and tangible results on these crucial issues. We also take positive note of the proposed increase in resources.

Besides that, our first assessment of the proposal already led to certain points that we are not convinced of at this stage and that certainly require further examination and discussion:

The first point is the proposed active role of Europol in the SIS. We would like to raise a scrutiny reservation on this point, as we will have to look further into this issue. We still have general questions, including the following:

- We would like to ask the Commission how they assess compatibility with EU primary law, liability for the alerts and for the follow up measures taken.
- It would be interesting to learn how the Commission envisages resolving the following situation: If the information available is not sufficient for Member States to issue an alert, on what basis would Europol be able to issue an alert in such a case? What is the added value of Europol issuing an alert compared with a solution in which Europol analyses and prepares the information for the Member States in such a way that it is sufficient for issuing an alert, which the Member States can then issue themselves?
- In addition, we would be interested in how the Commission assesses the practical use of a separate alert category for Europol, when the question of how to deal with a hit is left to MS. How does the Commission assess the shift in responsibility vis-à-vis the general principles of the SIS, that include mutual trust in the decisions of law enforcement authorities of Member States and that the information in the system is actionable?

The second point relates to proposals that would give the Commission a right to issue instructions to Europol, i.e. in the context of preparing situational analyses or when it comes to evaluation research projects. This could undermine the independence of the agency and it also contradicts the clear positioning in the Ministerial Declaration.

The third point relates to the proposed cooperation with the EPPO insofar as it would go beyond the cooperation foreseen in the EPPO regulation.

The fourth point relates to the proposal to provide operational support to special intervention units. The Home Affairs Ministers have clearly stated that the agency should not have executive powers.

The fifth point concerns the numerous changes concerning data protection, including the reaction to the EDPS decision concerning "Europol's big data challenge". We still have to examine more closely whether the proposal appropriately addresses the concerns raised by the EDPS and at the same time ensures that Europol can continue to process big data in their support of Member States.

Lastly, we would be interested to hear the reasons why the proposal lacks an improvement of the structural exchange of personal data with third countries and did not try to find a solution that takes into account the conditions set out in the ECJ's Schrems II decision. From an operational point of view, it seems urgently necessary to address this topic in the proposal, as no new third-country agreement has been concluded since the entry into force of the Europol Regulation in 2017 and therefore there was the conclusion in the recent discussions in LEWP that the current regime is dysfunctional.

Our further positioning will take place within the framework of discussions of the individual topics.

HUNGARY

Please find below the preliminary comments made by Hungary on the proposal for amending Regulation (EU) 2016/794. First of all we would like to stress that the Hungarian authorities are scrutinising the text of the regulation, and in this regard please consider our comments as initial ones.

In general Hungary agrees that the current Europol Regulation needs to be revised in a number of areas, as the challenges of recent years and the shortcomings identified in its implementation have made it clear that the Agency's role in supporting Member States can be implemented much more effectively, furthermore numerous tasks have arisen for Europol which need to be codified, for example strengthening cooperation with private parties and third countries is an urgent task. Having said this we would like to emphasize that by this regulation our aim should be to strengthen the core tasks of the agency and in this regard we consider it important to ensure the compliance with the Treaties and to avoid extending the mandate of the Europol to issues that fall within the exclusive competence of the Member States (such as the initiation/prioritisation of investigations).

However, in line with our preliminary observations, we would like to emphasize that we do not consider it acceptable that the revision of the Europol Regulation should go beyond the provisions set out in the EPPO Regulation. It is a matter of concern that, according to the draft text, Europol would be actively involved into EPPO procedures, as in our view, this would mean that Europol would be able to carry out its analysis based on its own initiative with the aim to suggest the initiation of investigations of the EPPO. In our view this could be considered as an indirect kind of "investigative" activity.

We are also concerned that the regulation would allow EPPO to have an indirect access to information stored in Europol's databases, as part of these information are provided by Member States which do not take part in the implementation of the EPPO regulation.

In our view, it is also worrying that, "in specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation". We think that this provision would allow the agency to set priorities for the Member States when it comes to investigations carried out in the territory.

Finally, we would like to emphasize that prior consultation of Member States would be essential when it comes to sharing data sharing with private parties especially when the "private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation".

ITALY

ITALIAN CONTRIBUTIONS ON THE "*PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL AMENDING REGULATION (EU) 2016/794, AS REGARDS EUROPOL'S COOPERATION WITH PRIVATE PARTIES, THE PROCESSING OF PERSONAL DATA BY EUROPOL IN SUPPORT OF CRIMINAL INVESTIGATIONS, AND EUROPOL'S ROLE ON RESEARCH AND INNOVATION*" **TO BE DISCUSSED AT THE LEWP MEETING ON 28 JANUARY**

DOC. ST.13908/20

PROPOSAL OF THE COMMISSION	**ITALIAN COMMENTS**
With reference to recital 3: *These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal organised crime groups that engage in a wide range of criminal activities.*	Italy believes that it is of utmost importance to recall the pivotal role that mafia-style and family-based criminal organizations have played in taking advantage of the opportunities of the health emergency and digitization. We therefore propose a revised version of recital 3: *These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal, mafia-style and family based organised crime groups that engage in a wide range of criminal activities.*
With reference to recital 6: *"High-risk criminals play a leading role in criminal networks and pose a high risk of serious crime to the Union's internal security. To combat high-risk organised crime groups and their leading members, Europol should be able to support Member States in focusing their investigative response on identifying these persons, their criminal activities and the members of their criminal networks".*	Italy believes that with reference to the establishment of the Operational Task Forces (OTF) and the identification of the High Value Targets (HVT), it is of utmost importance to better define, in the proposal Regulation, the evaluation criteria and the selection procedures. Moreover Italy believes that in this part, as said with reference to recital 3, it would be pivotal to mention, mafia style and family based organised crime groups.

With reference to recital 8 and the connected amendment of art.4 r)	Italy will give its contribution when the SIS-Europol proposal will be discussed at the dedicated meeting of IXIM and LEWP. We can anticipate however that we believe that giving Europol such power is likely to alter excessively the SIS general balanced structure based on national judicial or LEAs decision for any SIS alert. Italy believes that the system currently in place ensures the certainty of the actions to be taken and creates a clear responsibility for the Member State concerned.
With reference to recital 12 and connected new paragraph 4b of art.4 *".Europol should support the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes."*	Italy believes that UNEs and AROs should be explicitly involved in the screening of foreign direct investments. *Therefore* we propose to rephrase the recital as follows: *"Europol,* through its UNEs and in collaboration with ARO Offices, should support *the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes."*
With reference to recital 15 and the connected new article 18 f) **Recital 15:** *Publishing the identity and certain personal data of suspects or convicted individuals, who are wanted based on a Member State's judicial decision, increases the chances of locating and arresting such individuals. To support Member States in this task, Europol should be able to publish on its website information on Europe's most wanted fugitives for criminal offences in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals.*	Italy believes that the authorization to disclose information concerning investigative activities should be decided by the judicial authorities and investigators. In order to avoid confusion the text of recital 15 should clarify this aspect. Furthermore, we believe that any kind of support from Europol on activities related to informing the public should be only upon explicit support request coming from Member States. Moreover, we have to be cautious with this provision. We have a scrutiny reserve on this point in order to assess the actual need for a support from Europol in informing the public (especially for persons that are only suspects).

Art 18 f *"supporting Member States in informing the public about suspects or convicted individuals who are wanted based on a national judicial decision relating to a criminal offence in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals."*	Therefore we suggest to modify the text of recital 15 and Art 18f as follows: Recital 15 To *support Member States in this task, Europol, upon competent national judicial authority permission, should be able to publish on its website information on Europe's most wanted fugitives for criminal offences in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals*. Art 18 f supporting *Member States in informing the public, upon explicit request from Member States as well as authorization by the competent national judicial authority, about suspects or convicted individuals who are wanted based on a national judicial decision relating to a criminal offence in respect of which Europol is competent, and facilitate the provision of information by the public on these individuals*
With reference to recital 33: *(33) Any cooperation of Europol with private parties should neither duplicate nor interfere with the activities of the Financial Intelligence Units ('FIUs'), and should only concern information that is not already to be provided to FIUs in accordance with Directive 2015/849 of the European Parliament and of the Council.. Europol should continue to cooperate with FIUs in particular via the national units.*	Italy is in favour of this provision and strongly support it. Given its relevance, we would like it to be merged or incorporated under art 7 of the proposal. On top of that, Italy also believes that it would be very important that the new text explicitly refers to the principle that all cooperation between Europol and private parties should be in place in full respect of domestic legal framework. This addition is also motivated in order to align the text proposal with the principle set out under Directive 2019/1153. If agreed the new wording of Art 7 par 8 would be replaced by the following: *"8. Member States shall ensure that their financial intelligence units established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council* are allowed to cooperate without prejudice and respecting the domestic legal frameworks with Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European*

	*Parliament and the Council**, in particular via their national unit regarding financial information and analyses, within the limits of their mandate and competence. Any cooperation of Europol with private parties should neither duplicate nor interfere with the activities of the Financial Intelligence Units ('FIUs'), and should only concern information that is not already to be provided to FIUs in accordance with Directive 2015/849 of the European Parliament and of the Council. Europol should continue to cooperate with FIUs in particular via the national units.*
With reference to the amendment of art.4 h) and connected recital 4 "support *Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, and special intervention units, including by providing operational, technical and financial support;"*	As refers to the envisaged support that Europol should provide to Member State special intervention Units, we believe that it should be first made clear, within the text proposal, the exact procedures to be followed as well as the bodies that are supposed to request and certify the crisis as indicated in recital 4 of the proposal.
With reference to the amendment of art.4 m) *"support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the coordination of law enforcement authorities' response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;"*	Italy believes that the wording of the text is not very clear. It seems to give to Europol (though in cooperation with Member States) the possibility to coordinate (Member State) Law enforcement authorities response and the taking down of terrorist content online. On the contrary the main role of Europol should be, in our opinion, limited to supporting member States and not coordinating them. Furthermore we believe that it is premature to take decisions on such important topics also in consideration of the fact that the "Digital service act" is still in the in the work and TCO Regulation does not provide Europol such role as competent authority.
With reference to the amendment of art.4 r) and connected recital 8	

(r) "enter data into the Schengen Information System, in accordance with Regulation (EU) 2018/1862 of the European Parliament and of the Council, following consultation with the Member States in accordance with Article 7 of this Regulation, and under authorisation by the Europol Executive Director, on the suspected involvement of a third country national in an offence in respect of which Europol is competent and of which it is aware on the basis of information received from third countries or international organisations within the meaning of Article 17(1)(b);*	Italy recalls the observations made with reference to recital 8. We can not support the text,
With reference to the amendment of art.4 new paragraph 4b and connected recital 12: *"Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council* that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security"*	Italy, recalling what said with reference to recital 12, believes that is of utmost importance that such screening role of Europol with regard to foreign direct investments should be carried out through the ENUs. *Therefore* we propose to rephrase recital 12 as follows: Europol, through its national units, shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council* that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security
With reference to the new proposed version of Article 6 and connected recital 14: *"In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall*	We would like to have explanations on the need to replace the actual Art 6 (under current Europol Regulation) with the proposed version.

request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation."	We are not in favour of the reviewed text proposed as the actual Europol regulation has already proved to be sufficient and adequate. Furthermore, according to the connected recital 14, Europol would have the possibility to request the competent national authorities to initiate or conduct a criminal investigation even where there is not a cross border nature of the crime. We believe that no modification should involve art. 6 of the Europol actual Regulation.
With reference to the new proposed version of Article 7: *Member States shall ensure that their financial intelligence units established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council* are allowed to cooperate with Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and the Council**, in particular via their national unit regarding financial information and analyses, within the limits of their mandate and competence*	As already observed under our comment in relation to recital 33, Italy asks for the recital to be merged with Art 7.
***With* reference to the new article 18 3a:** *"Processing of personal data for the purpose of research and innovation as referred to in point (e) of paragraph 2 shall be performed by means of Europol's research and innovation projects with clearly defined objectives, duration and scope of the personal data processing involved, in respect of which the additional specific safeguards set out in Article 33a shall apply."*	We believe that the text here should be more specific. In particular, it should be made clear that processing personal data for such purposes is possible only if needed in order to reach the projects objectives. Therefore, we propose the following rephrasing: *"If needed in order to reach Europol's research and innovation project's* objectives, *processing of personal data for the purpose of research and innovation as referred to in point (e) of paragraph 2 shall be performed only by means of the mentioned projects with clearly defined objectives, duration and scope of the personal data processing involved, in respect of which th e additional* specific *safeguards set out in Article 33a shall apply".*

With **reference with the new Article 25 paragraph 5, replaced by the following:** *"By way of derogation from paragraph 1, the Executive Director may authorise the transfer or categories of transfers of personal data to third countries or international organisations on a case-by-case basis if the transfer is, or the related transfers are:"*	Italy would like to have explanations on this provision. If we compare this provision with the actual art 25 under the current regulation, we notice that the powers of the Executive Director now have increased including also « categories of transfers ». Why?
With **reference paragraph 8, the following sentence is deleted:** *"Where a transfer is based on paragraph 5, such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred."*	This part of the proposal is not clear to us, if the sentence « where a transfer.... » is added or deleted. It seems to us that the sentence is being added and not deleted.
With **reference to the Article 26 paragraph 2 that would be replaced by the following:** *"Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 in order to identify all national units concerned, as referred to in point (a) of paragraph 1. Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the*	Preliminarily Italy believes that any direct transmission of banking and financial data by private parties to Europol could lead to the possibility that the aforementioned European Agency gets to know this information before the national Law Enforcement Agencies do. This could create a delicate situation, also because of the fact that, to date, there is no similar obligation owed to the latter in the national legislation (except for Court orders to produce documents and measures provided for by special rules aimed at money laundering prevention). Italy considers this new version of article 26 not fully in line with Directive 1153/2019 art.11 « Each Member State shall ensure that its competent authorities are entitled to reply,

national units concerned. Europol may forward the personal data and relevant results from the processing of that data necessary for the purpose of establishing jurisdiction in accordance with Article 25 to contact points and authorities concerned as referred to in points (b) and (c) of paragraph 1. Once Europol has identified and forwarded the relevant personal data to all the respective national units concerned, ***or*** *it is not possible to identify further national units concerned, it shall erase the data, unless a national unit, contact point or authority concerned resubmits the personal data to Europol in accordance with Article 19(1) within four months after the transfer takes place."*	through the Europol national unit or, if allowed by that Member State, by direct contacts with Europol, to duly justified requests related to bank account information made by Europol on a case-by-case basis within the limits of its responsibilities and for the performance of its tasks. Article 7(6) and (7) of Regulation (EU) 2016/794 apply » and with the Recital 33 of the Proposal." Moreover, in our opinion both conditions should apply simultaneously in order to allow Europol to receive data from Private parties: — having identified and forwarded the relevant personal data — it is not possible to identify further national units concerned. Therefore we suggest to replace the word « or » with « and ». In general, Italy believes that any information exchange should comply with the current regulatory framework and fully involve the Europol National Units. Furthermore Italy believes that the first part of the article should be reworded according to the following version: "Europol may only receive personal data directly from private parties, based on third countries, in compliance with national legal framework ..."
Regarding **the new paragraphs 6a and 6b of art. 26:** "6a. *Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned.* *Irrespective of their jurisdiction over the specific crime in*	We need explanations as regards the concrete possibilities to verify that the condition is fulfilled. Will Europol somehow have to certify that the condition underlying its request is met? In general, to Italy the wording appears to us a bit confusing and redundant. In fact, MS can always ensure their competent authorities can lawfully process the request when this is in done in accordance with their national law (which automatically implies lawfully). So why foreseeing this obligation explicitly?

relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives".	

With regard to the new art. 26a	We want to raise the same objection of the new version of article 26
With reference to the new version of Article 57, paragraph 4 proposed: *"..Europol may benefit from Union funding in the form of contribution agreements or grant agreements in accordance with its financial rules referred to in Article 61 and with the provisions of the relevant instruments supporting the policies of the Union. Contributions may be received from countries with whom Europol or the Union has an agreement providing for financial contributions to Europol within the scope of Europol's objectives and tasks. The amount of the contribution shall be determined in the respective agreement."*	Italy believes the Europol cannot have a more specific relationship of financial dependence created with one State on the pretext that it would contribute more to its budget than others would. This situation would be harmful both for Member States but also for the credibly of the Agency, of the European institutions and the confidence that Member States place in it. Therefore, we cannot support the text proposed.

LITHUANIA

In accordance to the last LEWP meeting on 11/01/2021, please find enclosed the Lithuanian contribution/comments on the first two thematic blocks (cooperation with private parties and research and innovation) under the agenda item 5. Revision of Europol Regulation, as requested.

Lithuanian comments:

1. **Direct exchange of personal data between Europol and private parties.**

We do consider that current restrictions limits Europol‘s capacity to support some MS investigations. The Agency cannot proactively request data from private parties, moreover, there are national legal requirements to obtain such data. Those requirements can’t be fulfilled by Europol at the moment (National Court's, Prosecutor‘s, or other's decision/approval is needed).

Essentially, we agree to allow Europol to exchange personal data directly with private parties, however, further profound and detailed discussion is needed. It would be not sufficient to amend Europol's Regulation only. Authorization of the prosecutor or even judge according to Lithuania's legislation is required to obtain certain data from private parties. There is no possibility to obtain such data upon request of Europol according to national law. Moreover, multiple laws must be changed if such option for Europol will be approved, including changing details of procedures to obtain the data (e.g. rights, duties, responsibility, order of sanctions and submission, remuneration for private parties for information provided, etc.). Amendment of Europol Regulation would be not sufficient to change national law. Thus, the highest EU legal act should be in place. Also, worth to mention, that some of the data from private parties Lithuanian authorities can obtain through police databases that linked with those companies. Thus, the administrative bargain is less for private sector. From our point of view, the discussions could take place on possibility to give Europol access to mentioned police databases/systems in order to prepare/organize connection between Europol's information system and particular module of national police. Europol's opinion as well as practical examples would be welcome on how such way of getting information from private parties would work if the Agency would get a possibility.

In addition, such an intervention needs to include clear data protection safeguards and mechanisms to fully involve Member States in the exchanges between Europol and private parties

Europol should be able to request and obtain data directly from private parties, however, it should be discussed in detail what will give such legal power and especially requesting private sector in third countries which does not recognize EU law.

Furthermore, the competence of the national authorities should be considered.

Recital of the Proposal (Point 31) contains an explanation which may be applied in the cases provided for in Article 26 Para 6a and Article 26a Para 5, i. e. those cases where the jurisdiction of the Member States has not been established or in cases of multijurisdiction and the information requested is required to establish jurisdiction. However, this purpose does not follow from the wording of Article 26 Para 6a and Article 26a Para 5. On the contrary, following the wording "Irrespective of their jurisdiction", Article 26 Para 6a and Article 26a Para 5 could be applied also in cases, where jurisdiction of the particular Member State would be obvious, but a Member State would still be obliged to comply with Europol's request regardless of its jurisdiction.

2. Considering the explanation of the definition of competent authorities in Article 2 (a) of Regulation (EU) 2016/794, the term "competent authorities" used in Articles 26 Para 6a and 26a Para 5 of the Proposal could cover not only law enforcement but also judicial authorities of the Member States. Therefore, in accordance with the wording, these judicial authorities should be obliged to execute or take measures for execution of the Europol's requests. The judicial authorities of the Member State (prosecutors' offices, courts) cooperate with judicial authorities of the other Member State applying the EU mutual recognition instruments, other procedures of international judicial cooperation in criminal matters, including Eurojust, and special cooperation with the European Public Prosecutor's Office. This cooperation is strictly regulated particulary implementing the basic principle of cooperation - ensuring the eligibility and the protection of human rights, which is guaranteed by judicial supervision. Thus, the other means of communication for judicial authorities, especially direct ones with non-judicial institutions (agencies) of the EU, without judicial supervision, can not be provided.

In Articles 26 Para 6a and 26a Para 5 the Europol’s powers and means to request and receive personal data from private subjects are not separated depending the nature and content of this data. As an example that for the production of different kind of data different measures of legal protection should be applied could be the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters 2018/0108 (COD). In this Proposal 2018/0108 (COD) depending on the data and its nature requested by the European Production Order or European Preservation Order different levels of judicial validation shall be applied (Article 4 Para 1 and 2 of the Proposal 2018/0108 (COD).

It should be admitted that in crisis situations the specific measures of communication could be considered. However in such case these measures and the grounds for their application should be clearly defined. Nevertheless, Para 5 of new Article 26a, which is dedicated to the exchanges of personal data with private parties in crisis situations, establishes the same procedure as new Para 6a of Article 26, dedicated for all other cases.

Therefore, according to the provisions of Article 26 Para 6a and Article 26a Para 5 it is not clear in which cases, for what kind and content of data from private parties Europol could request, it is not clear on which national competent authorities and what kind of obligations would be imposed, as it is not clear wether these obligations wouldn't be contrary to the principles of judicial cooperation in criminal matters, to the rights of Member States to execute their jurisdiction, it is not clear how the judicial supervision of these requests in terms of protection the human rights ant personal data would be ensured.

2. **Research and Innovation**

We do see a need for Europol to step up its support to Member States on research and Innovation. Capacity of the separate MS in this area is limited due to limited human and financial resources. Furthermore, countries invest in the similar research and innovation so duplicates their efforts. Europol might coordinate those efforts at some point to avoid such duplicity, also could allocate resources for sophisticated solutions and products that would allow strengthen fight with serious and organized criminality. Although, the cutting-edge products and actual needs of MS must be identified initially. Existing tools at Europol should be exploited efficiently. Consideration of further cooperation with existing innovation labs must be developed.

SPAIN

Spain.- Follow-up comments to the last LEWP meeting (11/01/2021)

REVISION OF THE EUROPOL REGULATION

- Regarding Europol's cooperation with private parties, cooperation with third countries or the processing of large data, Spain's position on this matter is favorable.

- Relating to strengthen Europol's cooperation with the European Public Prosecutor's Office, Spain certainly believes that Europol's cooperation with the European Public Prosecutor's Office is clearly necessary.

- Concerning the entry of alerts by Europol, we in Spain, are currently studying this issue thoroughly. However, several legal pitfalls are anticipated to comply with the national and EU legislation. For this reason, Spain supports to explore an alternative and more practical solution which allows to incorporate and make available to MS the information provided by third countries, such as the option of inserting such data in the field of interoperability.

- Pertaining to clarify the role of Europol in the request for the initiation of an investigation into offences affecting the common interests of the Union, our position of this refers to the article 6 Europol Regulation (REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016). In this sense, it is considered that this Article provides sufficient legal cover to request the initiation of investigations and therefore it is not considered necessary to amend the regulation to this effect.

2. COMMENTS RECEIVED AFTER MEETING ON 25 JANUARY 2021 (BLOCKS 1 AND 3)

AUSTRIA

Please find below Austrian follow-up comments to the LEWP meeting on 25.01.2021.

Regarding the participation of Europol in the meetings of the LEWP:

Austria would strongly prefer if Europol attends the (virtual) meetings for some technical issues.

Europol can support delegations with its know how directly in the discussions if needed, for example during the discussions at the last Meeting of the LEWP regarding Article 4, para 4b"the screening of specific cases of foreign direct investments into the Union…" or Article 26, para 6b "Europols infrastructure may be used for exchanges between the competent authorities of Member States and private parties……."

Article 4(1), point (u):

We are of the opinion that the wordings „crisis situation" and "recent real world event" should be further defined in this article.

Article 4, para 4b:

We wonder if this task is within the mandate of Europol. It seems that here Europol's mandate is interpreted to extensively.

Article 26, para 6b:

We strongly support this paragraph. The possibility to use Europol's infrastructure for the exchanges between Member States and private parties will be a great added value from our point of view.

Especially when a common approach seems to be more useful and effective than the implementation of different solutions in every Member State this will be very helpful.

BELGIUM

Written comments by Belgium
concerning the proposed revision of the Europol Regulation (EU) 2016/794

Our main current concerns in relation to block 1 on private parties are the following:

- About the nature of the private parties Europol would be cooperating with we want to provide you with the following comments.
    - We appreciate the explanations provided by the Commission concerning the cooperation with financial institutions and their views on the duplication of efforts and other related issues when FIU-obliged entities would report directly to Europol. The Commission's intentions in this regard are reassuring. We do share some of the concerns as, for example, raised by France and would not be opposed to including the French text proposals in the relevant articles.
    - Based on a similar concern we are wondering whether Europol's interactions would not interfere with the current systems concerning the processing of information such as Passenger Name Records and Advanced Passenger Information data. Maybe this matter deserves to be explained in a recital.
    - Also, we welcome and support the French text proposal on the role of the Management Board of Europol with regard to private parties, namely the new articles 26(2a) and 26(9).
- While we agree that information exchange with private parties should be strengthened, giving information *to* private parties (art. 26(5)) should remain the exception. Therefore, we are not in favor of the reversed phrasing that "Europol **may** transmit or transfer personal data to private parties (…) where it is strictly necessary" under certain conditions. We believe it important to keep the current phrasing that "Europol **may not** transfer personal data to private parties **except** (…)".
- Furthermore, we would welcome a streamlined use of "transmission" and "transfer" throughout the text, namely in article 26(5), taking into account the terminology used in Regulation (EU) 2018/1725.

- In relation to the possibility of Europol to proactively request a MS to contact a private party, we have to further verify the proposal in light of our national legislation. However, we do already note several concerns with the current phrasing (art. 26(6a)).
    - Firstly, we are pleased to hear the Commission's agreement on the fact that Member States have the possibility to refuse and that private parties are not obliged to provide the requested information. Thus, it is necessary to explicitly include the possibility of the MS to refuse. Also, the text should indicate that private parties are not obliged to answer. Those two elements remain currently ambiguous. These changes would bring the text more in line with the Council Conclusions of 2 December 2019. Furthermore, a reference to private parties' own data protection obligations (e.g. art. 6(1)(e) GDPR) should be considered.
    - Secondly, we are satisfied with the proposed way of working; namely that the ENU is the intermediate actor in this process. For clarity reasons, we believe it necessary to make sure that this process is also explicitly subjected to same reasoning of art. 26(2) that the concerned MS has/have to be informed and has/have to resubmit the information to Europol via their national units.
- As regards Europol's possibilities in relation to TCO in crisis situations and namely the situation of art. 26a(4), we believe the authorization of the Executive Director requires further specification of the applicable conditions. We believe inspiration can be found in art. 26(6).

In relation to <u>block 3 on research and innovation</u> we have to maintain our scrutiny reservation for now. Next to this, we can provide you already with the following comments:

- We consider it important that synergies have to be sought with existing networks in this domain (such as ENLETS, I-LEAD, etc.).
- We located article 13 of the Regulation 2018/1725 and presume this is what the Commission referred to when asked about the preference for not using real operational data. In relation to this article 13 of the Regulation 2018/1725, we however do not believe it is currently applicable to Europol. Are there other articles the Commission understood to be of relevance?

BULGARIA

Bulgarian contribution to the
draft Regulation amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

General comments:

Bulgaria has always supported the strengthening of Europol's mandate so that the agency can assist Member States more effectively in countering serious crime.

As a general comment on the whole text of the draft Regulation, at the videoconference on 25 January we asked for clarification between **the terms "transmission" and "transfer" of data** and the Commission provided the explanation that "transmission" is used for providing data within the EU and "transfer" for providing data to third countries. We would like a thorough analysis of the text to be made once again in order to identify whether both terms are used properly and if there are any duplications or contradictions. We also propose a **definition of both terms to be included in Art. 2 of the Regulation**, among the other definitions.

Furthermore Bulgaria agrees in principle with the proposal **Europol to be invited to participate in the next meeting of LEWP** related to the discussion on the draft Regulation. Europol should be able to take the floor only on technical issues and after being officially invited to intervene by the Presidency or the Commission.

Comments on thematic block 1 "Enabling Europol to cooperate effectively with private parties":

We consider positive the proposed text.

On Art. 4, para 1 (u) we would like **a definition of "crisis situation" to be included in Art. 2**.

On Art. 26, para 2 we propose the following wording:

"Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 for the purpose of establishing jurisdiction and in order to identify the national unit, contact point or authority concerned, referred to in paragraph 1.

Subsequently, the personal data and any relevant results from the processing of that data shall be forwarded immediately to the national unit, contact point or authority concerned and shall be deleted unless the national unit, contact point or authority concerned resubmits those personal data in accordance with Article 19(1) within four months after the transfer takes place.

Europol shall ensure by technical means that, during that period, the data in question are not accessible for processing for any other purpose.

Europol shall delete (erase[1]) the data if the identification of the jurisdiction and the national units, contact points or authorities concerned is not possible."

On Art. 26, para 4 we propose the following wording of the last sentence:

"Where the conditions set out under paragraphs 5 and 6 of Article 25 are fulfilled, Europol may transfer ***the received personal data*** *to the third country concerned."*

It should be highlighted that Europol will transfer only the personal data received and not the result of its analysis and verification of such data. Europol should not be tasked to verify personal data received from private parties as well as a question is raised how this will be done.

On Art. 26, para 5, (d)

We propose to be added that the information will be used by Europol to identify not only the national units concerned, but also the contact points and authorities concerned.

(d) the transmission or transfer of personal data is strictly necessary for Europol to inform that private party that the information received is insufficient to enable Europol to identify the national units, ***contact points or authorities*** concerned, and the following conditions are met:

[1] Consultation is needed in order the correct term to be used – delete or erase.

(i) the transmission or transfer follows a receipt of personal data directly from a private party in accordance with paragraph 2 of this Article;

(ii) the missing information, which Europol may refer to in these notifications, has a clear link with the information previously shared by that private party;

(iii) the missing information, which Europol may refer to in these notifications, is strictly limited to what is necessary for Europol to identify the national units***, contact points or authorities*** concerned.

On Art. 26, para 6a we have the same proposal:

"6a. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units***, contact points or authorities*** concerned."

On Art. 26, para 6b we have some concerns in case SIENA is meant under the term "Europol's infrastructure" which will be used for exchanges between the competent authorities of Member States and private parties. We would like to understand **how SIENA will be directly accessed by the private party** which seems to be inappropriate. We heard the explanations of the Commission that the idea is to provide a legal possibility for communication with private parties, but we prefer the text could be amended and clarified.

Information exchange between national competent authorities and private parties within the MS (on national level) is done according the national legislation. If one MS would like to receive information from private parties which are established or have a legal representative on the territory of another MS or third country the request could be send via the existing channels for law enforcement information exchange (Interpol, Europol – SIENA, liaison officers network) to the NCA of this MS or third country and they on the ground of the received request will ask the respective private party for information according their national law.

On Art. 26a except the already mentioned proposal on including a definition of "crisis situation" we would like to be sure that **all hypotheses for receiving and transferring of personal data are really covered** in these provisions. Please see also our comments on Art. 26, para 5, (d) about national units, contact points and authorities concerned as well as - on Art. 26, para 4 about the verification of personal data.

Comments on thematic block 3 "Strengthening Europol's role on research and innovation":

We support in principle the proposed texts in this thematic block.

On Art. 18, para 2e and Art. 33a we propose to be analyzed the possibility to merge both, the provisions on the procedure on setting up of research and innovation projects with the similar procedure implemented for the analytical projects. It will avoid possible duplication, as **both kind of procedures could be stipulated in Art. 18**.

On Art. 33 we would like **to raise a question about the necessity to delete this provision**, since it introduces one of the main principles for personal data protection. Does the Commission envisage to propose a new version of Art. 33?

On Art. 33a we would like to be clarified **whether Member States, third countries and external contractors will participate in the research and innovation projects** and if so, these partners should also have authorized access to the personal data.

CYPRUS

Following the 1st meeting on revising Europol Regulation, please find below Cyprus ' positions:

The Republic of Cyprus expresses its general support to the amendments of the EUROPOL Regulation. Given the changing security landscape, it is our belief that the proposed amendments, provide Europol the capabilities and tools to support Member States effectively in countering serious crime and terrorism, through strengthening the Europol's' mandate.

Following the discussions held on 26/01/2021, please note the following comments on behalf of Cyprus:

Article 26, par. 5: Although it is clear that the term transfer and transmission refer to the transfer of personal data to third countries and to the transfer of personal data within the EU, respectively, the Republic of Cyprus proposes that definitions should be added to this effect.

Article 26a: The term "crisis situations", should be clearly defined in the Regulation. Paragraph 4 of the Preamble of the proposed Regulation, specifically refers to Council Decision 2008/617, which includes a definition of crisis situations. In this regard, it should be clarified whether this definition is relevant in the case of this article as well.

We do see a need for EUROPOL to step up its support to Member States on research and innovation. In relation to discussions carried out in regards to Article 4 (4)(a), we would like clarification regarding the provision of resources to EUROPOL, for the performance of its new tasks

Lastly, Cyprus supports the participation of EUROPOL to LEWP meetings.

CZECH REPUBLIC

On the involvement of Europol during the negotiations:

CZ **agrees to** (and prefers) the participation of Europol, which should be allowed to present its positions if requested, mainly as regards technical issues.

Drafting comments on document wk 757/2020 (CZ proposals marked in **red**):

Block 1

Article 4(1)(m)

The distribution of responsibilities in draft TCO regulation should be respected, as the Europol has no power to take down terrorist content online:

"(m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including **in taking down of terrorist content online, and**, in cooperation with Member States, **the coordination of law enforcement authorities' response to cyberattacks**~~**, the taking down of terrorist content online,**~~ **and** the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;

Article 4(1)(u)

While we understand that the EU reaction to online content is still developing, we do not consider it wise to legislate on insufficiently defined area. We note that there has not yet been an evaluation of the activation of crisis protocol in November 2020. In addition, we note that recital 35, while helpfully illustrating expected support of Europol, does not really elaborate on the relevant instances. In particular, we suggest that definitions in the crisis protocol[1] be kept. In particular, relation to "**events of suspected criminal nature**" should be included.

Article 26(5

Even if we rely on the estimate of the Commission that all relevant situations are covered, at least the wording should be streamlined by deleting the word "**either**".

Article 26(3)

While this provision has not been changed, it scope is expanded considerably by expanding Art. 4(1)(m). Therefore, specification of application to referrals only appears necessary to prevent collision with other mechanisms, such as draft TCO regulation:

3. Following the transfer of personal data in accordance with point (c) of paragraph 5 of this Article, Europol may in connection therewith receive personal data directly from a private party which that private party declares it is legally allowed to transmit in accordance with the applicable law, in order to process such data for the **making of referrals of internet content** ~~performance of the task~~ set out in point (m) of Article 4(1).

1 A crisis within the meaning of this Protocol constitutes a critical incident online where:
(1) the dissemination of content is linked to or suspected as being carried out in the context of terrorism or violent extremism, stemming from an on-going or recent real-world event which depicts harm to life or physical integrity, or calling for imminent harm to life or physical integrity and where the content aims at or has the effect of seriously intimidating a population; and
(2) where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.
A strong indicator of terrorist or violent extremist context is where the content is produced by or its dissemination is attributable to listed terrorist organisations or other listed violent extremist groups. The Protocol pertains only to online content stemming from events of a suspected criminal nature.

Article 26(5)(c)

Similar to Art. 26(3), this provision should focus on referrals:

5. Europol may ~~not~~ **transmit or** transfer personal data to private parties ~~except where~~, on a case-by-case basis, where **it is** strictly necessary**,** and subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67**, in the following cases:**

…

(c) the **transmission or** transfer of personal data which are publicly available is strictly necessary for the **making of referrals of internet content** ~~performance of the task~~ set out in point (m) of Article 4(1) and the following conditions are met:

…

Article 26(6a)

In the light of the 2019 Council Conclusions, the replies to requests should be voluntary both for Member State's authorities and private parties (because the private party can find legal basis under GDPR or national rules). It should be also clear what the second subparagraph requires (legal basis for processing on the part of competent authority is not the same as duty of private party to reply established in domestic law). We believe that obligatory cooperation of private parties should be left to consideration of domestic legislator. Therefore we suggest following changes:

6a. The Member States may reply to requests by Europol ~~may request Member States~~, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned.

Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives. The cooperation of private parties is voluntary, unless otherwise provided for by Member State law.

Article 26a

CZ maintains its scrutiny reservation.

Article 26a(5)

In the light of the 2019 Council Conclusions, the replies to requests should be voluntary both for Member State's authorities and private parties (because the private party can find legal basis under GDPR or national rules). It should be also clear what the second subparagraph requires (legal basis for processing on the part of competent authority is not the same as duty of private party to reply established in domestic law). We believe that obligatory cooperation of private parties should be left to consideration of domestic legislator. Therefore we suggest following changes:

5. The Member States may reply to requests by Europol ~~may request Member States~~, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned. Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives. The cooperation of private parties is voluntary, unless otherwise provided for by Member State law.

Block 3

Article 4(4a)

Neither this Article nor recital 11 suggest a solution for ensuring sufficient funding for research and innovation by Europol. Therefore, it is uncertain that the effects of new obligation to assist the Commission will have positive results.

Article 18(2)(e)

We understand that the Commission believes that all uses of operational data have been covered, but in light of data protection challenges we wish this provision to be future-proof. Therefore we suggest opening this purpose to all research activities covered by the Europol Regulation:

(e) research and innovation regarding matters covered by this Regulation, in particular for the development, training, testing and validation of algorithms for the development of tools;

Article 33a(1)

We believe that in (c), collaboration with Member States personnel should be promoted, subject to security protections:

(c) any personal data to be processed in the context of the project shall be temporarily copied to a separate, isolated and protected data processing environment within Europol for the sole purpose of carrying out that project and only specifically authorised staff of Europol and, subject to technical security measures, specifically authorised staff of Member States' competent authorities, shall have access to that data;

As regards (g), we believe that logs should be usable also for data protection enforcement and should be kept for 3 years, given that the tools are presumed to be deployed for a long term and specific concerns may arise in time:

(g) the logs of the processing of personal data in the context of the project shall be kept for the duration of the project and ~~1 year~~ 2 (3) years after the project is concluded, solely for the purpose of and only as long as necessary for verifying the accuracy of the outcome of the data processing and auditing compliance with data protection rules.

(end of file)

ESTONIA

Firstly, Estonia wants to thank the Portuguese Presidency for the constructive session regarding the Europol regulation amendments.

Estonia presents the following comments:

Data and private sector

1) **Article 4(1)(m) -** We welcome the inclusion of the provision, particularly in light of the need to coordinate MS actions under the TCO regulation.

2) **Article 4(1)(u)** – as discussed, the term 'crisis situation' is not defined in EU legal landscape and every MS understands this differently. Crisis situation depends on a variety of things and may be seen differently by the MSs. Therefore we ask, whether this term is needed here. Firstly, it doesn't matter if there is 1 victim or more, or if there was just an attempt. Disinformation spreads nevertheless. Secondly, Crisis Protocol aims to provide a "rapid response to contain the viral spread of terrorist and violent extremist content online"[1]. Therefore crisis refers more to the scope of information than a specific event.

Secondly, there is an explanation "depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and aims at or has the effect of seriously intimidating a population". In our opinion, each real life event based on which a certain online content campaign may be launched, qualifies into that description. **In short: to avoid confusion and unclarity, our proposal is to discuss the potential removal of this term.** In this regard, Estonia sees, that (u) could be further capped as following:

"(u) support Member States' actions in preventing the dissemination of online content related to terrorism or violent extremism in ~~crisis~~ situations, which stems from an ongoing or recent real-world event~~, depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and aims at or has the effect of seriously intimidating a population,~~ and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers."

As some MSs referred, there also lacks a description, what are Europol's competences in such situations. So we propose adding a clarification as a second section or creating a reference, if possible. As Commission said, this could refer informing the service providers by Europol. So the second section could set the criteria:

"In order to prevent dissemination of online content related to terrorism or violent extremism, Europol…" – and the competences are discussed among MS and the Commission and **actual capabilities that Europol possesses** + which are referred to in Crisis Protocol.

We would like to stress, that this is just a food for thought and in our view Europol's mandate would remain the same – Europol would take action if crisis protocol is triggered. Also we are not against, but rise this question since MSs expressed their concerns.

---

1 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf

3) **"Transmission", "transfer" and also "forward"**. GDPR has not defined either of the terms, however in practice, as Commission explained, it is differentiated. If there is a clear distinction, this should to be clarified. If reading the proposal, "forward" is used only towards Europol => Member State. For example art. 26 para 6(e) uses only transfer and in English this causes confusion. Estonia proposes the following solution:

a) Set the terms under article 2 with clear distinctions which allows to use the terms logically throughout the regulation.

4) **Article 26(2)** – we see a new term of "establishing jurisdiction" and would like to confirm the meaning of the term. Europol may use private party data to identify the national units. If identified, it may forward the results immediately to the national units concerned in order to "establish the jurisdiction" – **in other words to establish in which MS the investigative initiative should be started?**

5) **Article 26(5) and article 26a(3)** – Estonia agrees with Belgium, that previous wording and logic was better and more restricting. In either way, criteria has to be fulfilled. Comment was made on article 26 para 5, but the latter article has exactly the same point and structure.

"5. Europol may **not** transmit or transfer personal data to private parties ~~on a case-by-case basis,~~ **except** where, **on a case-by-case basis**, it is strictly necessary, and subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67, in the following cases:"

6) **Article 26(6)(e)** – we agree with Germany, that if there are already references that limit the scope of transfers, specific reference under this paragraph "shall not be systematic, massive or structural", is not necessary.

7) **Article 26a** – only if article 4(1)(u) is changed, this article should be adjusted.

Research & innovation

1) **Article 4(4a)** – we just want to stress here the importance of the Swedish reasoning and conclude, that in our opinion this paragraph needs further discussion.

2) **Article 4(4b)** – the screening of foreign direct investments is indeed part of European Union strategic autonomy and the aim of this paragraph is noble and necessary. However, such regulations are not in place in all MS's, also currently not in Estonia (currently being drafted and discussed). Our question is: How Europol would conduct the support of these screenings?

3) **Article 33a(1)(g)** – concern is shared regarding the 1 year retention limit of logs. However, Europol should be granted an opinion here, whether they see risks and if, then which ones. However, we would like to discuss the additional sentence as an alternative.

"(g) the logs of the processing of personal data in the context of the project shall be kept for the duration of the project and 1 year after the project is concluded, solely for the purpose of and only as long as necessary for verifying the accuracy of the outcome of the data processing. **Europol, on a case by case basis, may request the extension of the logs up to 1 year within one month prior to ending of the period from the European Data Protection Supervisor**".

This would allow, on exceptional cases we currently can't predict, an option to prolong the retention of logs. Each time EDPS assesses the request and reasoning. Therefore, we find it unnecessary to add the criteria, which such cases may be – a project delay, after-analysis delay, a mistake has occurred etc.

FINLAND

With regard to your question about Europol attending future meetings we are happy to approve of this.

General comments and questions on block 3. Research and innovation

Finland still has a scrutiny reservation.

We would like to ask the Commission for some clarifications and we also propose some text changes below.

In the light of Regulation (EU) 2018/1275, it is evident that proposed Article 33a would be necessary if the proposed new task in Article 18(2)(e) is included in the Europol Regulation and entails the processing of real personal data. This is even more so if, as the Commission has explained, operational data were used for the purposes of research.

1. It seems that the provisions other than those in Chapter IX of Regulation (EU) 2018/1275 would apply to the research activities. The Law Enforcement Directive, which has been used as a model for Chapter IX, is clearer on this question (LED, Art. 9(2)). It should be noted that Regulation (EU) 2018/1275 imposes strict limitations for the use of operational data. (As a main rule, Chapter IX, Article 72, of the Regulation prohibits the use of operational data for purposes other than for the performance of a task carried out by Union bodies, offices and agencies when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU and that it is based on Union law.) Research purposes seem to be allowed, however, although the exact relationship of Article 72 with those on further processing for other purposes is not entirely clear as regards EU agencies, considering that the operational personal data are forwarded by the Member States' authorities. We would appreciate some clarity from the Commission on this matter.

2. Also, as the general data protection framework does not use the concept of "innovation activities", it raises considerable questions. First, the concept of innovation may be problematic in the context of the processing of operational personal data, which are sensitive in nature and are subject to strict limitations even in the Law Enforcement Directive. There may also be issues of fundamental rights, considering the constitutional traditions of Member States. From that point of view, and to ensure consistency with the requirement of purpose limitation in the data protection legislation, it could be safest to choose another concept, such as development of "new technologies" which is a concept used in data protection legislation. It would also be important to examine the proposed Article jointly with the other proposed changes to the provisions on the processing of personal data. We would like to hear the Commission's thoughts on this matter.

3. It is not clear whether the Commission's proposal means that the processing of special categories of operational personal data is covered by Article 33a. Article 76 in principle prevents their use for purposes other than operational purposes. We would welcome a clarification by the Commission, and can later send a text proposal if special categories of operational personal data are also meant to be included.

4. We would also like to know if Europol can use other legal data for its research and innovation activities?

Text proposal for Article 4, paragraph (1)(t)

(t) proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States, and implement its research and innovation activities regarding matters covered by this Regulation, including **in** the development, training, testing and validation of algorithms for the development of tools.

Text proposal for Article 18(2)(e)

(e) research and innovation ~~**regarding matters covered by this Regulation**~~ for the development, training, testing and validation of algorithms for the development of tools **to support activities which fall within the scope of Chapter 5 of Title V of Part Three TFEU, covered by this Regulation**;

Reasons:

This modification in our view would help to avoid possible conflicts with the requirements set out in TFEU and Regulation (EU) 2018/1275, including particularly the purposes of processing of personal data and the rights of the data subject. In particular, in the light of Articles 71 and 72 of that Regulation, it would be advisable to have reference to activities which fall within the scope of Chapter 5 of Title V of Part Three TFEU.

Text proposal for Article 33a:

(a) any project shall be subject to prior authorisation by the Executive Director, based on a description of the envisaged processing activity setting out the necessity to process personal data, such as for exploring and testing innovative **new technological** solutions and ensuring accuracy of the project results, a description of the personal data to be processed, a description of the retention period and conditions for access to the personal data, a data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome, and the measures envisaged to address those risks;

Reasons:

See our explanation in question 2. for adding the words “new technological”.

(d) ~~**any**~~ **no** personal data processed in the context of the project shall ~~**not**~~ be transmitted, transferred or otherwise accessed by other parties;

(e) ~~**any**~~ **no** processing of personal data in the context of the project shall ~~**not**~~ lead to measures or decisions affecting the data subjects;

FRANCE

NOTE DE COMMENTAIRES DES AUTORITÉS FRANÇAISES

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leur commentaires écrits suite à la réunion de groupe LEWP du 25 janvier 2021, consacrée à l'examen des dispositions relatives à l'échange de données avec les parties privées et au rôle de l'agence en matière de recherche et d'innovation.

S'agissant de la présence d'Europol lors des réunions, les autorités françaises estiment pertinent de permettre à l'agence Europol d'assister à une séquence spécifique lui permettant de répondre aux questions techniques posées par les États membres.

S'agissant de l'examen du bloc 1 :

Les autorités françaises portent à la connaissance de la Présidence les remarques suivantes :

Considérant 25: **To support Member States in cooperating with private parties providing cross-border services where those private parties hold information relevant for preventing and combatting crime, Europol should be able to receive, and in specific circumstances, exchange personal data with private parties.**	**Les autorités françaises notent que le considérant 25 ne mentionne que le soutien d'Europol aux États membres pour coopérer avec les** parties privées prestataires de services transfrontaliers. **Les articles modifiés figurant dans la révision du Règlement vont cependant bien au-delà de cet objectif, soulevant un problème de cohérence entre les objectifs et la proposition.** **Aussi les autorités françaises s'interrogent sur la possibilité de mieux inscrire cet objectif dans les articles liés à l'échange d'information entre Europol et les parties privées (articles 26 et 26a).**
Considérant 31: **Member States, third countries, international organisation, including the International Criminal Police Organisation (Interpol), or private parties may share multi-jurisdictional data sets or data sets that cannot be attributed to one or several specific jurisdictions with Europol, where those data sets contain links to personal data held by private parties. Where it is necessary to obtain additional information from such private parties to identify all relevant Member States concerned, Europol should be able to ask Member States, via their national units, to request private parties which are established or have a legal representative in their territory to share personal data with Europol in accordance with those Member States' applicable laws. In many cases, these Member States may not be able to establish a link to their jurisdiction other than the fact that the private party holding the relevant data is established under their jurisdiction. Irrespective of their jurisdiction with regard the specific criminal activity subject to the**	La notion d'autorité compétente telle que définie à l'article 2 du Règlement Europol et évoquée au considérant 31 (partie en rouge) de la présente proposition de révision entraine des interrogations sur les autorités effectivement concernées. Les autorités françaises aimeraient obtenir des clarifications sur la nature des autorités compétentes nationales qui devraient pouvoir obtenir des données personnelles des parties privées pour le compte d'Europol. En effet, les échanges d'information entre Europol et certaines autorités publiques font l'objet de dispositions distinctes, notamment concernant les cellules de renseignement financier, celles énoncées par la Directive 2019/1153 fixant les règles facilitant l'utilisation d'informations financières aux fins de la prévention ou de la détection de certaines infractions pénales (dont la transposition doit intervenir au plus tard le 1er aout 2021). Les autorités françaises marquent leur attachement à ce que ces cadres existants soient respectés.

request, Member States should therefore ensure that their competent national authorities can obtain personal data from private parties for the purpose of supplying Europol with the information necessary for it to fulfil its objectives, in full compliance with procedural guarantees under their national laws.	
Considérant 33: Any cooperation of Europol with private parties should neither duplicate nor interfere with the activities of the Financial Intelligence Units ('FIUs'), and should only concern information that is not already to be provided to FIUs in accordance with Directive 2015/849 of the European Parliament and of the Council59. Europol should continue to cooperate with FIUs in particular via the national units.	Les autorités françaises saluent la proposition de la Commission qui prend en compte, dans ce considérant, des risques pesant sur l'articulation efficace avec les cadres nationaux LBC/FT – et par voie de conséquence sur les dispositifs relatifs aux cellules de renseignement financier – en cas d'ouverture sans réserve des échanges entre Europol et les parties privées et notent qu'aucun des articles de la proposition ne reprend les dispositions prévues au considérant 33. Néanmoins, en l'état, sont identifiés les risques suivants : - Duplication du système LBC/FT (risque de double traitement par les CRF et les polices) ; - Complexification des relations des parties privées avec les différentes autorités publiques (qui pourrait entraîner une baisse du volume et de la qualité des informations transmises par les parties privées) ; - Non-conformité aux normes internationales (les normes du GAFI – plus particulièrement la recommandation 29 – qui instituent les CRF comme centre nationaux pour la réception et l'analyse des déclarations de soupçons). Les autorités françaises soutiennent donc une modification des articles relatifs aux échanges de données personnelles entre Europol et les parties privées (articles 26 et 26 a du Règlement Europol (articles 1(12) et 1(13) de la proposition)) pour intégrer les dispositions prévues au considérant 33 : les informations transmises par les parties privées ne concerneront que des informations qui ne doivent pas être déjà transmises aux CRF selon

	la Directive LBC/FT.
Considérant 35: **Terrorist attacks trigger the large scale dissemination of terrorist content via online platforms depicting harm to life or physical integrity, or calling for imminent harm to life or physical integrity. To ensure that Member States can effectively prevent the dissemination of such content in the context of such crisis situations stemming from ongoing or recent real-world events, Europol should be able to exchange personal data with private parties, including hashes, IP addresses or URLs related to such content, necessary in order to support Member States in preventing the dissemination of such content, in particular where this content aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.**	Les autorités françaises soulignent la nécessité de clairement définir la notion de **« situation de crise ».** Le passage en situation de crise pourrait être décidé ad-hoc après concertation des États membres (exemple : attentats sur le territoire européen concernant plusieurs États membres).

Article 1(4) *Article 7 :* **"8. Member States shall ensure that their financial intelligence units established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council* are allowed to cooperate with Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and the Council**, in particular via their national unit regarding financial information and analyses, within the limits of their mandate and competence.** *** Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of**	**Les autorités françaises suggèrent de modifier à l'article 7 paragraphe 8 la phrase qui indique que les CRF sont autorisées à coopérer avec Europol par la phrase suivante : « les CRF sont habilitées à donner suite aux demandes dûment justifiées présentées par Europol ». Cela permettrait de mieux retranscrire la Directive (UE) 2019/1153 dont est issue cette modification.** **Soit la proposition de rédaction suivante :** ***8. Member States shall ensure that their financial intelligence units established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council* are entitled to reply to duly justified requests made by Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and the Council**, in particular via their national unit regarding financial information and analyses, within the limits of their mandate and competence.***

the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73). **** Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ L 186, 11.7.2019, p. 122).”**	
Article 1(2)(a)(iii) « support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the coordination of law enforcement authorities' response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions ».	Dans la poursuite des travaux sur l'outil PERCI d'Europol et en prévision du règlement sur les contenus terroristes en ligne, les autorités françaises soutiennent la proposition d'article. Dans la lignée du document de programmation 2022-2024 actuellement discuté au sein de l'agence, les autorités françaises estiment particulièrement nécessaire de rappeler, dans le cadre des discussions sur ce bloc, l'importance de délivrer le projet PERCI d'ici à fin 2022.
Article 1(2)(a)(iv) « support Member States' actions in preventing the dissemination of online content related to terrorism or violent extremism in crisis situations, which stems from an ongoing or recent real- world event, depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers ».	Les autorités françaises estiment pertinent que cette définition de la situation de crise soit inscrite dans l'article dévolu aux définitions.

Article 1(12)	**Comme indiqué pour le considérant 33, une modification de l'article 26 apparait opportune pour intégrer les dispositions prévues au considérant 33 : *« les informations transmises par les parties privées ne concerneront que des informations qui ne doivent pas être déjà transmises aux cellules de renseignements selon la Directive (UE) 2015/849 ».***
Article 1(12)(a) " Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 in order to identify all national units concerned, as referred to in point (a) of paragraph 1. Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the national units concerned. Europol may forward the personal data and relevant results from the processing of that data necessary for the purpose of establishing jurisdiction in accordance with Article 25 to contact points and authorities concerned as referred to in points (b) and (c) of paragraph 1. Once Europol has identified and forwarded the relevant personal data to all the respective national units concerned, or it is not possible to identify further national units concerned, it shall erase the data, unless a national unit, contact point or authority concerned resubmits the personal data to Europol in accordance with Article 19(1) within four months after the transfer takes place."	Les autorités françaises saluent cette proposition équilibrée de la Commission. Toutefois, elles rappellent que la coopération entre Europol et les parties privées doit être transparente envers les États membres et proposent à cet effet deux nouvelles dispositions (*cf. fin de document*).
Article 1 (13) : ***Article 26a*** 1. Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 to prevent the dissemination of online content related to terrorism or violent extremism in crisis situations as set out in point (u) of Article 4(1). 2. If Europol receives personal data from a private	Comme indiqué pour le considérant 33, une modification de l'article 26 apparait opportune pour intégrer les dispositions prévues au considérant 33 : *« les informations transmises par les parties privées ne concerneront que des informations qui ne doivent pas être déjà transmises aux cellules de renseignement*

party in a third country, Europol may forward those data only to a Member State, or to a third country concerned with which an agreement on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 TFEU has been concluded or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation. Where the conditions set out under paragraphs 5 and 6 of Article 25 are fulfilled, Europol may transfer the result of its analysis and verification of such data with the third country concerned. 3. Europol may transmit or transfer personal data to private parties, on a case-by-case basis, subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67, where the transmission or transfer of such data is strictly necessary for preventing the dissemination of online content related to terrorism or violent extremism as set out in point (u) of Article 4(1), and no fundamental rights and freedoms of the data subjects concerned override the public interest necessitating the transmission or transfer in the case at hand. 4. If the private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, the transfer shall be authorised by the Executive Director. 5. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol for preventing the dissemination of online content related to terrorism or violent extremism as set out in point (u) of Article 4(1). Irrespective of their jurisdiction with regard to the dissemination of the content in relation to which Europol requests the personal data, Member States shall ensure that the competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives. 6. Europol shall ensure that detailed records of all transfers of personal data and the grounds for such transfers are recorded in accordance with this Regulation and communicated upon request to the EDPS pursuant to Article 40.	*financier selon la Directive (UE) 2015/849 ».* Par ailleurs, les autorités françaises réitèrent leur commentaire précédent -Article 1(2) (a) (iv)- sur la définition de la situation de crise.

7. If the personal data received or to be transferred affect the interests of a Member State, Europol shall immediately inform the national unit of the Member State concerned."	

Les autorités françaises proposent en complément des articles additionnels :

- Pour mémoire les conclusions du ***Conseil sur la coopération entre Europol et les parties privées du 3 décembre 2019*** soulignent *« un renforcement du rôle du Conseil d'administration d'Europol »* dans la relation entre l'agence et les parties privées. Ainsi, afin de garantir la totale transparence de l'activité d'Europol avec les parties privées et renforcer le rôle des États membres, les autorités françaises proposent un mécanisme pérenne permettant aux États membres de prendre connaissance et de valider tous les protocoles d'entente (Memorandum of understanding - MoU) que l'agence a signé avec les partenaires privées.

- Proposition d'un article 7(12) : informations inchangées par Europol avec les États tiers et les parties privées :

  «Europol rédige un rapport annuel portant sur la nature et le volume des données personnelles fournies à Europol par les États tiers et les parties privées sur la base des critères d'évaluation quantitatifs et qualitatifs fixés par le conseil d'administration. Ce rapport annuel est transmis au Parlement européen, au Conseil, à la Commission et aux parlements nationaux».

- **Proposition d'article 26 paragraphe 9 échange de données à caractère personnel avec les parties privées (Nouveau) :**

  « Sous l'égide et avec l'accord du Conseil d'administration, Europol peut conclure des protocoles d'entente avec les parties privées. Ces protocoles n'autorisent pas l'échange de données à caractère personnel et ne lient ni l'Union ni ses États membres.

  Europol communique systématiquement aux États membres l'ensemble des protocoles d'ententes conclus par l'agence avec les parties privées, pour information et validation par le Conseil d'administration ».

- **Article 11 (r) Fonctions du Conseil d'administration (Amendement) :**

  r) Autorise la conclusion d'arrangements de travail, d'arrangements administratifs et ***de protocoles d'entente avec les parties privées*** *conformément à l'article 23, paragraphe 4, à l'article 25, paragraphe 1 et à* ***l'article 26 paragraphe 9 respectivement.***

- Également, dans la continuité de ces conclusions sur la relation entre Europol et les parties privées, les autorités françaises proposent l'article suivant :

  Article 26 paragraphe 2.bis : Échanges de données à caractère personnel avec les parties privées (Nouveau) :

« […] Europol peut recevoir et traiter des données à caractère personnel transmises directement par les parties privées conformément au paragraphe 2, et avec l'accord du Conseil d'administration. Cet accord prend la forme d'une liste de parties privées proposée par le directeur exécutif et adoptée par le Conseil d'administration ».

- **Article 11 : Fonction du Conseil d'administration (Amendement)**

  Article 11 v) : « adopte la liste des parties privées autorisées à transmettre des données à Europol ».

- **Ajouts d'un paragraphe aux articles 26 et 26a** : ***« les informations transmises par les parties privées ne concerneront que des informations qui ne doivent pas être déjà transmises aux cellules de renseignement financier selon la Directive (UE) 2015/849. »***

- Les autorités françaises proposent l'ajout d'un article 26 (b) visant à demander à Europol, sur sollicitation de **deux ou plusieurs États membres enquêtant sur un même dossier**, de recueillir des données personnelles auprès d'une entreprise privée dont le principal établissement légal se trouve sur ou hors du territoire de l'Union européenne. L'agence communiquera ensuite aux Unités nationales les informations captées et pourra elle-même les intégrer dans ses bases de données.

  Exemple : dans le cadre d'une enquête commune (ECE) entre la France, la Belgique et les Pays-Pays en matière de trafic de stupéfiants, les États membres travaillant sur un même dossier pourraient exiger d'Europol – via SIENA et un modèle de demande préétabli – que l'agence les représente et puisse exiger des données personnelles détenues par un GAFAM (Google, Apple, Facebook, Amazon, Microsoft).

  Justifications : Europol – agence représentant 500 millions de citoyens – disposerait d'un poids démographique beaucoup plus important qu'un État membre seul en termes de représentation et de négociation avec des entreprises mondialisées. En outre, elle déchargerait les services opérationnels de demandes chronophages et fastidieuses.

  Proposition d'article : article 26 (b) : Demande de données personnelles avec les parties privées (Nouveau) :

  « Dans le cadre d'une enquête relevant des infractions pour lesquelles l'agence est compétente et touchant au moins deux États membres, Europol peut, à la demande d'un État membres solliciter d'une partie privée, dont le principal établissement légal est établi sur ou en dehors du territoire de l'Union européenne, la communication de données personnelles pertinentes.
  Europol peut, dans la mesure où cela est nécessaire à l'accomplissement de ses missions traiter ces données personnelles et les communiquer aux Unités nationales concernées ».

***

S'agissant de l'examen du bloc 3 :

Les autorités françaises marquent leur soutien au rôle octroyé à Europol en matière d'innovation. Le positionnement de l'agence s'en trouve renforcé ce qui permettra de soutenir et d'apporter un appui utile aux services répressifs. À cet égard, et pour placer l'agence dans une perspective plus globale, outre le laboratoire d'innovation, le Hub d'innovation JAI aurait mérité d'être mentionné.

Considérant 11: In order to help EU funding for security research to develop its full potential and address the needs of law enforcement, Europol should assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation that are relevant to Europol's objectives. When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, it should not receive funding from that programme in accordance with the conflict of interest principle.	**Les autorités françaises rappellent que l'agence Europol n'est pas la seule agence de l'UE intervenant dans le domaine de la sécurité intérieure.** **À ce titre, elles estiment qu'une telle mission pourrait être dévolue au** pôle d'innovation (Hub) **actuellement en cours de création. Cette structure distincte d'Europol – qui n'en assure que le soutien et le secrétariat – apparait comme plus pertinente pour éviter les redondances et mutualiser les efforts.** **La rédaction de ce considérant devrait donc être adaptée en mettant en avant l'approche globale de mise en relation des agences et réseaux souhaitée par la création du pôle d'innovation.** **Soit la proposition de rédaction suivante :** Europol in association with relevant security agencies should assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation that are relevant to Europol's objectives
Considérant 12: **It is possible for the Union and the Members States to adopt restrictive measures relating to foreign direct investment on the grounds of security or public order. To that end, Regulation (EU) 2019/452 of the European Parliament and of the Council establishes a framework for the screening of foreign direct investments into the Union that provides Member States and the Commission with the means to address risks to security or public order in a comprehensive manner. As part of the assessment of expected implications for security or public order, Europol should support the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes**	Les autorités françaises rappellent que le règlement 2019/452 cité ne fait pas référence à l'agence Europol ce qui pourrait créer une situation d'insécurité juridique quant à la mise en pratique d'une telle mission. Elle précise que le règlement 2019/452 encadre les investissements directs étrangers en matière de "sécurité ou d'ordre public" qui n'entrent pas dans le champ de compétence de l'agence. Enfin, un conflit d'intérêt pourrait émerger quand il s'agira pour l'agence d'étudier des investissements directs étrangers qui pourraient concerner le développement/l'utilisation de technologies par Europol. Les autorités françaises proposent donc la suppression de ce considérant.

Considérant 37 : Given the challenges that the use of new technologies by criminals pose to the Union's security, law enforcement authorities are required to strengthen their technological capacities. To that end, Europol should support Member States in the use of	**Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.** **Elles rappellent que la Commission, dans sa stratégie de sécurité intérieure pour l'Union 2020-**

emerging technologies in preventing and countering crimes falling within the scope of Europol's objectives. To explore new approaches and develop common technological solutions for Member States to prevent and counter crimes falling within the scope of Europol's objectives, Europol should be able to conduct research and innovation activities regarding matters covered by this Regulation, including with the processing of personal data where necessary and whilst ensuring full respect for fundamental rights. The provisions on the development of new tools by Europol should not constitute a legal basis for their deployment at Union or national level.	**2025 évoquait dans la lignée de la révision du règlement Europol** *« la création d'un pôle d'innovation européen* ***pour la sécurité intérieure qui serait chargé de définir des solutions conjointes à des défis communs en matière de sécurité et face à des opportunités que les États membres ne peuvent exploiter seuls*** **». Elle précisait que ce pôle travaillerait avec Frontex, CEPOL, eu-LISA et le Centre commun de recherche (JRC).** **Afin de mutualiser les moyens humains et financiers, les autorités françaises souhaitent que** l'ensemble des agences JAI **soient impliquées dans le développement d'outils technologiques. Elles ajoutent que le CEPD et la FRA doivent pouvoir être impliqués dans ce processus si nécessaire.** **Proposition d'amendement :** **"To that end, Europol should** *in close cooperation with relevant Union bodies* **support Member States in the use of emerging technologies in preventing and countering crimes falling within the scope of Europol's objectives."**
Considérant 38 : **Europol should play a key role in assisting Member States to develop new technological solutions based on artificial intelligence, which would benefit national law enforcement authorities throughout the Union. Europol should play a key role in promoting ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety and fundamental rights.**	Les autorités françaises réitèrent leur commentaire précédent (considérant 37) et propose l'amendement suivant : **Europol should in close cooperation with relevant Union bodies play a key role in assisting Member States to develop new technological solutions based on artificial intelligence, which would benefit national law enforcement authorities throughout the Union. Europol should play a key role in promoting ethical, trustworthy and human centric artificial intelligence subject to robust safeguards in terms of security, safety and fundamental rights.**
Considérant 40: **Providing Europol with additional tools and capabilities requires reinforcing the democratic oversight and accountability of Europol. Joint parliamentary scrutiny constitutes an important element of political monitoring of Europol's activities. To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group with annual information on the use of these tools and capabilities and the result thereof.**	Afin de suivre et d'enrichir les travaux de l'agence, cette information annuelle doit être communiquée aux États membres. Les autorités françaises proposent de modifier le considérant comme suit : « *To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group and the Member States with annual information on its use of these tools and capabilities and the result thereof* ».

Considérant 41: **Europol's services provide added value to Member States and third countries. This includes Member States that do not take part in measures pursuant to Title V of Part Three of the Treaty on the Functioning of the European Union. Member States and third countries may contribute to Europol's budget based on separate agreements. Europol should therefore be able to receive contributions from Member States and third countries on the basis of financial agreements within the scope of its objectives and tasks.**	Les autorités françaises s'étonnent d'une telle proposition et rappellent que l'agence Europol ne peut voir se créer un lien de dépendance plus spécifique avec un État au prétexte qu'il contribuerait davantage à son budget que les autres. Cette situation serait préjudiciable à la fois pour les États membres mais également pour l'image de l'agence et la confiance que les États membres placent en elle. Elles souhaitent donc que la Commission soit interrogée sur l'existence d'un tel mécanisme dans d'autres agences de l'UE qui concerne non seulement **les États membres mais également les États tiers**. L'expérience acquise par les autorités françaises dans d'autres enceintes multilatérales où les États membres financent les projets au cas par cas leur permet **d'émettre d'importantes réserves sur ce mécanisme**. Celui-ci **créera inévitablement des déséquilibres forts, en matière d'influence, entre les États capables de financer des projets et ceux qui ne le peuvent ou ne le souhaitent pas.** Enfin il est à craindre que les projets soutenus par les États membres soient systématiquement soumis à des conditions de ressources dans les documents de programmation tandis que ceux portés par la Commission ou Europol seront considérés comme financés *ab initio*.

Article 1 (2) (a) (iv) Tasks **(t) proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States, and implement its research and innovation activities regarding matters covered by this Regulation, including the development, training, testing and validation of algorithms for the development of tools**	**Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 37.** **Pour mémoire : Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.**
Article 1 (2) (d) **Tasks** **4a. Europol shall assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation activities that are relevant to achieve the objectives set out in Article 3. When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, the Agency shall not receive funding**	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 37. Pour mémoire : les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.

from that programme.	
Article 1 (2) d) Tasks **4b. Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council* that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security.**	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 12. Pour mémoire : les autorités françaises rappellent que le règlement 2019/452 cité ne fait pas référence à l'agence Europol ce qui pourrait créer une situation d'insécurité juridique quant à la mise en pratique d'une telle mission. Elle précise que le règlement 2019/452 encadre les investissements directs étrangers en matière de "sécurité ou d'ordre public" qui n'entrent pas dans le champ de compétence de l'agence. Enfin, un conflit d'intérêt pourrait émerger quand il s'agira pour l'agence d'étudier des investissements directs étrangers qui pourraient concerner le développement/l'utilisation de technologies par Europol. Les autorités françaises proposent donc la suppression de cet article.

Article 1 (38) *Article 57* Budget 4. Europol may benefit from Union funding in the form of contribution agreements or grant agreements in accordance with its financial rules referred to in Article 61 and with the provisions of the relevant instruments supporting the policies of the Union. Contributions may be received from countries with whom Europol or the Union has an agreement providing for financial contributions to Europol within the scope of Europol's objectives and tasks. The amount of the contribution shall be determined in the respective agreement.	**Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 41.** **Pour mémoire :** **Les autorités françaises s'étonnent d'une telle proposition et rappellent que l'agence Europol ne peut voir se créer un lien de dépendance plus spécifique avec un État au prétexte qu'il contribuerait davantage à son budget que les autres. Cette situation serait préjudiciable à la fois pour les États membres mais également pour l'image de l'agence et la confiance que les états-membres placent en elle.** **Elles souhaitent donc que la Commission soit interrogée sur l'existence d'un tel mécanisme dans d'autres agences de l'UE qui concerne non seulement** les États membres mais également les États tiers**.** **L'expérience acquise par les autorités françaises dans d'autres enceintes multilatérales où les États membres financent les projets au cas par cas leur permet** d'émettre d'importantes réserves sur ce mécanisme**. Celui-ci** créera inévitablement des déséquilibres forts, en matière d'influence, entre les États capables de financer des projets et ceux qui ne le peuvent ou ne le souhaitent pas.

	Enfin il est à craindre que les projets soutenus par les États membres soient systématiquement soumis à des conditions de ressources dans les documents de programmation tandis que ceux portés par la Commission ou Europol seront considérés comme financés *ab initio*. **La définition** « countries with whom Europol or the Union has an agreement providing for financial contributions to Europol within the scope of Europol's objectives and tasks" mériterait d'être précisée.

GERMANY

Germany's follow-up comments to the LEWP meeting on 25 January 2021 (Revision of the Europol Regulation)

In addition to the comments made at the last LEWP meeting on 25 January 2021 please find below Germany's written comments on thematic blocks 1 (cooperation with private parties) and 3 (research and innovation). Further comments may be raised following ongoing scrutiny of the proposal.

Thematic block 1: Cooperation with private parties

Article 4(1)(m):

Please rephrase to clarify Europol's exact mandate on "Terrorist Content Online" more precisely, in particular in respect of the provisions of the TCO Regulation. For example, the latter's Article 13(1), (3) and (4) could be referred in order to specify Europol's role.

Article 4(1)(u):

In order to align Europol's proposed activities with the EUCP, the wording of the new Article 4(1)(u) should be amended as follows:

"(u) support Member States' actions in **a crisis within the meaning of the EU Crisis Protocol (EUCP) that constitutes a critical incident online where** preventingthe dissemination of online content **is linked to or suspected as being carried out in the context of** related to terrorism or violent extremism in crisis situations, which stem**ming**s from an ongoing or recent real-world event, **which** depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and **where the content** aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers."

If this amendment is included, the provision describes the scenario which it aims to govern but it does not yet precisely address what will be the exact action by Europol to support Member States, inter alia vis-à-vis Article 4(1)(m). We are not sure the new Article 26a sheds complete light on this. Could this be described more precisely?

Article 26(2):

According to the explanation given by the Commission at the meeting, the last clause of the new Article 26(2) (which reads as follows: "unless a national unit, contact point or authority concerned resubmits the personal data to Europol in accordance with Article 19(1) within four months after the transfer takes place") could be deleted. This deletion would clarify that the obligation to delete the data takes effect immediately after the transfer to all concerned units has been completed. In our view, this does not preclude the receiving Member State from resubmitting the data as national data to Europol in accordance with its national legislation for purposes covered by the Europol Regulation.

Article 26(4):

Editorial comment: The second sentence should read: "… may transfer the result of its analysis and verification of such data to the third country concerned."

Article 26(5):

As stated by the Commission at the meeting, "transfer" is used in the context of data exchange with states and international organisations. Based on this, "transfer" would seem to be the correct term in Article 26(5). As a general remark. Germany would prefer a definition of the terms "transfer" an "transmission" and its consistent use in the whole text.

Furthermore, if the provision aims at informing the private party that the information received is insufficient, why is there a need to transfer other personal data than the data already received from that party?

Article 26(6a):

According to the explanation given by the Commission at the meeting, it should be clarified that Member States are not legally bound to fulfil the requests made by Europol. Therefore, the first sentence should be amended as follows:

"Europol may request Member States, via their national units, to obtain personal data from private parties […] **in accordance with the applicable national law**.".

This applies accodingly to Art. 26a(5).

Article 26(6b):

How does this provision relate to the subjects covered by Art 88 TFEU?

Art. 26a:

As mentioned above in respect to Article 4(1)(u), it remains unclear what the supporting task of Europol would be, including the relationship to the current tasks under Article 4(1)(m).

Thematic block 3: Research and innovation

Article 4(1)(t):

Following the call of the Home Affairs Ministers in paragraph 6 of their Joint Declaration on the Future of Europol, it is important that measures to strengthen Europol in the area of research and innovation build upon the EU Innovation Hub for Internal Security in order to ensure a coherent approach. The creation of the EU Innovation Hub for Internal Security was supported by Ministers at the JHA Council on 8 October 2019 and taken up by the Commission in its EU Security Union Strategy 2020-2025.

Therefore, the proposed new Article 4(1)(t) should be amended as follows:

"(t) proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States, and implement its research and innovation activities regarding matters covered by this Regulation, including the development, training, testing and validation of algorithms for the development of tools**, and contribute to the coordination of activities of Justice and Home Affairs agencies in the field of research and innovation in close cooperation with Member States**;"

Article 4(4a):

The proposed new Article 4(4a) should be deleted. In line with the Agency's core mandate, measures to strengthen Europol in the area of innovation and research should be focused on supporting MS' law enforcement authorities and not the Commission. From a governance perspective, giving the Commission a right to issue instructions to Europol would undermine the independence of the Agency, thus contradicting the clear position of Home Affairs Ministers in their Joint Declaration. Moreover, the proposal would create a paradoxical situation to the detriment of Member States. Excluding Europol from funding in the areas where it assists the Commission would at the same time limit its own possibilities to implement innovation projects. Therefore, the proposed new Article 4(4a) would have a negative impact on one of the very objectives of the legislative proposal, namely to strengthen Europol's capacity to effectively support Member States in the field of innovation.

Article 4(4b):

Considering that screening mechanisms based on Regulation (EU) 2019/452 are conducted by Member States at national level and that said Regulation does not foresee a role for Europol, the proposed new Article 4(4b) should be deleted.

Article 18(2)(e):

Could „matters covered by this Regulation" be specified more precisely, e.g. by referring to specific tasks from the Europol mandate?

Although the Commission referred to Article 33a at the meeting, the preference of synthetic/anonymized data is not yet explicitly mentioned. This should be clarified here or in Article 33a.

ITALY

With reference to the request to the delegations during the LEWP's meeting of 25 January,

Italy supports Europol's participation in the upcoming LEWP meetings on Europol recast.

LITHUANIA

In accordance to the last informal videoconference of the LEWP on 25/01/2021, please be informed that Lithuanian delegation will remain with the same comments/remarks on the first two thematic blocks (cooperation with private parties and research and innovation) of the Revision of Europol Regulation, as stated in our message dated on 21/01/2021.

Hereby, we do agree that Europol could participate in these specific meetings.

POLAND

General remarks :

Poland positively assesses the support provided by Europol to the competent national authorities so far, while recognizing the possibility of introducing further improvements in its functioning. Poland is of the opinion that it is necessary to maintain the supportive role of Europol, while respecting the exclusive competences of the Member States.

Poland still raises the parliamentary reservation due to the ongoing consultations at the national level. We reserve our right to express further remarks and comments at a later stage of discussion and during the next LEWP VTCs.

Poland supports participation of Europol in LEWP VTCs

Recitals of Proposal:

PL suggest adding in the preamble the following motive :

Europol's new legal framework fully respects the principles enshrined in the art. 4.2 of the Treay on the European Union as well as recognizes that national security remains the sole responsibility of each Member State. Since the objective of this Reguation is to strenghten action by the Member States' law enforcement services and their mutual cooperation in preventing and combating serious crime and terrorism Europol's institutional role has to be carefully balance in order to guarantee a neccessary level of benefits for the Member States while maintaining and respecting the very essence of their exclusive competence in the area of national security.

On page 28 of 13908/20, Article 4:

(t) proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States, and implement its research and innovation activities regarding matters covered by this Regulation, including the development, training, testing and	Comment: Due to the cross-sectoral nature of the EU Innovation Hub, we believe that effective inter-agency cooperation is necessary

validation of algorithms for the development of tools.	

On page 29 of 13908/20, Article 4:

"4a. Europol shall assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation activities that are relevant to achieve the objectives set out in Article 3. When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, the Agency shall not receive funding from that programme.	Comment: We consider it important to provide adequate human and financial support to Europol, given the significant expansion of its competences and tasks.
4b. Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security.*	Comment: This provision enables Europol to seek active role in the process of screening foreign direct investment into the EU which may disort the balance between the Europol's scope of competence and the issues falling within the category of the exclusive competence of the EU Member States in accordane with art 4 (2) of the Treaty on EU. The process of screening foreign direct investment is closely related to security-sensitive area such as critical infrastructure, dual use items or critical techologies, listed in art. 4 regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union.

	Taking into account the specific nature of the activities carried out by the competent national authorities in these areas, the practical dimension of such cooperation between these authorities and the Europol may prove to be problematic due to the fact that it touches upon economic security of the Eu Member States which, being one of the core elements of national secuirty, is excluded from the scopeof EU law. Therefore, in the opinion of our experts Europol should not play an active role in the process of screening foregin direct investment.

On page 29 of 13908/20, Article 6

(3) in Article 6, paragraph 1 is replaced by the following: *"1. In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation."*	In the opinion of our experts (initial remarks) : There is no consent for any amendment introducing obligation to a Member State to act on request of Europol. We believe that Europol should not interfere in investigation proceddings.

On page 31 of 13908/20, Article 18a

1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where: *(a) a Member State or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2); and*	Comment: This issue requires detailed reflection in the framework of expert work and it is the subject of our analyzes, e.g. it has to be claryfied if a Memebr State is supposed to provide whole case file to Europol ?

(b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded.	

On page 34 of 13908/20, Article 26

PL suggests including in the text: the definition of private parties and the explanation of the scope of data which Europol is to receive from private parties

On page 36 of 13908/20, Article 26

"6a. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned. *Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives.*	Comment: This issue is analyzed by the Polish ENU, e.g. in the context of the possible generation of additional tasks for ENUs. The request made by Europol shall not pose any obligation to Member States. Obtaining any information from private parties should be contucted on a voluntary basis.

NETHERLANDS

Amendment of the Europol Regulation, blocks 1 and 3

Comments of the Netherlands following the LEWP meeting of 25 January

We have not been able to study all articles in detail yet, so we may have further comments on these two blocks at a later point.

Article 26(2)

In the amended version of this article, the only aim of Europol receiving personal data directly from private parties is to identify all national units concerned. After it has forwarded the personal data to those national units, it will delete the information, unless it is resubmitted. It therefore seems that the intention of this article is that Europol receives the information on behalf of the national units concerned and then transfers ownership of the information to them. Once the national units concerned are the owners of the information, they can put restrictions on access to that information when they resubmit it.

However, in addition to those national units, Europol can also provide the information to third countries and international organisations. Since the aim of this article seems to be to transfer ownership of the information to the national units concerned, we were wondering whether Europol consults those national units before forwarding the information to a third country? What would happen if a Member State would resubmit the data with the restriction that it cannot be forwarded to third countries, but Europol has already done so?

Article 26(4)

Should it be “with” or “to” the country concerned in the final line?

Article 26(5)

Should “either” be deleted in para 5 sub a, since “or” has been deleted too?

Article 26(6a)

We would appreciate it if it could be clarified in the text that Member States can refuse a request from Europol to obtain personal data from private parties.

Article 26(6b)

In this article it says that: “In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data.” Does this mean that Europol does have access to the data if the crimes fall within its mandate? In what way?

Article 26a(2)

Should it be “with” or “to” the country concerned in the final line?

Article 26a(5)

Since this is a similar paragraph to 26(6a), maybe we should consider also clarifying in this text that Member States can refuse a request from Europol to obtain personal data from private parties.

Article 33a

There seem to be a paragraph 1 and 3, but no paragraph 2?

POLAND

ROMANIA

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

- **Romanian written comments on blocks 1 and 3 -**

- ✓ **Block 1: enabling Europol to cooperate effectively with private parties**

- Art. 1(2)(a)(iii)/ art 4 (1) (m) – We do not consider it necessary to propose the extension of Europol's area of competence from the *referral* (as is foreseen in the current Regulation) to supporting MS actions to prevent and combat **crimes promoted or committed using the Internet**, **in particular by coordinating** the response of law enforcement authorities' response to cyberattacks or the taking down of terrorist content online **for the following reasons**:

a) cyberattacks do not fall into the category of crimes foreseen under the Europol mandate;

b) there are already provisions in the new TCO Regulation regarding the taking down of terrorist content online;

c) it is important to avoid overlapping and duplication of mechanisms.

- art 1 (12) (a)/ Art 26 (2). We consider that **through the amendments provided in Art. 26 (2) no improvements have been made compared to the current provisions considering the fact that the data obtained from private parties can be processed only pursuant to art.18 (a) (cross-checks) and not pursuant to letter (b) and (c), respectively strategic or operational analyses and after the identification of the competent authority the personal data thus obtained will be deleted. For a better management of this type of data, we consider that the personal data obtained from private parties should be stored at Europol level only for a determined period, only for fulfilling Europol's objectives and processed under art 18 (a), (b) and (c) of the Europol Regulation.**

-Art. 1 (12) (c)/ Art *26 (5).* An additional amendment should be made by adding *and following prior consent of MS* as follows: *Europol may transmit or transfer personal data to private parties on a case-by-case basis, where it is strictly necessary,* ***and following prior consent of MS*** *and subject to any possible restrictions stipulated pursuant to Article 19 (2) or (3) and without prejudice to Article 67, in the following cases: (..)* **Europol may transmit or transfer data to private parties only after consultation and approval of the data provider (MS concerned).**

With regard to recital (25), the specific circumstances that could allow such an exchange of personal data should be defined. As for recital (35) the exchange of personal data with private parties should take place only with MS agreement, so as not to affect ongoing operations.

-Art 1 (12) (d)/ 26 (6b). Further details are needed on the Europol infrastructure that could be used in the exchange of data and information between a competent authority of a Member State and private parties.

With regard to data protection, the legal conditions for the processing of personal data and the transfer of personal data must be complied with, in accordance with the provisions of Regulation (EU) 2018/1725. We support the provisions of paragraph 1 of art. 36 for maintain the provisions regarding the manner of exercising the right of access.

- **Block 3 - strengthening Europol's role on research and innovation**

- **Art.1(5)(a)(ii), art. 1(5)(b) și art. 1(19). We need additional information / clarifications regarding these Articles, respectively the personal data / categories of personal data that are intended to be processed for research and innovation purposes in relation to the issues covered by this proposal for a Regulation on the development, preparation, testing and validation of algorithms for the development of tools, as well as whether this activity cannot be performed by using fictitious personal data or previously established personal data to be used in the case of such tests.**

With regard to the processing of personal data, in the context of the proposed Europol Regulation and the role that EUROPOL will play in the field of research and innovation**, a new provision on processing personal data for research and innovation purposes is necessary in order to strengthen the safeguard of fair and lawful processing, .**

SPAIN

Follow-up comments to the last LEWP meeting (25/01/2021)

REVISION OF THE EUROPOL REGULATION

DEFINITION CRISIS SITUATION (Article 4.1 u)

Regarding "crisis situations" definition pursuant **to Article 4.1 u**, this Delegation suggest the crisis situation definition offers in Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, adding the requirements of the Europol mandate:

"It is considered a crisis situation at Union level when a crime under Europol's mandate (serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy, as listed in Annex I- Art. 3) and the disruption caused an incident with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at Union political level".

Moreover, taking as a reference the definitions of crisis provided by the Council of the European Union in documents such as the Decision on the modalities for the implementation by the Union of the solidarity clause (2014/415/EU), this concept should be understood as follows:

"crisis" means a disaster or terrorist attack whose far-reaching effects or political significance are such as to require timely coordination of measures and a response at the political level of the Union.

In order to clarify the casuistry covered by this concept beyond terrorism - the purpose of which is to subvert the constitutional order or seriously alter public peace - in the case of Spain, and taking the terms used from Organic Law 5/2010, of 22 June, which modifies Organic Law 10/1995, of 23 November, of the Criminal Code, the concept of crisis situation should include any act with criminal casuistry that directly undermines the very basis of democracy and quantitatively multiplies its damaging potential by altering the normal functioning of markets and institutions, corrupting the nature of legal business, and even affecting the management and capacity for action of the organs of the State.

CLARIFYING THE ROLE OF EUROPOL IN THE REQUEST FOR THE INITIATION OF AN INVESTIGATION (Art.6.1)

Pertaining to clarify the role of Europol in the request for the initiation of an investigation into offences affecting the common interests of the Union, our position of this refers to the article 6 Europol Regulation (REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016). In this sense, it is considered that this Article provides sufficient legal cover to request the initiation of investigations and therefore it is not considered necessary to amend the regulation to this effect.

ON INTERPRETATION OF ARTICLE 7.8 AND POSSIBLE DYSFUNCTIONS OF FINANCIAL INTELLIGENCE UNITS

With regard to Article 7.8, it is specified that the cooperation of the above-mentioned Financial Intelligence Units (FIUs) may cooperate with Europol within the terms and limits set by the national units and always within their competences as laid down in Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of criminal offences.

In particular, Chapter IV of the above-mentioned Directive on Exchange of Information with Europol, and in particular Article 12 thereof, which provides that each Member State shall ensure that its FIU is empowered to respond to duly motivated requests made by Europol through the Europol national unit or, if permitted by that Member State, through direct contacts between the FIU and Europol. This is within Europol's responsibilities and for the performance of its tasks.

In this regard, it is considered that the wording of this article is appropriate and respects the interests of Spain, being consistent with our legal system and regulations regarding the entity responsible for the management of the Financial Titles File (FTF), which is SEPBLAC.

REQUEST FOR THE PRESENCE OF STAFF TO DEAL WITH TECHNICAL ISSUES THAT MAY ARISE IN CONNECTION WITH THE NEW EUROPOL REGULATION.

Given the technical complexity of certain terms and concepts of the regulation to be reformed and of the proposed new wording, it is considered of interest to have Europol staff present to clarify the doubts raised by the different delegations, such as those that arose at the last VTC meeting held on 25 January:

-discussion of terms: transfer of data, crisis situations, key themes, private parties, etc.

-data protection declarations

-other

3. COMMENTS RECEIVED AFTER THE MEETING ON 8 FEBRUARY 2021 (BLOCKS 1, 3, 5 AND 7)

AUSTRIA

Concerning the presence of Europol at the meetings of the LEWP (Europol Regulation)

Dear Chair, do you think it would be possible that Europol will be present for the entire duration of our meetings? This would give them the opportunity to follow the discussions and to better understand the concerns delegations have. To be present for one hour answering questions which Europol's representative doesn't know why they come up, seems to be not very effective.

EUROPOL will intervene only by request of the Presidency and for technical reasons/clarification, bilateral discussions are not possible in the format of a video conference, we don't see therefore the risk of influencing the legislative process.

Comments to document WK 757/2021 REV 1

Article 4/4b + recital 12

We are still not convinced that this task is within the mandate of Europol.

EUROPOL is established with a view to supporting cooperation among **law enforcement authorities.**

The screening of foreign direct investments is not necessarily the task of law enforcement authorities in the Member States.

We propose to delete Article 4/4b and recital 12.

Article 7/ 8

Article 12 of Directive (EU) 2019/1153 reads "…Member State shall ensure that its FIU is entitled to reply to duly justified requests made by Europol through the Europol national unit **or, if allowed by that Member State, by direct contacts between the FIU and Europol.**

This second part of the sentence is an important aspect for us. It should be reproduced in order to avoid confusion.

We propose the following wording:

8. Member States shall ensure that their financial intelligence units established pursuant to Directive (EU) 2015/849 ~~2005/60/EC~~ of the European Parliament and of the Council are **entitled to reply to duly justified requests made by** ~~**allowed to cooperate with**~~ Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and the Council, in particular via their national unit **or, if allowed by that Member State, by direct contacts between the FIU and Europol** regarding financial information and analyses, within the limits of their mandate and competence **and subject to national procedural safeguards.**

Article 26/6b + recital 34

The scope of SIENA is currently to facilitate "**the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations"** (recital 24 of the current EUROPOL Regulation)

In fact, when SIENA is used by Member States for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol has not access to that data.

whereas article 26/6b and recital 34 provide for

……. "exchanges **between the competent authorities of Member States and private parties."**

Either it is foreseen to create a new system or to use the capacities of SIENA for exchanges between competent authorities of Member States and private parties. In any case EUROPOL shall not have access to that data unless authorised by that Member State**.**

Therefore, we propose the following wording for article 26/6b and recital 34:

6b. Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws. ~~In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data.~~ **EUROPOL shall not have access to that data unless authorised by that Member State.**

Recital 34

The last part of the new sentence is not clear to us. This infrastructure provides a channel for interactions between LEAs and private parties, we do not see any connection to the access by a private party to information in Europol's systems (related to the exchange with that private party). We propose to delete the last part of the new sentence and the last sentence.

(34) Europol should be able to provide the necessary support for national law enforcement authorities to interact with private parties, in particular by providing the necessary infrastructure for such interaction, for example, when national authorities refer terrorist content online to online service providers or exchange information with private parties in the context of cyberattacks. **Europol should ensure by technical means that any such infrastructure is strictly limited to providing a channel for such interactions between the law enforcement authorities and a private party, and that it provides for all necessary safeguards against access by a private party to any other information in Europol's systems, ~~which is not related to the exchange with that private party~~.** ~~Where Member States use the Europol infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol should not have access to that data.~~ **EUROPOL shall not have access to that data unless authorised by that Member State**.

BELGIUM

Written comments by Belgium

concerning the proposed revision of the Europol Regulation (EU) 2016/794

Our remaining concerns in relation to block 1 on private parties are the following:

- In art. 26(6a) we believe that clarifications are still necessary. The private party will ideally send the information requested by Europol back to Europol via the MS, and COM believes this then should be considered as national information. To us this is not clear from the text. Also, the private party might provide information to Europol directly (seeing as this remains an open question in the current text) and COM explained to me that in that case the guarantees from art. 26(2) do not apply. So this means then that Europol does not have an obligation in that case to inform concerned MS, nor other concerned states. So this unclarity on the status of this information and what will be done with it is problematic according to us. We propose the following sentence to be added after the first sentence of paragraph 6a: 26(6a): *"If following this request Europol receives information directly from private parties, the procedures of the second paragraph will apply."*

- We support the Dutch question on private parties not being prohibited to forward information received from Europol, as is the case for others in art. 23(7). Maybe also art. 23(6) requires similar attention to ensure purpose-limited use by private parties of the information they receive from Europol. We wonder if in both paragraphs of this article private parties could be added to the list of partners.

Our remaining concerns in relation to block 3 on research and innovation are the following:

- We support the previous German question on including an explicit reference to the preference for synthetic/anonymized data in the Regulation, because we believe that this task – using real data for research and innovation projects – is quite new within the EU data protection acquis and the principle of data minimization is insufficiently precise to this end. Taking inspiration from art. 13 of Regulation 2018/1725 we propose the following sentence to be added to art. 33a as a new paragraph (possibly replacing the non-existing paragraph 2): *"The principle of data minimization should be ensured through measures including pseudonymisation provided that the purposes of Europol's research and innovation projects can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."* Another option is the following sentence: *"Preference should be given to using synthetic, pseudonymized and/or anonymized personal data."*

Related to blocks 5 and 7 we would like to express an ongoing scrutiny reservation.

BULGARIA

Bulgarian contribution to the draft

Regulation amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

Bulgaria would like to thank to the Portuguese Presidency for continuing the detailed discussion on the draft Regulation text by text and for considering our proposals.

Bulgaria would like to support the concerns raised by some delegations whether the participation of **Europol** in the **LEWP** meetings will be effective and of full value for so short time (1 hour). We believe that the full time participation of Europol in the meetings will contribute to the better understanding of some specific aspects related to the practice and daily activity of the Agency.

Comments on thematic block 1 - Enabling Europol to cooperate effectively with private parties:

We would like to resubmit our comments on **Article 26 Exchange of personal data with private parties** with request for additional clarifications in case the wording proposed by the Commission remains unchanged:

We would like to kindly ask Portuguese Presidency Europol to be consulted if the text of the art. 26 will in any way affect the agreements for operational cooperation/working arrangements with third countries currently in force, especially the provisions for the information exchange.

We would also like to kindly ask Europol to examine if the proposed wordings of art. 26 do not exclude any hypothesis of receiving and processing personal data from private parties and its subsequent transmission or transfer to the stakeholders concerned.

Denmark, Norway, Switzerland, Iceland, USA, Canada, Western Balkans countries and other countries are considered by the Member States as strategic operational partners and they should be on an equal footing when it comes to exchange of information, including personal data, which concerns them and which could be essential for their security or for prevention, investigation and prosecution of crime.

Comments on thematic block 5 - Cooperation with third countries:

We would like clarification of the provision of Art. 25, para 8, which introduces a new term "operational personal data". This term is used in the Eurojust Regulation, but not in the Europol Regulation which requires including the necessary definition.

A possible option to regulate this issue is to adapt the legal framework for personal data exchange with third countries on the model of Eurojust, which will provide more flexibility. This approach should be thoroughly discussed. In case there is a consensus in this regard, it should be reflected in the whole text of the draft Regulation.

Comments on thematic block 7: Clarifying that Europol may request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

Bulgaria prefers the current wording of art 6 of Europol Regulation (EU) 2016/794 and sees no need for its amendment.

CYPRUS

Written comments by Cyprus concerning the proposed revision of the Europol Regulation (EU) 2016/794 (Blocks 5 & 7):

Cyprus in general supports the proposed amendments which are clearly aiming to strengthen the mandate of EUROPOL.

Article 6

However, Cyprus believes that there is no need for the proposed amendment of Article 6, since the existing form responds to the mandate of Europol. Europol's role is, and must continue to be a supporting Agency to the Member States and their Competent Authorities.

Article 25

Cyprus agrees with the amendments on Article 25. However, the Regulation of Europol must ensure that all data will be transferred to Third Countries, after the written approval of the country which is the owner of the information, in each case of transfer. Also, Cyprus strongly believes that the information should be transferred to Third Countries that are directly related with the case and their contribution is required for purposes of preventing and combating crime such as terrorism and organized crime that affect the interests of the European Union.

CZECH REPUBLIC

Drafting comments on document wk 757/1/2020 REV 1:

Block 1

Article 2(r)

We welcome this definition; in order to align it fully with the Crisis Protocol[1], following changes are introduced:

"(r) "online crisis situation" means the dissemination of online content that is linked to or suspected as being carried out in the context of terrorism or violent extremism stemming from and ongoing or recent real-world event **of suspected criminal nature**, which depicts harm to life ...."

Article 4(1)(m)

In order to specify the coordination powers and reflect the distribution of responsibilities in draft TCO regulation, as the Europol has no power to take down terrorist content online, following redrafting is proposed:

"(m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including **in taking down of terrorist content online, and**, ~~in cooperation with Member States,~~ ~~**the coordination of law enforcement authorities' response to cyberattacks**~~, ~~**the taking down of terrorist content online, and**~~ the making of referrals of internet content, **and, on request of a Member State, the coordination of law enforcement authorities' response to cyberattacks;"**

"referral of Internet content" should be defined in Article 2 to mean "referral of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions";

---

1 A crisis within the meaning of this Protocol constitutes a critical incident online where:
(1) the dissemination of content is linked to or suspected as being carried out in the context of terrorism or violent extremism, stemming from an on-going or recent real-world event which depicts harm to life or physical integrity, or calling for imminent harm to life or physical integrity and where the content aims at or has the effect of seriously intimidating a population; and
(2) where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.
A strong indicator of terrorist or violent extremist context is where the content is produced by or its dissemination is attributable to listed terrorist organisations or other listed violent extremist groups. The Protocol pertains only to online content stemming from events of a suspected criminal nature.

Article 26(2)

Obligation to identify "all" national units concerned could in theory lead to infinite or very long processing of received personal data. Therefore we suggest to add maximum limit for processing in the first sentence:

2. Europol may receive personal data directly from private parties and process those personal data**, for a period no longer than 6 months,** in accordance with Article 18 in order to identify all national units concerned, as referred to in point (a) of paragraph 1. ...

In addition, it would be strongly preferable for policy reasons to include in the second sentence the Member State of main establishment of private party among the national units notified:

Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the national units concerned**, including the national unit of the Member State of the main establishment of such private party**.

Article 26(6a)

We support amended recital 31 and understand that there is only so much that may be provided for at EU level. Still, more can be done, while respecting the role of national legislators. In the light of the 2019 Council Conclusions, the replies to requests should be voluntary both for Member State's authorities and private parties (because the private party can find legal basis under GDPR or national rules). It should be also clear what the second subparagraph requires (legal basis for processing on the part of competent authority is not the same as duty of private party to reply established in domestic law). Therefore we suggest following changes:

6a. At the request of Europol, ~~may request~~ Member States, via their national units, may ~~to~~ obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned.

Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives. The cooperation of private parties is voluntary, unless otherwise provided for by Member State law.

Article 26a(5)

We support amended recital 31 and understand that there is only so much that may be provided for at EU level. Still, more can be done, while respecting the role of national legislators. In the light of the 2019 Council Conclusions, the replies to requests should be voluntary both for Member State's authorities and private parties (because the private party can find legal basis under GDPR or national rules). It should be also clear what the second subparagraph requires (legal basis for processing on the part of competent authority is not the same as duty of private party to reply established in domestic law). Therefore we suggest following changes:

5. At the requests of Europol Member States, via their national units, may ~~to~~ obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned. Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives. The cooperation of private parties is voluntary, unless otherwise provided for by Member State law.

Block 3

CZ supports changes already made in Articles 18(2)(e), 18(5), 33a(1)(c)(g) by the Presidency.

Article 4(4a)

CZ believes that the wording should focus more on:

(a) the research and innovation being done at Europol,

(b) the innovation monitoring and

(c) the support Europol gives to research prioritization by the Member States.

Certain parts of Art. 66(1)(2) of Frontex Regulation could be used in this regard.

Block 5

Article 25(5)

We propose to use the term "or category of transfers" to align the text with Art. 38(1) LED.

We also support to strengthen substantially the transfer tools available, similarly to those used by Eurojust. Situation of Schengen-associated countries should be clarified. As German delegation announced drafting proposal, CZ refrains from proposing particular wording at this moment.

Block 7

Article 6(1)

We refuse the proposed addition of "Member State or". While this proposal falls into scope of mandate of Europol under Art. 3(1), it is unnecessary, superfluous, burdensome and disproportionate. Already under existing rules, the Europol can and should send any information that may lead to start of investigations to relevant Member State. However, the formal mechanism of Art. 6 is inappropriate for crimes that affect only that Member State and contravenes the principle of subsidiarity.

(end of file)

FINLAND

With regard to our meeting on Europol-recast on 8th of February and DE proposal for wording for block 5: "We therefore consider to add a paragraph to the proposed new Article 27a stating that Article 25 does not apply to Schengen-associated countries, but that data transfers to these countries are subject to the requirements of Article 19(2) and (3) and Article 67 and would appreciate an opinion of the GSC legal service regarding this question."

We agree with DE in that an adequacy decision or an international agreement would not fit with the countries implementing Schengen that have also implemented the LED, and confirm our initial support for the DE proposal. However, we would be grateful if the Presidency and the Legal Service verified the correct drafting from a legal-linguistic point of view, considering that this Regulation concerns an EU agency. To our understanding, the usual way of taking Schengen-associated countries into account in EU legislation has been to state it in the recitals for each Schengen State, for example:

> "As regards Switzerland, [this Directive] constitutes a development of provisions of the Schengen *acquis*, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis.*" (see the recitals of the LED)

FRANCE

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leur commentaires écrits suite à la réunion de groupe LEWP du 8 février 2021, consacrée à l'examen des dispositions relatives à l'échange de données avec les parties privées et au rôle de l'agence en matière de recherche et d'innovation, ainsi qu'aux dispositions relatives à la capacité d'initiative d'enquête de l'agence et la coopération avec les pays tiers.

I – Sur le document WK757 REV1 /21

S'agissant de l'examen du bloc 1 :

Les autorités françaises portent à la connaissance de la Présidence les remarques suivantes :

Considérant 25: **To support Member States in cooperating with private parties providing cross-border services where those private parties hold information relevant for preventing and combatting crime, Europol should be able to receive, and in specific circumstances, exchange personal data with private parties.**	**Les autorités françaises notent que le considérant 25 ne mentionne que le soutien d'Europol aux États membres pour coopérer avec les** parties privées prestataires de services transfrontaliers. **Les articles modifiés figurant dans la révision du Règlement vont cependant bien au-delà de cet objectif, soulevant un problème de cohérence entre les objectifs et la proposition.** **Aussi les autorités françaises s'interrogent sur la possibilité de mieux inscrire cet objectif dans les articles liés à l'échange d'information entre Europol et les parties privées (articles 26 et 26a).**
Considérant 31: Member States, third countries, international organisation, including the International Criminal Police Organisation (Interpol), or private parties may share multi-jurisdictional data sets or data sets that cannot be attributed to one or several specific jurisdictions with Europol, where those data sets contain links to personal data held by private parties. Where it is necessary to obtain additional information from such private parties to identify all relevant Member States concerned, Europol should be able to ask Member States, via their national units, to request private parties which are established or have a legal representative in their territory to share personal data with Europol in accordance with those Member States' applicable laws. **Member States should assess Europol's request and decide in accordance with their national laws whether or not to accede to it. Data processing by private parties should remain subject to their obligations under the applicable rules, notably with regard to data protection.** In many cases, these Member States may not be	Les autorités françaises sont favorables à cet ajout qui permet aux autorités compétentes de respecter leurs obligations dérivant du droit national (issues parfois elles-mêmes du droit européen), notamment en matière de confidentialité et de respect des sources.

able to establish a link to their jurisdiction other than the fact that the private party holding the relevant data is established under their jurisdiction. Irrespective of their jurisdiction with regard the specific criminal activity subject to the request, Member States should therefore ensure that their competent national authorities can obtain personal data from private parties for the purpose of supplying Europol with the information necessary for it to fulfil its objectives, in full compliance with procedural guarantees under their national laws.	
Considérant 35: **Terrorist attacks trigger the large scale dissemination of terrorist content via online platforms depicting harm to life or physical integrity, or calling for imminent harm to life or physical integrity. To ensure that Member States can effectively prevent the dissemination of such content in the context of such crisis situations stemming from ongoing or recent real-world events, Europol should be able to exchange personal data with private parties, including hashes, IP addresses or URLs related to such content, necessary in order to support Member States in preventing the dissemination of such content, in particular where this content aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.**	Le passage en situation de crise pourrait être décidé ad-hoc après concertation des États membres (exemple : attentats sur le territoire européen concernant plusieurs États membres).

Article 2 (r) 'online crisis situation' means the dissemination of online content that is linked to or suspected as being carried out in the context of terrorism or violent extremism stemming from an ongoing or recent real-world event, which depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and where the online content aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.	**En relation avec la modification du titre de l'article 26a qui précise qu'il est question de l'échange de données personnelles entre Europol et les parties privées en situation de crise « en ligne » et de celle de l'article 4 (u), les autorités françaises sont favorables à l'ajout d'une définition de ce qui est entendu par « situation de crise en ligne ».** **Les autorités françaises souhaitent obtenir des clarifications ou des exemples de situations pour lesquels la dissémination de contenu en ligne pourrait être uniquement** suspectée **d'être organisée dans un contexte de terrorisme ou d'extrémisme violent découlant d'un événement récent ou en cours dans le « monde réel ».** **Cette notion étant peu claire et pouvant entrainer des interprétations divergentes, en fonction de la réponse apportée, il pourra être demandé de**

	supprimer : « or suspected as being carried out in ».
Article 4 (u) support Member States' actions in preventing the dissemination of online content **in an online crisis situation, in particular by providing private parties with the information necessary to identify relevant online content**. ~~**Related to terrorism or violent extremism in crisis situations, which stems from an ongoing or recent real-world event, depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.**~~	Les autorités françaises soutiennent cette suppression, la définition d'une situation de crise en ligne étant prévue à l'article 2.
Article 1(4) **Article 7 :** Member States shall ensure that their financial intelligence units established pursuant to Directive (EU) 2015/849 2005/60/EC of the European Parliament and of the Council are **entitled to reply to duly justified requests made by allowed to cooperate with** Europol in accordance with Article 12 of Directive (EU) 2019/1153 of the European Parliament and the Council, in particular via their national unit regarding financial information and analyses, within the limits of their mandate and competence **and subject to national procedural safeguards.** _____ * Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73). ** Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ L 186, 11.7.2019, p. 122)."	Les autorités françaises remercient la Présidence pour la prise en compte de leur proposition d'amendement.

Article 1(2)(a)(iii) « support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the coordination of law enforcement authorities' response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions ».	Dans la poursuite des travaux sur l'outil PERCI d'Europol et en prévision du règlement sur les contenus terroristes en ligne, les autorités françaises soutiennent la proposition d'article. Dans la lignée du document de programmation 2022-2024 actuellement discuté au sein de l'agence, les autorités françaises estiment particulièrement nécessaire de rappeler, dans le cadre des discussions sur ce bloc, l'importance de délivrer le projet PERCI d'ici à fin 2022.
Article 1(2)(a)(iv) « support Member States' actions in preventing the dissemination of online content related to terrorism or violent extremism in crisis situations, which stems from an ongoing or recent real- world event, depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers ».	

Article 1(12)(a) **" Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 in order to identify all national units concerned, as referred to in point (a) of paragraph 1. Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the national units concerned. Europol may forward the personal data and relevant results from the processing of that data necessary for the purpose of establishing**	**Les autorités françaises saluent cette proposition équilibrée de la Commission. Toutefois, elles rappellent que la coopération entre Europol et les parties privées doit être transparente envers les États membres et proposent à cet effet deux nouvelles dispositions (*cf. fin de document*).**

jurisdiction in accordance with Article 25 to contact points and authorities concerned as referred to in points (b) and (c) of paragraph 1. Once Europol has identified and forwarded the relevant personal data to all the respective national units concerned, or it is not possible to identify further national units concerned, it shall erase the data, unless a national unit, contact point or authority concerned resubmits the personal data to Europol in accordance with Article 19(1) within four months after the transfer takes place."	
Article 26 (6b) Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws. In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data.	Les autorités françaises réitèrent leurs commentaires précédents sur cet article à savoir que **SIENA ne peut être en aucun cas utilisé pour permettre l'échange de données personnelles avec les parties privées**.
Article 1 (13) : **Article 26** 1. Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 to prevent the dissemination of online content related to terrorism or violent extremism in crisis situations as set out in point (u) of Article 4(1). 2. If Europol receives personal data from a private party in a third country, Europol may forward those data only to a Member State, or to a third country concerned with which an agreement on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 TFEU has been concluded or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation. Where the conditions set out under paragraphs 5 and 6 of Article 25 are fulfilled, Europol may transfer the result of its analysis and verification of such data with the third country concerned. **2a. Any cooperation of Europol with private parties shall neither duplicate nor interfere with the activities of Member States' financial intelligence units established pursuant to Directive (EU) 2015/849 of the European**	Les autorités françaises remercient la Présidence pour la prise en compte de leur remarque et la modification subséquente de cet article. Par ailleurs, à l'article 26a *"Exchanges of personal data with private parties in **online** crisis situations"*, les autorités françaises sont favorables à l'ajout du terme online qui, en lien avec la définition proposée à l'article 2, permet de préciser le type de crise dont il est question.

Parliament and of the Council, and shall not concern information that is to be provided to financial intelligence units for the purposes of that Directive. 3. Europol may transmit or transfer personal data to private parties, on a case-by-case basis, subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67, where the transmission or transfer of such data is strictly necessary for preventing the dissemination of online content related to terrorism or violent extremism as set out in point (u) of Article 4(1), and no fundamental rights and freedoms of the data subjects concerned override the public interest necessitating the transmission or transfer in the case at hand. 4. If the private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, the transfer shall be authorised by the Executive Director. 5. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol for preventing the dissemination of online content related to terrorism or violent extremism as set out in point (u) of Article 4(1). Irrespective of their jurisdiction with regard to the dissemination of the content in relation to which Europol requests the personal data, Member States shall ensure that the competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives. 6. Europol shall ensure that detailed records of all transfers of personal data and the grounds for such transfers are recorded in accordance with this Regulation and communicated upon request to the EDPS pursuant to Article 40. 7. If the personal data received or to be transferred affect the interests of a Member State, Europol shall immediately inform the national unit of the Member State concerned."	

Les autorités françaises proposent en complément des articles additionnels :

Les autorités françaises estimeraient opportun de soumettre ces différentes propositions à la discussion des États membres et inviter ceux-ci à les commenter, éventuellement sous forme d'une « procédure écrite » afin de ne pas alourdir les travaux en réunion par visioconférence LEWP.

- Pour mémoire les conclusions du ***Conseil sur la coopération entre Europol et les parties privées du 3 décembre 2019*** soulignent *« un renforcement du rôle du Conseil d'administration d'Europol »* dans la relation entre l'agence et les parties privées. Ainsi, afin de garantir la totale transparence de l'activité d'Europol avec les parties privées et renforcer le rôle des États membres, les autorités françaises proposent un mécanisme pérenne permettant aux États membres de prendre connaissance et de valider tous les protocoles d'entente (Memorandum of understanding - MoU) que l'agence a signé avec les partenaires privées.

- **Proposition d'article 26 paragraphe 9 échange de données à caractère personnel avec les parties privées (Nouveau) :**

  « Sous l'égide et avec l'accord du Conseil d'administration, Europol peut conclure des protocoles d'entente avec les parties privées. Ces protocoles n'autorisent pas l'échange de données à caractère personnel et ne lient ni l'Union ni ses États membres.

  Europol communique systématiquement aux États membres l'ensemble des protocoles d'ententes conclus par l'agence avec les parties privées, pour information et validation par le Conseil d'administration ».

- **Article 11 (r) Fonctions du Conseil d'administration (Amendement) :**

  r) Autorise la conclusion d'arrangements de travail, d'arrangements administratifs et ***de protocoles d'entente avec les parties privées*** *conformément à l'article 23, paragraphe 4, à l'article 25, paragraphe 1 et à* ***l'article 26 paragraphe 9 respectivement.***

- Également, dans la continuité de ces conclusions sur la relation entre Europol et les parties privées, les autorités françaises proposent l'article suivant :

  Article 26 paragraphe 2.bis : Échanges de données à caractère personnel avec les parties privées (Nouveau) :

  « […] Europol peut recevoir et traiter des données à caractère personnel transmises directement par les parties privées conformément au paragraphe 2, et avec l'accord du Conseil d'administration. Cet accord prend la forme d'une liste de parties privées proposée par le directeur exécutif et adoptée par le Conseil d'administration ».

- **Article 11 : Fonction du Conseil d'administration (Amendement)**

Article 11 v) : « adopte la liste des parties privées autorisées à transmettre des données à Europol ».

***

S'agissant de l'examen du bloc 3 :

Les autorités françaises marquent leur soutien au rôle octroyé à Europol en matière d'innovation. Le positionnement de l'agence s'en trouve renforcé ce qui permettra de soutenir et d'apporter un appui utile aux services répressifs.

Considérant 12: It is possible for the Union and the Members States to adopt restrictive measures relating to foreign direct investment on the grounds of security or public order. To that end, Regulation (EU) 2019/452 of the European Parliament and of the Council establishes a framework for the screening of foreign direct investments into the Union that provides Member States and the Commission with the means to address risks to security or public order in a comprehensive manner. As part of the assessment of expected implications for security or public order, Europol should support the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes	**Les autorités françaises rappellent que le règlement 2019/452 cité ne fait pas référence à l'agence Europol ce qui pourrait créer une situation d'insécurité juridique quant à la mise en pratique d'une telle mission. Elle précise que le règlement 2019/452 encadre les investissements directs étrangers en matière de "sécurité ou d'ordre public" qui n'entrent pas dans le champ de compétence de l'agence.** **Enfin, un conflit d'intérêt pourrait émerger quand il s'agira pour l'agence d'étudier des investissements directs étrangers qui pourraient concerner le développement/l'utilisation de technologies par Europol.** **Les autorités françaises proposent donc la suppression de ce considérant et de l'article afférent**

Considérant 37 : **Given the challenges that the use of new technologies by criminals pose to the Union's security, law enforcement authorities are required to strengthen their technological capacities. To that end, Europol should support Member States in the use of emerging technologies in preventing and countering crimes falling within the scope of Europol's objectives**, also in cooperation with relevant networks of Member States' practitioners. Europol should also work with other EU agencies in the area of justice and home affairs to drive innovation and foster synergies within their respective mandates, and support related forms of cooperation such as secretarial support to the 'EU Innovation Hub for Internal Security' as a collaborative network of innovation labs. **To explore new approaches and develop common technological solutions for Member States to prevent and counter crimes falling within the scope of Europol's objectives, Europol should be able to conduct research and innovation activities regarding matters covered by this Regulation, including with the processing of personal data where necessary and**	**Les autorités françaises remercient la Présidence pour la prise en compte de leurs remarques s'agissant de la coopération avec les autres agences JAI.**

whilst ensuring full respect for fundamental rights. The provisions on the development of new tools by Europol should not constitute a legal basis for their deployment at Union or national level.	
Considérant 40: **Providing Europol with additional tools and capabilities requires reinforcing the democratic oversight and accountability of Europol. Joint parliamentary scrutiny constitutes an important element of political monitoring of Europol's activities. To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group with annual information on the use of these tools and capabilities and the result thereof.**	Afin de suivre et d'enrichir les travaux de l'agence, cette information annuelle doit être communiquée aux États membres. Les autorités françaises proposent de modifier le considérant comme suit : « *To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group and the Member States with annual information on its use of these tools and capabilities and the result thereof* ».

Article 1 (2) d) Tasks 4b. Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council* that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security.	**Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 12.** **Pour mémoire : les autorités françaises rappellent que le règlement 2019/452 cité ne fait pas référence à l'agence Europol ce qui pourrait créer une situation d'insécurité juridique quant à la mise en pratique d'une telle mission. Elle précise que le règlement 2019/452 encadre les investissements directs étrangers en matière de "sécurité ou d'ordre public" qui n'entrent pas dans le champ de compétence de l'agence. Enfin, un conflit d'intérêt pourrait émerger quand il s'agira pour l'agence d'étudier des investissements directs étrangers qui pourraient concerner le développement/l'utilisation de technologies par Europol. Les autorités françaises proposent donc la suppression de cet article.**

II – Commentaires suite à la réunion du 8 février consacrée à l'examen des blocs 5 et 7

S'agissant du bloc 5 : coopération avec les pays tiers

Analyse détaillée :

Considérant 24: *Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation.*	Les autorités françaises doutent que la modification mineure du régime dérogatoire de l'article 25 du règlement Europol puisse résoudre le problème de fond lié à la rigidité du régime juridique applicable aux relations d'Europol avec les parties privées. Pour mémoire, la France soutient « l'option 2 » proposée par la Commission européenne : *ajouter la possibilité, en l'absence d'une coopération opérationnelle structurelle visée à l'option 1, de transférer des données à caractère personnel dans les cas où l'existence de garanties appropriées dans le pays tiers, en ce qui concerne la protection des données à caractère personnel, est prévue dans un instrument juridiquement contraignant (intervention législative).* Les autorités françaises proposent que le régime juridique des relations d'Europol avec les pays tiers soit assoupli tout en permettant un contrôle strict des États membres et l'assurance du respect des codes de gestion dans cet échange de données entre l'agence et les États tiers. Ces échanges devront impérativement respecter les principes de la règle du tiers service. Également, les autorités françaises s'interrogent sur la notion « categories of transfers » ajoutée par la Commission à l'article 25 paragraphe 5 et souhaiterait disposer d'éclaircissements. Au titre de la gouvernance des EM sur Europol, et au regard de la règle du tiers service/propriété de l'information, ces derniers doivent être impliqués dans le dispositif de validation visant au transfert de données. Proposition d'amendements : *Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries within the agreement of the management board while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects.*
Article 1 (6) : ***Article 18a(4) :*** *Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article*	Les autorités françaises s'étonnent de la possibilité offerte à certains États tiers de pouvoir bénéficier du soutien d'Europol dans l'analyse de données. Sur le plan juridique, la mise en œuvre d'une telle proposition nécessiterait de réviser l'ensemble des accords opérationnels de l'agence en prenant en compte ces nouvelles dispositions. Par ailleurs, les autorités françaises considèrent que si ces transmissions de données personnelles n'ont

25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, or the EDPS, reaches the conclusion that there are preliminary…	pas donné lieu à une ouverture d'enquête par un Etat membre, une telle proposition implique pour Europol la nécessité de soutenir une enquête criminelle menée par un État tiers. Or, Europol est une agence qui soutient en priorité les États membres dans leurs enquêtes. Il est donc indispensable que, si les données fournies par un Etat tiers devaient être ainsi exploitées, cela ne devrait se faire qu'au profit d'un ou plusieurs États-membres ayant ouvert une enquête miroir permettant d'exploiter ces données. Les autorités françaises rappellent l'importance de la règle du tiers service/propriété de l'information s'agissant des données communiquées à Europol. Dès lors, les échanges relatifs à des données en provenance des États membres doivent strictement respecter ce cadre.
Article 1 (11) ***Article 25*** *Transfer of personal data to third countries and international organisations* *(a) In paragraph 5, the introductory phrase is replaced by the following:* *"By way of derogation from paragraph 1, the Executive Director may authorise the transfer or categories of transfers of personal data to third countries or international organisations on a case-by-case basis if the transfer is, or the related transfers are:* ***(b) In paragraph 8, the following sentence is deleted :*** ***Where a transfer is based on paragraph 5, such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.***	Les autorités françaises soulignent que la Commission européenne n'a pas modifié le régime général de l'échange de données par Europol avec les États tiers. Les autorités françaises estiment que l'article 25 ne permet pas de pallier aux rigidités du cadre juridique actuel en la matière. Enfin, elles proposent que le cadre relatif à l'échange de données personnelles entre Europol et les États tiers soit **calqué sur celui d'Eurojust**. En effet, le règlement Eurojust dans ses articles 56 à 59 prévoit notamment le transfert de données personnelles vers un Etat tiers présentant des garanties appropriées en matière de protection des données (art. 58). Ces garanties sont évaluées par l'agence et implique un mécanisme d'information du CEPD.

***

S'agissant de l'examen du bloc 7 sur la capacité d'initiative d'enquête de l'agence :

Remarques préliminaires :

S'agissant des enquêtes transfrontalières, les autorités françaises rappellent leur attachement au cadre actuel, qui consiste pour Europol à proposer **une enquête d'initiative quand au moins deux États membres sont concernés.**

Analyse détaillée :

Considérant 14 : *One of Europol's objectives is to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combatting forms of crime which affect a common interest covered by a Union policy.* *To strengthen that support, Europol should be able to request the competent authorities of a Member State to initiate, conduct or coordinate a criminal investigation of a crime, which affects a common interest covered by a Union policy, even where the crime concerned is not of a cross-border nature. Europol should inform Eurojust of such requests.*	Dans la continuité de la note de commentaire des autorités françaises du 30 octobre 2020, les autorités françaises sont défavorables à la révision de l'article 6 du règlement Europol actuel. En effet, cette disposition n'est quasiment pas mise en œuvre et les enquêteurs, en lien avec leurs autorités judiciaires, doivent disposer de la maîtrise de l'ouverture de leurs enquêtes. Les autorités françaises rappellent tout de même que, interrogées sur le sujet, ni la Commission, ni Europol n'ont pu fournir de statistiques concernant le recours à l'article 6 du règlement Europol actuel. Toutefois, les autorités françaises constatent que la nouvelle rédaction de l'article 6 tient compte de certaines réserves exposées et ne prévoit pas de pouvoir d'enquête d'initiative pour l'agence. Elles relèvent enfin que la préservation de l'efficacité des choix des stratégies d'entrave milite en faveur de la maitrise du dialogue entre services enquêteurs et autorités judiciaires. Les autorités françaises rappellent que la déclaration des ministres de l'Intérieur sur l'avenir d'Europol du 22 octobre 2020 précise clairement que les États membres détiennent les « ***compétences exclusives exécutives pour initier et conduire des enquêtes*** ». En outre, elles rappellent qu'une telle disposition pourrait altérer le principe de subsidiarité tel que prévu à l'article 5 du Traité sur l'Union européenne qui **consiste à** réserver à l'UE – uniquement ce que l'échelon inférieur – **les États membres–** ne pourrait effectuer que de manière moins efficace. **Or il apparait qu'Europol ne peut en aucun cas disposer d'informations et de moyens lui permettant d'évaluer la situation interne d'un seul Etat membre.** Également, conformément au principe de proportionnalité, les moyens mobilisés par l'Union européenne ne doivent pas être plus contraignants que ce qui est nécessaire pour atteindre un objectif donné. En l'état ni la Commission, ni Europol n'ont

	démontré des défaillances des États membres à ce niveau. Au contraire, les autorités françaises rappellent que l'article 6 n'a été que rarement mobilisé par Europol.
Article 1 (3) *Request by Europol for the initiation of a criminal investigation* *In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation.*	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 14. Elles rappellent également que la déclaration des ministres de l'intérieur sur l'avenir d'Europol souligne clairement qu'il appartient aux EM d'initier et de conduire des enquêtes. Pour mémoire : Dans la continuité de la note de commentaires des autorités françaises du 30 octobre 2020, les autorités françaises sont défavorables à la révision de l'article 6 du règlement Europol actuel. En effet, cette disposition n'est quasiment pas mise en œuvre et les enquêteurs, en lien avec leurs autorités judiciaires, doivent disposer de la maîtrise de l'ouverture de leurs enquêtes. Les autorités françaises rappellent tout de même que, interrogées sur le sujet, ni la Commission, ni Europol n'ont pu fournir de statistiques concernant le recours à l'article 6 du règlement Europol actuel. Toutefois, les autorités françaises constatent que la nouvelle rédaction de l'article 6 tient compte de certaines réserves exposées et ne prévoit pas de pouvoir d'enquête d'initiative pour l'agence. Elles relèvent enfin que la préservation de l'efficacité des choix des stratégies d'entrave milite en faveur de la maitrise du dialogue entre services enquêteurs et autorités judiciaires. **Les autorités françaises** rappell**ent** que la déclaration des ministres de l'Intérieur sur l'avenir d'Europol du 22 octobre 2020 précise clairement que les **États** membres détiennent les « *compétences exclusives exécutives pour initier et conduire des enquêtes* ».

	En outre, **elles rappellent** qu'une telle disposition pourrait altérer le principe de subsidiarité tel que prévu à l'article 5 du Traité sur l'Union européenne qui consiste à **réserver à l'UE – uniquement ce que l'échelon inférieur** – les États membres– **ne pourrait effectuer que de manière moins efficace**. Or il apparait qu'Europol ne peut en aucun cas disposer d'informations et de moyens lui permettant d'évaluer la situation interne d'un seul Etat membre. **Également, conformément au** principe de proportionnalité, les moyens mobilisés par l'Union européenne ne doivent pas être plus contraignants que ce qui est nécessaire pour atteindre un objectif donné. En l'état ni la Commission, ni Europol n'ont démontré des défaillances des **États** membres à ce niveau. Au **contraire, les autorités françaises rappellent** que l'article 6 n'a été que rarement mobilisé par Europol.

Proposition d'article :

Les autorités françaises réitèrent la proposition formulée à l'occasion du dernier LEWP, à savoir l'ajout d'un nouvel article 7(12) :

"Europol rédige un rapport annuel portant sur la nature et le volume des données personnelles fournies à Europol par les États tiers et les parties privées sur la base des critères d'évaluation quantitatifs et qualitatifs fixés par le CAE. Ce rapport annuel est transmis au Parlement européen, au Conseil, à la commission et au parlement nationaux".

Article 7(12) ***Europol shall draw up an annual report on the number of cases in which Europol issued notifications to private parties on missing information in accordance with point (d) of paragraph 5 of Article 26 or requests Member States to obtain personal data from private parties in accordance with paragraph 6a of Article 26, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks;***	**Les autorités françaises remercient la Présidence pour la reprise de** l'esprit général **de ses propositions, qui couvre l'ensemble des données échangées entre Europol et les parties privées.** Cette proposition d'article concernant la présentation d'un rapport annuel demeure toutefois **trop restrictive** et devrait prendre en compte un bilan de l'ensemble des données reçues et communiquées aux parties privées par Europol (Cf. articles 26(2), 26(4) 26(5) et 26 (6a & 6b).)

Concernant le sujet du financement et la coopération avec les pays tiers :

Les autorités françaises font part de leur étonnement concernant l'ajout d'une disposition (article 57) permettant aux États membres ou États tiers (ayant signé un accord avec l'UE ou l'agence) de contribuer directement au budget d'Europol. Quand bien même le conseil d'administration approuverait le budget, y compris les contributions directes d'États, cette pratique n'a jamais été codifiée auparavant et introduirait un mécanisme susceptible de perturber considérablement l'équilibre sur lequel Europol est construite.

Considérant 41: Europol's services provide added value to Member States and third countries. This includes Member States that do not take part in measures pursuant to Title V of Part Three of the Treaty on the Functioning of the European Union. Member States and third countries may contribute to Europol's budget based on separate agreements. Europol should therefore be able to receive contributions from Member States and third countries on the basis of financial agreements within the scope of its objectives and tasks.	**Les autorités françaises s'étonnent d'une telle proposition et rappellent que l'agence Europol ne peut voir se créer un lien de dépendance plus spécifique avec un État au prétexte qu'il contribuerait davantage à son budget que les autres. Cette situation serait préjudiciable à la fois pour les États membres mais également pour l'image de l'agence et la confiance que les États membres placent en elle.** **Elles souhaitent donc que la Commission soit interrogée sur l'existence d'un tel mécanisme dans d'autres agences de l'UE qui concerne non seulement** les États membres mais également les États tiers**.** **L'expérience acquise par les autorités françaises dans d'autres enceintes multilatérales où les États membres financent les projets au cas par cas leur permet** d'émettre d'importantes réserves sur ce mécanisme**. Celui-ci** créera inévitablement des déséquilibres forts, en matière d'influence, entre les États capables de financer des projets et ceux qui ne le peuvent ou ne le souhaitent pas. **Enfin il est à craindre que les projets soutenus par les États membres soient systématiquement soumis à des conditions de ressources dans les documents de programmation tandis que ceux portés par la Commission ou Europol seront considérés comme financés *ab initio*.**
Article 1 (38) **Article 57** **Budget** ***4. Europol may benefit from Union funding in the form of contribution agreements or grant agreements in accordance with its financial rules referred to in Article 61 and with the provisions of the relevant instruments supporting the policies of***	Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 41. Pour mémoire : Les autorités françaises s'étonnent d'une telle proposition et rappellent que l'agence Europol ne peut voir se créer un lien de dépendance plus spécifique avec un État au prétexte qu'il contribuerait

the Union. Contributions may be received from countries with whom Europol or the Union has an agreement providing for financial contributions to Europol within the scope of Europol's objectives and tasks. The amount of the contribution shall be determined in the respective agreement.	davantage à son budget que les autres. Cette situation serait préjudiciable à la fois pour les États membres mais également pour l'image de l'agence et la confiance que les états-membres placent en elle. Elles souhaitent donc que la Commission soit interrogée sur l'existence d'un tel mécanisme dans d'autres agences de l'UE qui concerne non seulement **les États membres mais également les États tiers**. L'expérience acquise par les autorités françaises dans d'autres enceintes multilatérales où les États membres financent les projets au cas par cas leur permet **d'émettre d'importantes réserves sur ce mécanisme**. Celui-ci **créera inévitablement des déséquilibres forts, en matière d'influence, entre les États capables de financer des projets et ceux qui ne le peuvent ou ne le souhaitent pas.** Enfin il est à craindre que les projets soutenus par les États membres soient systématiquement soumis à des conditions de ressources dans les documents de programmation tandis que ceux portés par la Commission ou Europol seront considérés comme financés *ab initio*. La définition « **countries with whom Europol or the Union has an agreement providing for financial contributions to Europol within the scope of Europol's objectives and tasks" mériterait d'être précisée.**

III – S'agissant de la proposition de la Commission visant à conférer à l'agence un rôle d'incrémentation du SIS

En vue de la réunion du LEWP plénier du 22 février, les autorités françaises réaffirment leur opposition ferme à la proposition de la Commission visant à conférer à l'agence un rôle d'incrémentation du SIS.

GERMANY

Germany's follow-up comments to the LEWP meeting on 8 February 2021 (Revision of the Europol Regulation)

Please find below Germany's written comments both on the first revised version of the text of the Commission proposal (changes to the provisions pertaining to thematic blocs 1 and 3) and – in addition to the comments already made at the last LEWP meeting on 8 February 2021 – on thematic blocs 5 and 7. Further comments may be raised following ongoing scrutiny of the proposal.

Thematic bloc 3: research and innovation

Article 4(4a):

The proposed new Article 4(4a) should be deleted. In line with the Agency's core mandate, measures to strengthen Europol in the area of innovation and research should be focused on supporting Member States' law enforcement authorities and not the Commission. The proposal would create a paradoxical situation to the detriment of Member States. Excluding Europol from funding in the areas where it assists the Commission would at the same time limit its own possibilities to implement innovation projects. Therefore, the proposed new Article 4(4a) would have a negative impact on one of the very objectives of the legislative proposal, namely to strengthen Europol's capacity to effectively support Member States in the field of innovation. Neither Europol nor the Commission have been able to demonstrate that the ability to support the Commission would better serve this objective than if Europol could continue to benefit from funding in its innovation activities. Furthermore, from a governance perspective, giving the Commission a right to issue instructions to Europol would undermine the independence of the Agency, thus contradicting the clear position of Home Affairs Ministers in their Joint Declaration on the Future of Europol.

Article 4(4b):

Considering that screening mechanisms based on Regulation (EU) 2019/452 are conducted by Member States at national level and that the said Regulation does not foresee a role for Europol, the proposed new Article 4(4b) should be deleted.

Thematic bloc 5: cooperation with third countries

Cooperation with third countries is essential to the success of Europol's work, as successfully fighting terrorism and organised crime requires cooperation beyond the European level. If Europol is to properly fulfil its role as EU criminal information hub, more effective mechanisms must be put in place through which it can exchange information with third countries. Of course, this goes hand in hand with appropriate safeguards, e.g. a high level of data protection. Therefore, the Home Affairs Ministers in their Joint Declaration on the Future of Europol have called for strengthening Europol's ability to cooperate effectively with third countries.

We would like to thank the Commission for taking up this demand in their proposal. The COM proposal provides for the possibility for the Executive Director of Europol to authorise "categories of transfers" of personal data to third countries. This possibility is limited to the specific situations laid down in Article 25(5) and shall be carried out "on a case by case basis". We would appreciate an explanation how the authorisation of "categories of transfers" can be brought in line with the required assessment "on a case by case basis". Furthermore, please clarify the difference between such "categories of transfers" and "a set of transfers" dealt with in Article 25(6).

Beyond the original proposal, we have the following comments:

First of all, from our point of view the revision of the Europol Regulation would be a good opportunity to put the Schengen-associated countries on an equal footing with Member States when it comes to the legal basis for the exchange of personal data. The Schengen-associated countries have the same level of data protection in the JHA field as the Member States, as they have implemented and apply the Directive on data protection in the area of police and justice (Directive (EU) 2016/680). In view of this, an adequacy decision under Article 36 of the Directive in relation to Schengen-associated countries is out of the question. Also, an international agreement under Article 218 TFEU to establish the required level of data protection ("adequate safeguards") appears neither necessary nor appropriate. In line with the aim of strengthening Europol's cooperation with third countries, it rather seems justified to treat Schengen-associated countries in the same way as Member States. We therefore consider adding a paragraph to the proposed new Article 27a stating that Article 25 would not apply to Schengen-associated countries. Instead, data transfers to these countries would be subject to the requirements of Article 19(2) and (3) and Article 67. We would appreciate an opinion of the GSC legal service regarding this question.

Secondly, when it comes to the structural exchange of data, the Europol Regulation in Art. 25(1) – aside from existing cooperation agreements – only foresees the possibility of an adequacy decision or an international agreement pursuant to Art. 218 TFEU. Unlike Directive (EU) 2016/680 (cf. Art. 35(1)(d) thereof) or the Eurojust Regulation (Art. 56(2)(a) thereof), the Europol Regulation lacks reference to "appropriate safeguards". Practical experience shows that the scope of application of the options foreseen in the Europol Regulation is very limited: As of yet, no adequacy decision for the JHA area has been rendered. Although an adequacy decision for the UK will in all likelihood be reached, further decisions for other third countries or international organisations are not to be expected for the time being, according to the Commission itself. It is therefore doubtful that adequacy decisions for the JHA area will be of practical relevance in the future. The same applies to international agreements under 218 TFEU. No significant progress has been made so far in the ongoing negotiations. On the contrary, Europol has described the legal regime for structural

cooperation with third countries as dysfunctional. Against this background, it seems incomprehensible that Europol should not have any additional possibilities for a structural exchange of information with third countries. Therefore, we propose to give Europol the possibility, in the same way as the Directive (EU) 2016/680 and the Eurojust Regulation, to base the exchange of data also on "appropriate safeguards".

For this purpose, we have worked out the following proposals for wording:

Art. 25(1)(a):

"(a) decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision') **or in the absence of such a decision, appropriate safeguards have been provided for or exist in accordance with paragraph 4a of this Article, or in the absence of both an adequacy decision and of such appropriate safeguards, a derogation applies pursuant to paragraph 5 or 6 of this Article**;"

new Art. 25(4a):

"**4a. In the absence of an adequacy decision, Europol may transfer operational personal data to a third country or an international organisation where:**

(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or

(b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data."

Art. 25(8): "… Where a transfer is based on paragraph **4a** or 5, …".

Furthermore, we have some specific remarks and questions on certain provisions:

Article 25(1)(a) refers to Article 36 of Directive (EU) 2016/680: In this respect, Regulation (EU) 2018/1725 (in Art. 94(1)(a)) refers more specifically and correctly to Article 36(3) of the Directive. The reference in Article 25(1)(a) should be worded accordingly.

Article 25(1)(b) and Article 25(6) both refer to "adequate safeguards", which corresponds to the terminology of Regulation (EU) 2018/1725 (cf. Art. 94(1)(b) thereof), but deviates from the language used in the Directive (EU) 2016/680 (cf. Art. 37(1) thereof: "appropriate safeguards"). From our point of view, it is unclear whether this refers to different legal standards. In particular, the question arises whether "adequate safeguards" are stricter than "appropriate safeguards" due to a conceptual proximity to the "adequacy decision"? If it is only a matter of different terminology but the same meaning, harmonising the terminology would be desirable in order to prevent ambiguities. We would appreciate an opinion of the GSC legal service regarding this question.

Thematic bloc 7: ability to request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

In their Joint Declaration on the Future of Europol, Home Affairs ministers have explicitly emphasised that the exclusive executive power including the initiation and conducting of investigations lies with the law enforcement authorities of the Member States. Against this background, we see no need to amend Article 6. On the contrary, we would like to remind you that Europol, according to its own statement, has not made formal use of Article 6 in a single case so far. Neither the Commission nor Europol could demonstrate that there is a real need for the amendment of Article 6.

Following the clear rejection of this proposal by the Member States at the meeting on 8 February 2021, we ask the Presidency to delete the proposal in the next revision of the text.

HUNGARY

Comments by Hungary on Blocks 1, 3, 5 and 7 of the proposal for amending Regulation (EU) 2016/794

Please find below the preliminary comments made by Hungary on thematic Blocks 1, 3, 5 and 7 of the proposal for amending Regulation (EU) 2016/794. First of all we would like to stress that the Hungarian authorities are scrutinising the text of the regulation, and in this regard please consider our comments as initial ones.

In general Hungary agrees that the current Europol Regulation needs to be revised in a number of areas, as the challenges of recent years and the shortcomings identified in its implementation have made it clear that the Agency's role in supporting Member States can be implemented much more effectively, furthermore numerous tasks have arisen for Europol which need to be codified, for example strengthening cooperation with private parties and third countries is an urgent task. Having said this we would like to emphasize that by this regulation our aim should be to strengthen the core tasks of the agency and in this regard we consider it important to ensure the compliance with the Treaties and to avoid extending the mandate of the Europol to issues that fall within the exclusive competence of the Member States (such as the initiation/prioritisation of investigations).

Block 1:

As a general comment on this Block, we would like to have more clarity what would prevent the private parties located in third countries to provide the information received from Europol to any other party. We think that this is of concern especially when we talk about a private party which is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision.

We can support the newly proposed text in recital 31, as we think that Member States should assess Europol’s request and decide in accordance with their national laws whether or not to accede to it. However we would have appreciated a similar reference in the operational part of the text, but in the spirit of compromise we are ready to accept the proposal made by the Presidency.

As it was mentioned by several Member States regarding Article 26 we think that it would be important to find a solution according to which Europol should consults the national units concerned before forwarding the relevant information to a third country or international organisation, to be able to avoid cases when the relevant Member State wants to resubmit this information with a restrictions on access to it.

We welcome the addition of the definition of “online crisis situation”.

Block 3:

In point (q) of Article 4 we would like to have more clarity if the wording “risk for security” refers to the security of the EU or it shall also refer to cases where only the security of one Member State is concerned.

Regarding Paragraph 4b we are still analising if involving Europol in the screening of foreign direct investments should be part of the text, especially as Regulation (EU) 2019/452 has no specific reference to the involvement of the agency in such screening activities.

Block 5:

We would appreciate more clarity on the procedure according to which the Executive Director may authorise the transfer or categories of transfers of personal data to third countries or international organisations.

Furthermore as it was stated by some Member States during the LEWP meeting of 8 February we would like to ask the opinion of the CLS on the issue of treating the Schengen-associated countries in the same way as Member States when it comes to the cooperation of Europol and third countries.

Block 7:

Hungary would like to reiterate its firm position according to which it is of great concern that, "in specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation". We think that this provision would allow the agency to set priorities for the Member States when it comes to investigations carried out in the territory and this regard we would like to suggest the deletion of the changes in Article 6(1).

ITALY

ITALIAN CONTRIBUTIONS ON THE "*PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL AMENDING REGULATION (EU) 2016/794, AS REGARDS EUROPOL'S COOPERATION WITH PRIVATE PARTIES, THE PROCESSING OF PERSONAL DATA BY EUROPOL IN SUPPORT OF CRIMINAL INVESTIGATIONS, AND EUROPOL'S ROLE ON RESEARCH AND INNOVATION*" **BLOCKS 1-3-5-7**

DOC. ST.13908/20

WK 757/21 REV. 1

PROPOSAL OF THE COMMISSION	**ITALIAN COMMENTS**
RECITALS	
With reference to recital 3: *"These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal organised crime groups that engage in a wide range of criminal activities".*	Italy believes that it is of utmost importance to recall the pivotal role that mafia-style and family-based criminal organizations have played in taking advantage of the opportunities of the health emergency and digitization. **We therefore propose a revised version of recital 3:** These *threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal, mafia-style and family based organised crime groups that engage in a wide range of criminal activities.*
With reference to recital 6: *"High-risk criminals play a leading role in criminal networks and pose a high risk of serious crime to the Union's internal security. To combat high-risk organised crime groups and their leading members, Europol should be able to support Member States in focusing their investigative response on identifying these persons,*	Italy believes that with reference to the establishment of the Operational Task Forces (OTF) and the identification of the High Value Targets (HVT), it is of utmost importance to better define, in the proposal Regulation, the evaluation criteria and the selection procedures. Moreover Italy believes that in this part, as said with reference to recital 3, it would be pivotal to mention, mafia style and family based organised crime groups.

their criminal activities and the members of their criminal networks".	
With reference to recital 12 and connected new paragraph 4b of art.4 *".Europol should support the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes."*	Considering the different and heterogeneous Offices and Agencies involved at national level in the screening of foreign direct investments, Italy believes that further discussions on the role of Europol through ENUs in this matter are needed.
ARTICLES	
With reference to the amendment of art 2 (f) (e) *'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;* *(f) 'private parties' means entities and bodies established under the law of a Member State or third country, in particular companies and firms, business associations, non-profit organisations and other legal persons that are not covered by point (e);*	Considering the ongoing discussion and the pivotal importance of the cooperation with Private parties in the Europol new proposed regulation, Italy believes that it is extremely useful to define further the term "private parties". This would avoid any misinterpretation and would facilitate the cooperation among all stakeholders involved in the matter.
With reference to the amendment of art.4 h) and connected recital 4 "support *Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, and special*	Given the specific nature of the special intervention units, it would be preferable to specify the operational support given by Europol.

intervention units, including by providing operational, technical and financial support;"	During the discussion in the LEWP's meetings and as said in the Explanatory Memorandum of the Proposal, we understood that the support to MSs would be through ATLAS, therefore it could be useful to specify this in the text proposal. We propose to rephrase the sentence as follows: "support *Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, and special intervention units by means of ATLAS network, including by providing operational, technical and financial support"*
With reference to the amendment of art.4 m) *"support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the coordination of law enforcement authorities' response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;"*	Italy believes that the wording of the text is not very clear. It seems to give to Europol (though in cooperation with Member States) the possibility to coordinate (Member State) Law enforcement authorities response and the taking down of terrorist content online. On the contrary the main role of Europol should be, in our opinion, limited to supporting member States and not coordinating them. On a general basis, Italy believes that it has to be clarified within the text of art. 4 par. 1(m) that any action taken by Europol on this matter should be upon Member States' express request. As a consequence we propose the following wording: *"support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States and upon their request, the coordination of law enforcement authorities' response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;*

With reference to the amendment of art.4 par.1 (u) *"support Member States' actions in preventing the dissemination of online content in an online crisis situation, in particular by providing private parties with the information necessary to identify relevant online content".*	On a general basis, as in our previous comment, Italy believes that it has to be clarified in the text of art. 4 par. 1(u) that any action taken by Europol on this matter should be at the express request of a Member State and in accordance with its national law. Therefore we propose to amend the text as follows: *"Support, upon Member State request and in accordance to their national legislation, Member States' actions in preventing the dissemination of online content in an online crisis situation, in particular by providing private parties with the information necessary to identify relevant online content"*
With reference to the amendment of art.4 new paragraph 4b and connected recital 12: *"Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council* that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security"*	Italy recalling what said with reference to Recital 12 believes that according to Regulation (EU) 452/2019, the possibility of carrying out screening on investments from third countries into EU is an exclusive prerogative for Member States and the Commission. Italy believes that the provision of granting specific attributions to Europol in this sector seems to lay outside of the Law Enforcement prerogatives considering: -the screening activities of FDI involve not only Law enforcement agencies but also Intelligence's National Agencies, AML national Offices and national economic and fiscal Agencies; -Giving Europol such role as defined by new art. 4 par 4b could lead to unnecessary or undesirable overlaps. Italy thinks that further discussion, apart from the approval of Europol new Regulation, are necessary on this matter.

With reference to the new proposed version of Article 6 and connected recital 14: *"In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation."*	Italy believes that the current version of article 6 is in line with Council conclusion on the Future of Europol and with the July's European Parliament Resolution which stated that "..the strengthening of Europol capacity to request an investigation has to be with regards to crimes of cross border nature". Our general remark is that is not a clarifying but an amendment, considering that the current interpretation of art. 6 is that Europol can request the initiation of an investigation only in case of a cross border crime. Italy believes that the proposal moves the focus for the request of the investigation from the cross border approach to the common interest approach. As this would be an important and crucial transformation of the role of the Agency Italy believes that further discussion and explanations are required. This is why we are not in favour of the reviewed text proposed as the actual Europol regulation has already proved to be sufficient and adequate. Italy believes that no modification should involve art. 6 of the Europol actual Regulation.
***With* reference to the new article 18 3a:** *"Processing of personal data for the purpose of research and innovation as referred to in point (e) of paragraph 2 shall be performed by means of Europol's research and innovation projects with clearly defined objectives, duration and scope of the personal data processing involved, in respect of which the additional specific safeguards set out in Article 33a shall apply."*	Italy believes that the text here should be more specific. In particular, it should be made clear that processing personal data for such purposes is possible only if needed in order to reach the projects objectives. Therefore, we propose the following rephrasing: *"If needed in order to reach Europol's research and innovation project's* objectives, *processing of personal data for the purpose of research and innovation as referred to in point (e) of paragraph 2 shall be performed only by means of the mentioned projects with clearly defined objectives, duration and scope of the personal data processing involved, in respect of which the additional* specific *safeguards set out in Article 33a shall apply".*

***With* reference with the new Article 25 paragraph 5, replaced by the following:** *"By way of derogation from paragraph 1, the Executive Director may authorise the transfer or categories of transfers of personal data to third countries or international organisations on a case-by-case basis if the transfer is, or the related transfers are:"*	Italy would like to have explanations on this provision. If we compare this provision with the actual art 25 under the current regulation, we notice that the powers of the Executive Director now have increased including also « categories of transfers ». Why? On a general basis Italy believes that any transfer of data that Europol received by Member States or private parties before being transmitted or transferred has to be approved by the originating Member State -sender- (or the MS where the PP is based). We appreciated the explanations given by the Commission on the expression "categories of transfers" however we believes that there is still room for a further specification in the text proposed.
With* reference to the Article 26 paragraph 2 that would be replaced by the following:** *"Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 in order to identify all national units concerned, as referred to in point (a) of paragraph 1. Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the national units concerned. Europol may forward the personal data and relevant results from the processing of that data necessary for the purpose of establishing jurisdiction in accordance with Article 25 to contact points and authorities concerned as referred to in points (b) and (c) of paragraph 1. Once Europol has identified and forwarded the relevant personal data to all the respective national units concerned,* ***or *it is not possible to identify further national units concerned, it shall erase the data, unless a national unit, contact point or authority concerned resubmits the personal data to Europol in*	In general, Italy believes that any information exchange should comply with the current regulatory framework and fully involve the Europol National Units in case of a PP based in EU. Any direct exchange of information of Europol with PP should involve only Private Parties based in Third Countries. Italy believes that the first part of the article should be reworded according to the following version: *"Europol may only receive personal data directly from private parties, based on third countries, in compliance with national legal framework ..."*

accordance with Article 19(1) within four months after the transfer takes place."	
<u>*Regarding*</u> <u>the new paragraphs 6a and 6b of art. 26:</u> *"6a. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned...* *<u>(6b)</u> Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws. In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data.*	In order to avoid any overlapping with the domestic legislation Italy believes that it would be better to replace the part"...*under their applicable laws*.." with the part " *in accordance with the national legal framework*". If agreed the new version would be the following: 6a. *Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, ~~under their applicable laws~~ in accordance with the national legal framework , for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned...* Concerning the new proposed art. 26 par 6b Italy appreciated the Europol explanation during the 8 February LEWP meeting, however we believe that further discussions are required on this new tool.

<u>*With regard to the new art. 26a*</u> *"Exchanges of personal data with private parties in online crisis situations* *1. Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 to prevent the dissemination of online content related to terrorism or violent extremism in online crisis situations as set out in point (u) of Article 4(1)".*	In order to avoid any possible risk of overlapping with the national ongoing investigations Italy believes that it would be better that any exchange of data with Private parties based in EU have to be carried out via the ENUs.

LATVIA

LV written comments regarding the Commission (COM) proposal amending Europol Regulation[1] (hereinafter – COM proposal)

LV overall position on the COM proposal

In general, LV **welcomes** COM proposal that corresponds to the existing and foreseeable future challenges, for instance, in the context of developments in digitalisation and modern technologies.

LV believes that in view of the proposed changes Europol will be able to provide **a more effective, operational and innovative support** to the Member States regarding cross-border investigations with adequate respect of fundamental rights, in particular personal data.

LV also believes that it is important to ensure that **powers, tasks and aims of the strengthened Europol** do not duplicate the work performed by the law enforcement authorities (LEAs), but supplement it. It is also important that the new mandate of Europol does not result in an unjustified burden on the Member States.

Furthermore, any amendments in the Europol mandate should be assessed against **Article 88 of the Treaty on the Functioning of the European Union** (EU) and Europol's mission to **support and strengthen** action by the Member State's police authorities and other law enforcement authorities and their mutual cooperation. LV also finds it important to ensure that, when enlarging the mandate of Europol, **the tasks of the EU decentralized agencies do not overlap** that, inter alia, would allow promoting a well-considered use of the Multiannual Financial Framework funding.

In addition, LV finds it crucial to ensure **adequate and meaningful involvement of Member States in Europol's decision-making processes.**

LV is also convinced that, in the course of discussion within the Council, **the main emphasis must be placed on the quality of the amendments rather than on their speedy adoption.**

LV detailed position on specific thematic blocs of the COM proposal

Thematic bloc **I**: enabling Europol to cooperate effectively with **private parties**

- *Article 23(7) of the Europol Regulation*

LV **agrees** that private parties should not be able to onward personal data held by Europol. In view of this, LV **supports NL proposal** to add a reference to "private parties" in Article 23(7) of the Europol Regulation.

[1] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, COM (2020) 796 final

- *Article (1)(12)(d) (new Article 26(6a) of the Europol Regulation)*

LV **welcomes** PRES changes in the related Recital 31 that clarify that Member States are not obliged to reply to Europol's requests on privates parties. At the same time, LV believes that this aspect should also be **duly reflected in the relevant article**. Thus, LV suggests to replace the beginning of Article 26(6a) *"Europol may **request** (...)"* with *"Europol may **ask** (...)"*. LV also notes that in the related Recital 31 such a wording is used *"(...) **Europol should be able to ask** Member States, via their national units, to request private parties (...)"*.

- *Article (1)(12)(d) (new Article 26(6b) of the Europol Regulation)*

LV notes that so far no clear answer has been provided to the questions (1) on Europol's rights to access personal data exchanged between the competent authorities and private parties on crimes falling in the scope of the objectives of Europol and (2) on the specific Europol's infrastructure to be used for such exchanges between the competent authorities and private parties. In view of this, LV **continues having concerns** with regard to the relevant provision.

Thematic bloc **III**: strengthening Europol's role on **research and innovation**

- *Article (1)(2)(d) (new Article 4(4b) of the Europol Regulation)*

As far as the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 is concerned, LV notes that **information on the possible Europol's role in the screening process provided to date has not been convincing enough.**

Thematic bloc **VII**: clarifying that Europol may request the **initiation of an investigation of a crime** affecting a common interest covered by a Union policy

- *Article 1(3) (amended Article 6(1) of the Europol Regulation)*

LV **reiterates its reserved position** regarding the amendments in Article 6(1) of the Europol Regulation as proposed by COM. In LV view, these amendments **substantially expand Europol's rights** to request the initiation of an investigation of a crime affecting a common interest covered by a Union policy and only one Member State rather than clarify the relevant provision. LV sees that in such a way, a cross-border dimension is abandoned, as well as distribution of competences between the EU and the Members States laid down in the EU Treaties is not respected.

LITHUANIA

Lithuanian comments on thematic blocks in regards to the last working document (Brussels, 05 February 2021, Document WK 757/2021 REV 1) discussed in LEWP VTC on 08/02/2021

Block 1: enabling Europol to cooperate effectively with private parties

Lithuania would like to propose the following wording in **RED** colour.

31 recital

Member States, third countries, international organisation, including the International Criminal Police Organisation (Interpol), or private parties may share multi-jurisdictional data sets or data sets that cannot be attributed to one or several specific jurisdictions with Europol, where those data sets contain links to personal data held by private parties. Where it is necessary to obtain additional information from such private parties to identify all relevant Member States concerned, Europol should be able to ask Member States, via their national units, to request private parties which are established or have a legal representative in their territory to share personal data with Europol in accordance with those Member States' applicable laws. **Member States should assess Europol's request and decide in accordance with their national laws whether or not to accede to it. Data processing by private parties should remain subject to their obligations under the applicable rules, notably with regard to data protection.** In many cases, these Member States may not be able to establish a link to their jurisdiction other than the fact that the private party holding the relevant data is established under their jurisdiction. **In those cases when it is a need to establish (identify) the jurisdiction** ~~Irrespective of their jurisdiction~~ with regard the specific criminal activity subject to the request, Member States should therefore ensure that their competent national authorities can obtain personal data from private parties for the purpose of supplying Europol with the information necessary for it to fulfil its objectives, in full compliance with procedural guarantees under their national laws.

Article 26

Exchanges of personal data with private parties

6a. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned.

In those cases when it is a need to establish (identify) the jurisdiction ~~Irrespective of their jurisdiction~~ over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully

process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives.

Article 26a

*Exchanges of personal data with private parties in **online** crisis situations*

5. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol for preventing the dissemination of online content related to terrorism or violent extremism as set out in point (u) of Article 4(1). **In those cases when it is a need to establish (identify) the jurisdiction** ~~Irrespective of their jurisdiction~~ with regard to the dissemination of the content in relation to which Europol requests the personal data, Member States shall ensure that the competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives.

Block 3: strengthening Europol's role on research and innovation

Lithuania does not have any additional remarks.

Block 5: strengthening Europol's cooperation with third countries

Lithuania would like to ask the Commission to provide the detalization or more concrete examples of the provided new wording in Article 25 paragraph 5 „ *or categories of transfers"* . What is meant by this wording?

Block 7: clarifying that Europol may request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

Lithuania would like to ask to provide concrete examples on the situation when one MS is involved and it is requested to start/conduct the criminal investigation. We would like to support the initial wording of this Article 6 paragraph 1, according to the existing Europol manadate and Regulation.

Likewise, wording "request" Member States to intitiate criminal investigations is wrong itself and should be replaced by "offering/suggesting" to initiate investigation, as it relates to national law (Penal and Procedural Codes in particular) that clearly states the conditions under which investigation can be started.

Lithuania would like to propose the following wording in **RED** colour.

Article 6

Request by Europol for the initiation of a criminal investigation

1. In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it may suggest/can offer ~~shall request~~ the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation.

MALTA

Malta's Comments on the revision of the draft Europol Regulation

General Comments

Malta welcomes the priorities set by the Portuguese Presidency and supports the discussions to revise Europol's mandate as a response to increased operational needs and to a changing security landscape.

Specific Comments

The following comments are without prejudice to the Malta position and the substantive reservation placed on the revision of the Europol Regulation as a whole.

a) the revisions made to the draft proposal amendments in bloc 1 enabling Europol to cooperate effectively with private parties and in bloc 3 strengthening Europol's role on research and innovation (including relevant new additions to support the amendments in the blocs)

Bloc 1 - enabling Europol to cooperate effectively with private parties:

Article 2(r)

Malta agrees on the addition of a definition for 'online crisis situation'.

Article 4(1)(u)

Supports the deletion of part of the provision which hindered a clear understanding of the sub article. However, there is concern on the phrase 'relevant online content'. If this is not clearly defined, Europol may be legally obstructed to carry out its task based on interpretation.

Article 25(4) and 26(5)

Malta agrees on the linguistic changes proposed by the Presidency.

Article 26(2a)

Malta agrees on the addition of a new provision regarding non-duplication and non-interference.

Article 26a

Malta agrees on the addition of wording to reflect revised 'online crisis situation' term.

Bloc 3: strengthening Europol's role on research and innovation:

Article 4(1)(t)

Malta agrees on the addition of text which enables Europol to coordinate with other JHA agencies in the field of research and innovation in close cooperation with Member States.

Article 4(4a)

Malta agrees on broadening the scope of the sub article in relation to other research and innovation activities.

Article 33(a) and 33(c)

Malta believes that there is no added value in adding the word 'new' as the previous term 'innovative' already implies the same meaning.

Malta agrees on the addition of the wording which further safeguards against improper handling of personal data.

b) the revisions made to the draft proposal amendments in articles 7(8) concerning Europol cooperation with financial intelligence units

Malta agrees on clarifying further the legal relationship between Europol and financial intelligence units.

c) the addition of a sub article 7(12) concerning the issuance of notifications by Europol to private parties on missing information

Malta agrees on the addition of a new provision for an annual report to be drawn up on such notifications. On a linguistic point, a full stop should replace the semi colon at the end of the sub article.

d) the request by Germany for a legal opinion by the General Secretariat of the Council on the addition of a new provision which exempts Schengen Associated Countries from article 25 of the draft proposal

Malta agrees that a legal opinion is delivered by the General Secretariat of the Council to Member States for further examination of the German proposition.

e) the addition of a new task enabling Europol to submit alerts on the Schengen Information System (SIS) on the suspected involvement of third country nationals on offences within the Agency's mandate

Malta would like to continue placing a substantive scrutiny reservation on this aspect as further internal discussions at a national level are required.

f) the clarification on article 6(1) of the draft proposal whereby Europol may request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

Malta acknowledges the reasoning behind the Commission's amendment to sub article 6(1). As the provision currently stands, there is the possibility of a legal ambiguity which may impede Europol from fulfilling its task under article 3(1) of the current Europol Regulation. Article 6(1) requires the presence of two or more Member States when Europol requests the initiation of a criminal investigation of a crime affecting a common interest covered by a Union policy. Such crimes do not necessarily require a cross-border dimension to occur. As a consequence of this, Europol may be obstructed from supporting and strengthening Member State action and mutual cooperation in preventing and combatting such forms of crime. For this reason, Malta in principle considers this

proposal with a positive scrutiny and looks forward to further discussion between Member States and the Commission.

NETHERLANDS

Comments of the Netherlands on the proposal amending the Europol Regulation, following the LEWP of 8 February 2021

The Netherlands appreciates this opportunity to submit its comments on blocks 1, 3, 5 and 7. We very much appreciate the clarification that a Member State can refuse a request from Europol to obtain information from a private party in recital 31, that there will be no overlap between the cooperation of Europol with private parties and the activities of the FIUs through the insertion of a new paragraph 2a in article 26 and that article 26a only refers to online crisis situations. We are also grateful that the presidency has agreed to discuss the question whether Europol should be able to insert alerts in SIS at the LEWP meeting on 22 February. Please find some questions and comments from our side below. As we are still studying several aspects of the proposal, we reserve the right to make additional comments at a later moment.

1) Comments on the text

Block 1 Enabling Europol to cooperate effectively with private parties

General questions

- How can we ensure that on the rare occasions that Europol shares personal data with private parties, they do not forward it to another organisation? Should private parties be able to forward personal data they have received from Europol? Article 23 paragraph 7 of the Regulation says that: "Onward transfers of personal data held by Europol by Member States, Union bodies, third countries and international organisations shall be prohibited, unless Europol has given its prior explicit authorisation." Why are private parties not included in this paragraph? What reasons could there be for private parties to forward personal data?

Our text proposal for article 23 para 7 is:

"Onward transfers of personal data held by Europol by Member States, Union bodies, third countries, and international organisations and private parties shall be prohibited, unless Europol has given its prior explicit authorisation."

- Should we maybe include a stipulation that the MB will establish further guidelines or conditions for the exchange of information with private parties? These could for example specify how Europol can decide whether to forward information it has received from private parties to third countries or international organisations under article 26 para 2, how Europol can decide whether to request Member States to obtain personal data from private parties under art. 26 para 6a and art. 26a para 5 or how Europol's infrastructure may be used for exchanges between MS and private parties (art. 26 para 6b).

Article 7 para 12

- We have two suggestions for additions to the current text (although we are not sure why the text describing the report is different here from that in article 51 para 3 sub f):

"Europol shall draw up an annual report on the number of cases in which Europol issued notifications to private parties on missing information in accordance with point (d) of paragraph 5 of Article 26 or requests **to** Member States to obtain personal data from private parties in accordance with paragraph 6a of Article 26 **and paragraph 5 of Article 26a**, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks;"

- Furthermore, we think that the MB should not only receive the document that is described in article 51 para 3 sub f, but all the documents that the JPSG will receive.

Article 26(2)

- The Netherlands appreciates the fact that the goal of receiving information from private parties has been limited to identifying member states. We agree with the Commission that Europol is there to support MS, not third countries or international organisations.

- Do the "national units concerned" automatically include the ENU of the Member State where the private party has been established?

- The Netherlands supports replacing "or" with "and", as proposed by Italy.

Article 26(6a) (en 26a lid 5)

- What does the new sentence in recital 31 mean that says: "Data processing by private parties should remain subject to their obligations under the applicable rules, notably with regard to data protection." Which applicable rules does this refer to?

- Recital 32 stipulates that when Europol has received data from a private party in response to a request to a Member State to obtain this data and cannot expect to identify any further MS concerned, it needs to delete the data within 4 months after the last transmission had taken place. But where paragraph 2 of article 26 explicitly mentions this retention period, paragraph 6a does not. Maybe the relevant text from paragraph 2 should be included (i.e.: "Once Europol has identified and forwarded the relevant personal data to all the respective national units concerned, and or it is not possible to identify further national units concerned, it shall erase the data, unless the national unit concerned resubmits the personal data to Europol in accordance with Article 19(1) within four months after the transfer takes place.")?

- We might also consider including another sentence from paragraph 2 in article 26(6a), namely: "Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the national units concerned." (subject to article 19(2) of course).

Article 26a

- Should article 26a contain a provision on a retention period? It seems to be a specialised version of article 26, which does contain its own retention period.

- We are still studying article 26a, so further comments on this may follow later.

Block 3: Strengthening Europol's role on research and innovation

Article 4(1)(t)

How would we decide who gets the intellectual property of the innovations, including the algorithms, that are developed? Should we include something about this in the Regulation, for example that the MB will establish rules for this? Will all MS get access to the source codes of the innovations that are developed by or in cooperation with Europol?

Article 4(4b)

We are still studying the proposal for Europol to support the screening of foreign direct investments, so our comments on this will follow later.

Article 18(2)(e)

Could Europol hire (sub)contractors to process data for research and innovation, or is "Europol staff" limited to staff directly employed by Europol itself?

Article 18 para 5a

Since the processing of data for research and innovation under para 2 sub e has been excluded from paragraph 5 of article 18, we are wondering whether it should also be excluded from paragraph 5a? The aim of processing under 5a is to determine whether the data complies with the requirements of para 5, but this no longer applies to para 2 sub e.

Article 33a

- Which personal data will Europol use for research and innovation? The personal data that is already in its systems? Is Europol allowed to use data for research and innovation that has been shared with it for other purposes?

- We agree with the Belgian suggestion to include an explicit reference to a preference for synthetic/anonymised data in art. 33a and/or recital 39.

- Para 1 sub f: We understand that using the word "erase" is preferable to using the word "delete".

Block 5 Strengthening Europol's cooperation with third countries

Article 25 para 5

- We would like to see a clarification that "categories of transfers" refers to a number of transfers related to one event. Maybe "categories" could be defined?

- We would appreciate it if we could receive a written opinion by the CLS on the German proposals for cooperation with third countries.

2) Questions to Europol

Block 1 Enabling Europol to cooperate effectively with private parties

Article 26(2)

In the amended version of this article, the only aim of Europol receiving personal data directly from private parties is to identify all national units concerned. After it has forwarded the personal data to those national units, it will erase the information, unless it is resubmitted. It therefore seems that the intention of this article is that Europol receives the information on behalf of the national units concerned and then transfers ownership of the information to them. Once the national units concerned are the owners of the information, they can put restrictions on access to that information when they resubmit it.

However, in addition to those national units, Europol can also provide the information to third countries and international organisations. Since the aim of this article seems to be to transfer ownership of the information to the national units concerned, we were wondering whether Europol consults those national units before forwarding the information to a third country? What would happen if a Member State would resubmit the data with the restriction that it cannot be forwarded to third countries, but Europol has already done so? Is it desirable for Europol to forward the information to a third country before consulting the MS, or could that lead to problems for the MS concerned? Europol seemed to suggest during the meeting that it mainly intended to contact third countries in order to obtain data to be able to identify the members states concerned. Is that the intention of this article or will third countries also be sent the information for other reasons?

Article 26(6a)

When does Europol expect to use this provision, that is: what kind of requests for information does Europol expect to make to private parties through the national units?

POLAND

General remarks

Poland positively assesses the support provided by Europol to the competent national authorities so far, while recognizing the possibility of introducing further improvements in its functioning. Poland is of the opinion that it is necessary to maintain the supportive role of Europol, while respecting the exclusive competences of the Member States.

Poland still raises the parliamentary reservation due to the ongoing consultations at the national level. We reserve our right to express further remarks and comments at a later stage of discussion and during the next LEWP VTCs

COMMENTS

On page 24 of 5388/1/21 REV 1, Article 4

4b. Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security.*	Comment: We suggest deleting this point. In the opinion of our experts Europol should not play an active role in the process of screening foreign direct investment. This provision enables Europol to seek active role in the process of screening foreign direct investment into the EU which may disort the balance between the Europol's scope of competence and the issues falling within the category of the exclusive competence of the EU Member States in accordance with art 4 (2) of the Treaty on EU. The process of screening foreign direct investment is closely related to security-sensitive area such as critical infrastructure, dual use items or critical technologies, listed in art. 4 regulation (EU) 2019/452 establishing a framework for the screening of foreign direct investments into the Union. Taking into account the specific nature of the activities carried out by the competent national authorities in these areas, the practical dimension of such cooperation between these authorities and the Europol may prove to be problematic due to the fact that it touches upon economic security of the EU.

On page 25 of 5388/1/21 REV 1, Article 6

(3) in Article 6, paragraph 1 is replaced by the following: *"1. In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation."*	*Comment:* In the light of the results of the discussions at LEWP on 08.02 and in connection with our previous comments on the preservation of the supporting role of Europol and the exclusive competence of the member bodies in the area of initiating investigations, we propose to abandon the amendments and keep the current content of this article.

On page 25 of 5388/1/21 REV 1, Article 7

(4bis) In Article 7, the following paragraph 12 is added: ***"12. Europol shall draw up an annual report on the number of cases in which Europol issued notifications to private parties on missing information in accordance with point (d) of paragraph 5 of Article 26 or requests Member States to obtain personal data from private parties in accordance with paragraph 6a of Article 26, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks;"***	*Comment:* In our opinion, it could be considered to supplement the provision with names of the institutions to which the report will be addressed.

ROMANIA

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

RO comments on doc. 5388/1/21 REV 1 and blocks 5 and 7

- **Doc. 5388/1/21 REV 1. We are maintaining the previous observations on blocks 1 and 3 as are mentioned in RO written comments (doc 5527/1/REV 1). Furthermore on block 3, Art. 18 (2)(e)[1], additional information/clarifications are needed on what other research and innovation activities have been taken into consideration as the term *"other"* does not provide sufficient clarity to the text.**

- **Block 5: strengthening Europol's cooperation with third parties**

Recital 24: *Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries* ***in specific situations*** **and on a case-by-case basis***, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation.*

It is not clear what those specific situations are. It is necessary to define them, as well as the criteria for analyzing the respective situations (case-by-case basis). Clarifications are also needed on the authorization of the transfer of personal data to third parties (Europol's Executive Director level).

Art. 25 (5)[2]. Additional information / clarifications are needed on what was taken into account when the phrase "*categories of transfers*" was used and if the current wording of art. 25 (5) of Regulation (EU) 2016/794 does not already cover transfer situations to third countries or international organizations.

[1] Art 1 (5) (a) (ii) reference in proposal COM (2020) 794 final
[2] Art 1 (11) (a) reference in proposal COM (2020) 794 final

Art. 67, para 1: Member States control over the transferred data (as originators) and compliance with the third party rule are necessary elements in the process of transferring personal data to third countries. In this regard, we propose the following addition on this Article:

Any administrative arrangement on the exchange of classified information with the relevant authorities of a third country or, in the absence of such arrangement, any exceptional ad hoc release of EUCI to those authorities, shall be subject to the Commission's prior approval ***and shall be carried out in compliance with third party rule*****.**

- **Block 7: clarifying that Europol may request the initiation of an investigation of a crime affecting a common interest covered by a Union policy**

Recital 13: *Europol provides specialised expertise for countering serious crime and terrorism. Upon request by a Member State, Europol staff should be able to provide operational support to that Member State's law enforcement authorities on the ground in operations and investigations, in particular by facilitating cross-border information exchange and providing forensic and technical support in operations and investigations, including in the context of joint investigation teams. Upon request by a Member State, Europol staff should be entitled to be present when investigative measures are taken in that Member State and assist in the taking of these investigative measures. Europol staff should not have the power to execute investigative measures.*

Recital 14: *To strengthen that support, Europol should be able to request the competent authorities of a Member State to initiate conduct or coordinate a criminal investigation of a crime, which affects a common interest covered by a Union policy, even where the crime concerned is not of a cross-border nature. Europol should inform Eurojust of such requests.*

Art 6, para 1: *Request by Europol for the initiation of a criminal investigation*

In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member State or Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation.

Similar to FR position (doc. 5527/21), it is unclear how Europol staff will assist Member States in undertaking investigative measures (recital 13).

From the counter terrorism perspective, we consider that Europol's mandate and role must respect the limits set by the Treaties, namely supporting the action of police authorities and cooperation between them. By strengthening the Agency's capacity to request the initiation of transnational investigations, these limits are exceeded, with Europol being given a coordinating role.

The same position is underlined by FR and DE (doc 5527/21).

In this case, too, we consider it necessary to clearly define the criteria on the basis of which Europol takes the decision to initiate an investigation, namely the way in which the Agency will support the work of the MS on this component. By initiating such investigations, there could be a duplication of the efforts of the competent authorities.

SPAIN

Follow-up comments to the last LEWP meeting (08/02/2021)

REVISION OF THE EUROPOL REGULATION

EXAMINATION OF THEMATICS BLOCKS 1 AND 3

- **On interpretation of article 7.8 and possible dysfunctions of financial intelligence units**

With regard to Article 7.8, it is specified that the cooperation of the above-mentioned Financial Intelligence Units (FIUs) may cooperate with Europol within the terms and limits set by the national units and always within their competences as laid down in Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules to facilitate the use of financial and other information for the prevention, detection, investigation or prosecution of criminal offences.

In particular, Chapter IV of the above-mentioned Directive on Exchange of Information with Europol, and in particular Article 12 thereof, which provides that each Member State shall ensure that its FIU is empowered to respond to duly motivated requests made by Europol through the Europol national unit or, if permitted by that Member State, through direct contacts between the FIU and Europol. This is within Europol's responsibilities and for the performance of its tasks. In this regard, it is considered that the wording of this article is appropriate and respects the interests of Spain, being consistent with our legal system and regulations regarding the entity responsible for the management of the Financial Titles File (FTF), which is SEPBLAC

- **On Article 4(1), point (m):**

In general, it is considered appropriate but should be included after "cooperation", "and under consent of member states"

- **On Article 4.4b:**

Europol's supporting role should be further defined.

- **26.5.d :**

It is considered appropriate to include, together with the mention of the national units, the contact points and competent authorities.

- **On Article 26.6a:**

There must be possibility of choice for Member States to refuse a request to share private data.

- **On Article 26.6b:**

A clarification should be made: it follows from the proposed wording that, in cases falling within Europol's objectives, the agency will have access to personal data exchanged via its infrastructure by Member States with third parties, which may pose problems from a data protection point of view. Member States should be able to use Europol's infrastructure to exchange data in a secure way, without the agency being able to access them (under national authorities' criteria). EDPS should be consulted on this.

- **On Article 26.b:**

It is considered appropriate to add this article proposed by THE FRENCH DELEGATION.

- **On Article 33.a:**

EDPS should be consulted on the use of personal data and the data protection regulations of the Member States should be assessed. In any case, the use of synthetic data should be prioritized whenever possible.

INITIAL EXAMINATION OF THEMATIC BLOCKS 5 AND 7

- **Strengthening Europol's cooperation with third countries**

Relating to strengthening Europol's cooperation with third countries, regarding article 25.5, we propose for clarify a definition of "category of transfers" and included this definition in Art. 2.

- **Clarifying that Europol may request the initiation of an investigation of a crime affecting a common interest covered by a Union policy**

Pertaining to clarify the role of Europol in the request for the initiation of an investigation into offences affecting the common interests of the Union, our position of this refers to the article 6 Europol Regulation (REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2016). In this sense, it is considered that this Article provides sufficient legal cover to request the initiation of investigations and therefore it is not considered necessary to amend the regulation to this effect.

4. COMMENTS RECEIVED AFTER THE MEETING ON 22 FEBRUARY 2021 (BLOCK 4)

BELGIUM

Written comments of Belgium about proposed SIS alert by Europol following the LEWP meeting of 22 February 2021

We are thankful to the Portuguese Presidency for continuing to create the necessary space to focus on the principles underlying the proposed SIS alert by Europol and to find a common ground among Member States before diving into the articles. Belgium has expressed at several moments throughout the preparatory process some concerns, especially on principal grounds, related to this proposal. **These concerns are in essence two-fold: there is the unclear operational added value, and there is the unclear and/or unwanted impact of this proposal.**

The unclear operational value, is our main issue. We have consulted our Belgian partners and we have **a lot of difficulty imagining the concrete situations in which it would be useful for frontline officers to receive certain information they need and are supposedly not receiving, especially taking into account the fact that alerts can be issued for the whole of Europol's mandate**. We are trying to see the gap as well as the nature of this gap, that the Commission sees. Although the Commission's explanations sound logical in general, our frontline officers and SPOC operators do not see it. That is why we keep insisting on having this gap explained. Because otherwise, we cannot successfully determine whether this proposed solution is adequate to solve the problem.

One of the issues we have always brought forward is the **big risk of duplicating the Interpol alerts**. The Commission previously stated that these alerts are not always visible to the frontline offers in Member States. As previously stated, in Belgium all Interpol alerts and notices are visible to our frontline officers. So you can understand that we are worried to which degree the Europol alerts will create double hits for our frontline officers and to what degree it will cause a duplication with the Interpol alerts. If the proposal is trying to ensure the availability of "Interpol" information to frontline officers, this would of course mean a very strange way of ensuring implementation of the appropriate and best way to move forward; namely improving the availability of Interpol alerts. And also, how big is this Interpol gap? How many countries are we talking about? We would very much welcome clarifications on how the duplication of Interpol alerts and these new SIS alerts by Europol will be handled.

Another important issue for us is the **very new and vague kind of responsibility that is placed on the MS**. MS and their frontline officers will have to decide which action to undertake based on a lot of unclarity and in an indirect manner, but with the responsibility of adequately responding. We are not sure if this corresponds to one of the important principles mentioned in the JHA Declaration on the future of Europol: **Europol should support the MS' investigations**. The protocol developed by the Terrorist Working Party and endorsed by COSI to deal with lists of third countries on non-EU Foreign Terrorist Fighters on the other hand does clearly follow the principle of MS being in the lead of SIS alerts. Next to this, the responsibility of each MS to adequately respond to this proposed alert by Europol will result in a **diverse implementation at the national level of each MS.** Thus we will have a big risk at fragmentation.

Or do we have to see this alert as an **incentive to start proactive investigations or as an open suggestion to assist a third country** in their investigation, but thus without a clear interest for the MS themselves? If this is the case, however, MS should not receive this message in the form of an alert, which is an instrument to ask for a specific and needed concrete action. The Schengen Information System derives its strength and its credibility from dealing with actionable information, from alerts requiring concrete action. Or maybe the proposal attempts to mainly provide an **extra monitoring tool for travel movements** of third country nationals? Although it sounds surely interesting for third countries, do we want third countries and Europol to use SIS for this end? We are most likely talking about cases with no clear link to a certain MS. We are afraid this **could open the door for misuse**.

Do we want to change to SIS for these ambiguous purposes instead of looking into the **upcoming Interoperability framework and all the databases** the EU has been creating so intensely? The Commission announced that an impact assessment of the recent ETIAS and VIS amendments will follow. We want to stress the importance and necessity of taking a close look at the ETIAS watchlist. This ETIAS watchlist namely has a lot of similarities in relation to the source and content of the information, the scope of the third country nationals concerned as well as the described objectives. A lot of questions thus arise about the added value and the overlap between these two instruments. How will Europol decide on whether to introduce the proposed SIS alert or rather using the ETIAS watchlist? Also, if such a SIS alert is supposed to take precedent, this will most likely affect the actual "raison d'être" of the ETIAS watchlist.

All these concerns hopefully clarify why we are very doubtful about the operational value and why we are uncomfortable about the unclear and unwanted effects and impacts. We should only undertake this radical change to SIS if no other and better suited means are possible. That is why it is essential to have a thorough gap analysis and impact analysis which includes all these elements described above. Because otherwise we risk **undermining the strong, clear, useful and above all operational instrument** that SIS is, and turning it into a channel for information exchange with unclear benefits for the MS.

Another very important reason why all this remains so unclear is because we have little indications of how Europol will handle all the creation of alerts; **which criteria will Europol use to decide to start the procedure to enter a for information alert? What's the minimum threshold and especially where does it stop?** Europol will also have to determine the reliability of the information (which also may include whether the third country information concerns intelligence information) while the MS are often better placed to determine this aspect. Currently the MS themselves use SIS based on solid legal grounds, a solid national investigation, most of the time solid national links and often with a magistrate involved. We have policies and working processes to this end. How will Europol handle these decisions? Which thresholds will they apply? Moreover, how can one assess at all the necessity of an alert without an action to be undertaken linked to it?

In conclusion, we have a lot of questions mainly directed at helping us decide whether or not there is sufficient operational value to the proposal. **First and foremost, we need to better understand – on a concrete operational level – the specific, actual gaps.** We need clear answers of the Commission to the questions and unclarities raised above, preferably in written form. Once these answers are available, we are interested in participating in a **constructive debate in searching for the most appropriate solution** – taking into account Europol's tasks and the characteristics of our SIS system – and we are willing to join other MS that are also willing to do so.

BULGARIA

Bulgarian contribution to the draft Regulation amending Regulation (EU) 2016/794, as regards to enabling Europol to enter data into the Schengen Information System (Block 4)

Bulgaria agrees that there is an operational need to make verified third-country sourced information on terrorists and other criminals available to frontline officers.

Without any doubts, the Schengen Information System is the most widely used system by the front-line police officers. In this regard it could be considered that SIS is the right tool to make this information available to frontline officers.

We could agree that there is a clear need to overcome the security gap, related to the large amount of data on criminals and suspects, mainly foreign terrorist fighters, who are not accessible to the Member States because they are not entered in the SIS. It could be done by entering this information in the SIS, but we should find the most appropriate solution on the modalities of this approach.

As stated in the Explanatory Memorandum of the European Commission, Europol has the above-mentioned information. Therefore, the current proposal could provide a real benefit and positive effect on increasing the level of security in the EU, as well as enhancing the effectiveness of the largest European data base in the field of security – SIS. Nevertheless, up to the moment there are many issues of concern by the Member States which do not allow us to fully support the draft Regulation amending Regulation 2018/1862. But we are ready to further discuss and find possible compromise solutions.

In this regard, we have several comments on the text:

1. The introduction of new category of alerts - we propose **not** to introduce a new category (Alerts entered by Europol on persons of interest), but to use the current provisions of the SIS Regulation. Europol should be able to introduce alerts **only under Art. 36, para 2**[1] **with a measure "discreet checks" for persons third-country nationals** (Alerts on persons for discreet checks). First, this alert will provide the possibility for collecting information which is in line with the tasks of the Agency under Art. 4 (1) (a)[2] of the Europol Regulation. And secondly - the measures under this alert, which are clearly described, are close to the concept of the proposed measures in the new art. 37b of the SIS Regulation. Thus, there will be no confusion regarding the procedures and measures to be applied by the end users.

---

1 When entering alerts for discreet checks, inquiry checks or specific checks and where the information sought by the issuing Member State is additional to that provided for in points (a) to (h) of Article 37(1), the issuing Member State shall add to the alert all the information that is sought. If that information relates to special categories of personal data referred to in Article 10 of Directive (EU) 2016/680, it shall only be sought if it is strictly necessary for the specific purpose of the alert and in relation to the criminal offence for which the alert has been entered.

2 Article 4 Tasks
1.Europol shall perform the following tasks in order to achieve the objectives set out in Article 3: (a) collect, store, process, analyse and exchange information, including criminal intelligence

The added value for the Member States will be not so much the existence of a hit in the SIS, but the **sharing of useful and relevant information with the national competent authorities**, which would help them to prevent the commitment of serious crimes. In this regard, we suggest in the post-hit procedure to be added that Europol shall carry out additional checks in its databases after the Agency has been notified for a hit on its alert. The summarized/ analysed information should be shared with the competent authorities of the MS where the hit is identified. If other Member States are identified during the subsequent processing of the hit information, they should also be notified.[3] For example a person subject of Europol alert under art.36.2 is entering in Bulgaria accompanied by a person who is German citizen or has a permission for stay in Germany. In this case Europol during the subsequent processing of the hit information should inform Bulgaria and Germany and should provide both countries with the collected and analysed information.

In all cases, end-users will benefit if the alerts entered by Europol are only under **Article 36, paragraph 2 "discreet checks":**

- at the first line / border control - there will be no change in the working processes;

- when the MS investigating officers make a search in the SIS and identify that there is an alert entered by Europol, they will know that the Agency has information on the person and will be able to request it and thus support their investigation.

Last but not least, as an argument it can be pointed out that by avoiding the introduction of a new category of alert for Europol, but providing the right to enter alerts only under Article 36, paragraph 2, "discreet checks", it will not be necessary to change the current procedures with small exceptions.

2. The quality of the data entered / consultation procedure before entering an alert - we believe that the procedures proposed by the EC to ensure the quality of the data and the preliminary consultations before entering an alert by Europol in the SIS in Article 37a, paragraph 3 are in the right direction, but more guarantees for the data completeness are needed. It is important for us, reliable mechanisms to be provided in order to ensure the completeness and accuracy of the information received from third countries and organizations. As a front-line MS located at the transit routes of foreign fighters, this issue is of particular importance for us.

With regard to the **pre-alert consultation procedure**, some questions arise:

The current proposal[4] should be implemented through the Europol National Units under Article 7 of the Europol Regulation, but the question arises in case consultation is needed with the Schengen associated countries, which do not fall within the scope of Article 7 of the Europol Regulation and should be considered as third countries, as in the case of Denmark.

In addition, the SIRENE Bureaus operate 24/7 and the ENU do not. In case of an urgent need for a consultation procedure for entering an alert by Europol in the SIS, how will this be done? If there are deadlines for the consultation procedure it will be a challenge.

---

3 Which can be done by an explicit entry in the SIS Regulation or based on Article 22 of the Europol Regulation

4 In both Europol Regulations (art.4, para.1 new letter (r)) and for SIS (art. 37a, para 3, letter (d))

3. Duplication with the already agreed Protocol in the Terrorism WP for entering data from third countries on terrorism.

We support the European Commission's desire to have a long-term solution to the issue of entering data from third countries regarding foreign fighters. From our point of view, duplication with the Protocol already agreed in the Terrorism Working Party can be avoided, if Europol will introduce information received from third countries with which it has an agreement for operational cooperation. Member States could enter information from other third countries except those with which Europol has agreements, such as the MENA countries.

We would like once again to emphasize the necessity of qualitative and reliable data.

In addition, as another compromise solution, we propose to be considered, the Europol's right to enter alerts in the SIS to be initially limited only to alerts on terrorism-related activities (again only under Article 36, paragraph 2 "discreet checks"). After a certain period of time, the use of this instrument can be analysed and evaluated, and then its scope can be extended to include other offenses under Europol's mandate.

Based on the above, we believe that if a compromise solution is found to the outlined issues, the introduction of Europol alerts in the SIS would have added value in enhancing security in Europe.

Finally, Bulgaria supports the proposal of the Netherlands to have an Ad Hoc working group for discussing SIS and Europol related issues. In order to ensure the best possible effectiveness of this format, we believe that the Presidency and the Commission should present concrete provisions as alternative of the current text, in order to serve as a basis for the forthcoming discussions.

CROATIA

Following up to the meeting of LEWP on 22 February, attached to this message please find enclosed the comments from the Republic of Croatia related to:

5397/21

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

- block 4: enabling Europol to enter data into the Schengen Information System

It is indisputable that a third country's verified information on serious crime and terrorism should be made available to police officers in the field. This is why it has already been realized in Croatia through connecting the Ministry of the Interior Information System with the INTERPOL I24/7 system. Please note that this solution is applicable in all the other Member States, including SAC-Countries, since they are all INTERPOL member countries as well. In fact, most of them have this solution already implemented as this is the simplest solution to the issue.

However, in looking at a bigger picture of the comprehensive fight against organized crime and terrorism, we believe that it is not sufficient to provide police officers in the field with the access to information received form the third countries. Instead, the Member States should systematically exchange with Europol the new information emerging from activities performed based upon the initial information, and for the purpose of further analysis processing on the part of Europol. Since the SIS II is the primary choice for communication and exchange of information by police officers in the field, we believe the only logical solution would be to use it for the above mentioned purpose. In this respect, we support the proposal of the European Commission.

Furthermore, we believe that most of the remarks made at the meeting were unclear or unfounded. There is undoubtedly a legal basis in place for police action in each Member State, because the police powers include checking the information received irrespective of its source. Police action is also unambiguous because the conduct of the so-called discrete checks is expected. Moreover, the added value is unquestionable as well, for the reasons stated above. Regarding the remarks made, the ones we support are those pertaining to the need to exactly determine conditions under which Europol could forward the new information received from a Member State to the third country that has sent the initial information to Europol.

CZECH REPUBLIC

Following the informal videoconference of the members of the Law Enforcement Working Party (LEWP) which was held on 22 February 2021, please see the written comments of the Czech Republic:

7) Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation (doc. 5388/1/21 REV 1, 5397/21)

Regarding question number 1, CZ agrees there is an operational need and sees it as very important to make verified third-country sourced information on terrorists and other criminals available to frontline officers.

Concerning question number 2, we do see the SIS based solution to be effective in covering the existing gap in the area of fight against terrorism. This has been proven in the past, when the CZ voluntarily supported the EU by entering alerts in SIS based on information from Western Balkans, which has been since bringing lot of important operational information. The present proposal is a logical next step, which will reduce the workload of MS and will bring necessary systemic and on-time approach filling the already mentioned gap.

Finally, during the videoconference, multiple options and next steps regarding further discussion of this topic were suggested. The CZ is of the opinion that before we discuss this matter further at LEWP, all the questions raised by member states should first be clarified either by written procedure or at the IXIM working group.

ESTONIA

Estonian written comments (22.02.2021 LEWP – Europol alerts on SIS)

1) **Do you agree that there is an operational need to make verified third-country sourced information on terrorists and other criminals available to frontline officers (border guards and police officers) in order to detect those persons when they seek to cross EU external borders or when they are being checked within the EU?**

Regarding the first question, of course it is important. And in our opinion on Estonian external border such information is already available, if it's put into Interpol's database. Therefore for us such information would be duplication.

2) **If so, do you agree that the Schengen Information System is the right tool to make this information available to frontline officers (border guards and police officers)? If not, what alternative solution would you propose?**

Regarding the second question, if such information is not inserted into Interpol's databases, what is the reason behind it? Our opinion is, that we don't need an alternative solution, we already have a functioning mechanism.

Also we recall, that TWP discussed last year a list of potential foreign terrorist fighters. The solution that MS agreed upon was that MS verify the list and insert the information into SIS on a voluntary basis. International cooperation and verification process. Now it's said, that Europol has information about 1000 potentially crime-involved persons, which, possibly, could not have been verified. Are there estimates on how many of these 1000 already are inserted into Interpol databases? And considering the numbers, are these investments reasonable? It's unclear, how many such alerts there would exist in the future.

If the amount of such possible notifications would be high (in thousands), the administrative burden for Europol would be significant and there are much more pressing needs for Europol to focus its resources.

And finally, the difficulties in implementation, since the post-hit procedure is unclear. It's required, that MS has to explain, why specific action was taken post-hit. Therefore it's also not clear, based on which internal legal acts we could take various measures regarding that person, if there is no on-going investigation and it's, as stressed, just for informative purposes.

To conclude, unfortunately, Estonia is not convinced is the proposals necessity because in our opinion there is no proper problem here to solve. If MS agree, that there is a problem, maybe one option could be to make such information available in Europol's database and try to solve it there.

FRANCE

NOTE DE COMMENTAIRES DES AUTORITÉS FRANÇAISES

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leurs commentaires écrits suite à la réunion de groupe LEWP du 22 février 2021.

S'agissant de la proposition de règlement du Parlement européen et du Règlement modificatif du Conseil (UE) 2016/794, concernant la coopération d'Europol avec les parties privées, le traitement des données personnelles par Europol en appui des enquêtes pénales et le rôle d'Europol dans la recherche et l'innovation *(5388/REV1/21 ; 5397/21) :*

Les autorités françaises prient la Présidence de se référer au Non papier élaboré sur le sujet. Outre le fait que celui-ci rappelle notre opposition à ce qu'Europol puisse se voir conférer un rôle d'alimentation du SIS, ce non papier a la vertu de formuler un certain nombre de propositions alternatives visant à combler les lacunes exposée par la Commission.

GREECE

Following the debate during the last VTC on Feb. 22nd, and with view to the next upcoming one, please find below our comments/contribution regarding Block 4: enabling Europol to enter data into the Schengen Information System:

"Greece proposes the deletion of section r, para 1 of Article 4, following concerns, reservations and remarks from most of the Member States during the 22nd Feb. 2021 LEWP VTC.

Following your questions referred to your Flash Note, definitely we agree there is an operational need front-line officers to have all information available; that stands as an imperative from our experiences as a front-line Member State. However, in this regard we highlight the fact that there is a significant difference between availability and accessibility to information.

Further, the discussions within LEWP and the debate concerned are about reviewing Europol's Regulation, the Agency's new mandate. To this end, efforts should focus on what, how and why Europol will support Member States. This exercise focuses on what authority we shall give the Agency to fulfill its mission; and again, allow us to stress that every form of authority equals to specific extend of responsibility.

Consequently, the given concerns and queries from Member States during the last VTC are fundamentally valid. Allow us to recall, some:

- *What is meant with consultation at the referred provision of the Article?*
- *Are the information received by Article 17(1)(b) alone enough, as a criterion for the Agency to enter data ti SIS II? Following, are this data valid, cross-checked and verified and who is competent to confirm so?*
- *In a positive case, who is responsible for handling the case? Europol or the Member State? We should not neglect that for every measure on SIS II, there is a national legally binding decision, which is not the case for Europol.*
- *In case of an appeal and respective legal consequences, who is responsible for the judicial proceedings and jurisdiction for the case concerned?*
- *And many other important ones raised throughout the 22.02.21 LEWP VTC.*

The outcome of this debate was, and remains, more or less evident; Member States are hesitant to permit this authority to Europol. This applies to the next and second question of your Flash Note, if SIS II is the right tool to avail information to front-line officers. The answer leans to be positive; nevertheless, if Europol will be able to add data onto it is another case.

Concerning national position on the subject matter, SIS II is one of the main tools for such tasks and to this end we add the added value of Interpol databases, that long pre-exist and remain rich and updated. We do consider that Member States do efficiently cooperate in this matter and exchange information and the respective "Interpol Notices" in a satisfying manner that cover needs. It is kindly noted that these notifications can easily be employed also for the provisions of Articles 36 para 2 and para 3 of SIS II, while direct communication and exchange (with no third party involvement) proves faster, while not resource-effort-time consuming.

Additionally, significant work and progress has been achieved at the interoperability project; which, actually serves the same purpose, the interconnectivity of databases (including entry/exit, VIS, SIS II, etc) for the viability of information. Worth mentioning though, the funds and efforts (also at the legal and technical) level invested for this project.

Concluding, in the future debate, we expect the Presidency to acknowledge the volume and extent of Member States concerns and hesitance, and to assist in the the consultations with the Commission to clarify between the "benefit" and the "necessity" of the questioned authority to Europol.

The more, is not always the better. SIS II derives from the fundamental Conventions of the EU and built to be used and serve Member States, as political entities within the international and European community, governed democratically and embodying legislative, executive and judicial authorities. We shall ensure Europol supports Member States, without allow it to behave like one."

IRELAND

Please find below, the written official response from Ireland on the questions posed by the proposal for Europol to enter SIS alerts.

Question 1 - We could agree that there is an operational need, but highlight a need for clarity in terms of how this need can be progressed.

Question 2 - SIS II has the network and automation to best present instantaneous information to law enforcement end-users. However, governance of information from third-countries needs to be specified and detailed in regulations. In this regard SIS Recast will be a better option.

ITALY

On behalf of the Italian Delegation please find attached the Italian follow up contribution to the meeting of 22 February 2021 on the General discussion regarding block 4: enabling Europol to enter data into the Schengen Information System.

General discussion regarding block 4: enabling Europol to enter data into the Schengen Information System

ITALIAN Contribution

In relation to the discussion that took place on the 22 February meeting within the LEWP on the Reform of the SIS Regulation 1862/2018 and consequent amendments to the Europol Reg. 796/2016, Italy considers essential to timely address the current information gap.

The Commission's proposal to involve Europol in the process of sharing verified information from reliable third countries through SIS has the undoubted advantage of offering a solution of the gap avoiding further delays.

However, the information gap concerns in particular data on terrorism from third countries.

Italy therefore believes that the information involved in the Proposal should only involve terrorism data.

Furthermore, in order not to alter the operational functioning of the SIS system, we believe that it is necessary to make some substantial changes to the Proposal with reference to the data verification process and to the actions to be taken by the tracing States.

In summary, Italy:

- Supports the continuation of the discussions on the Commission Proposal on the block 4, in order to reach a solution of the information gap in a reasonably short time.
- Highlights the need to make changes to the text of the Commission's Proposal in order to minimize the impact on the SIS general principles, the overall architecture and on its action to be taken framework.
- Considers it necessary to limit Europol's power to issue alerts in the SIS to data from reliable third countries;
- Considers it necessary to limit the alerts issued by Europol in SIS to data relating to terrorism only and not all crimes covered by Europol's mandate
- Stresses the need to provide only information-based actions for the tracing State, eliminating any reference to further actions to be taken by the States according to national law, which could entail differentiated and non-homogeneous actions by the tracing States and operational uncertainties for the front line agents.
- Considers it necessary to define and foresee in the text of the Proposal rigorous verification processes, especially of a qualitative nature, on the data of third States to be included in the SIS by Europol.
- Considers the ETIAS-Watch List system to be the privileged and essential tool for ensuring the sharing of information relating to serious crimes falling within the mandate of Europol.
- Urges the timely initiation of the discussion within LEWP and IXIM in order to develop proposals for the revision of the regulatory framework of the ETIAS-Watch List tool to ensure the interoperability of data on terrorists and criminals with the SIS.

LATVIA

LV written comments regarding block 4 - enabling Europol to enter data into the Schengen Information System (SIS)

Q 1) Do you agree that there is an operational need to make verified third-country sourced information on terrorists and other criminals available to frontline officers (border guards and police officers) in order to detect those persons when they seek to cross EU external borders or when they are being checked within the EU?

LV agrees that such an information should be made available to frontline officers. LV also tends to believe that **there is a gap** in this regard that should be addressed. Thus, LV considers that at first **the scale of the problem** (**information gap**) should be determined regarding both FTFs and other offences in respect of which Europol is competent (for instance, CSA etc.). In view of this, LV expects COM to present **precise figures**. Only then – on the basis of those figures provided by COM – **the final decision on the scope** should be taken, namely, whether a future solution should refer only to FTFs (or whether it should cover a wider range of offences).

2) If so, do you agree that the Schengen Information System is the right tool to make this information available to frontline officers (border guards and police officers)? If not, what alternative solution would you propose?

LV agrees that SIS is the right tool to make this information available to frontline officers. In this regard, LV sees the **TWP protocol**[1] agreed last year as the best way forward. In LV view, it provides **a clear and harmonised procedure** for entering relevant data in the SIS, as well as it **ensures availability of those data** to frontline officers. Depending on the reply to the question on information gap, the scope of the TWP protocol could be either maintained only for FTFs' purposes or supplemented by other/all offences in respect of which Europol is competent.

[1] Process for evaluating and possibly entering information from third countries on suspected FTFs in the SIS; doc. 13037/20

LITHUANIA

In accordance with the lats LEWP meeting on 22/02/2021, please find enclosed the Lithuanian answers and additional questions in regards to the Presidency's prepared two questions of thematic bloc 4, enabling Europol to enter data into the Schengen Information System, as stated in the Precidency flash letter.

LITHUANIAN ANSWER AND ADDITIONAL QUESTIONS:

1) Do you agree that there is an operational need to make verified third-country sourced information on terrorists and other criminals available to frontline officers (border guards and police officers) in order to detect those persons when they seek to cross EU external borders or when they are being checked within the EU?

Yes.

2) If so, do you agree that the Schengen Information System is the right tool to make this information available to frontline officers (border guards and police officers)? If not, what alternative solution would you propose.

Yes, the Schengen Information System is the right tool.

Nevertheless, concerns exist if the proposal on entry of alerts by Europol will deliver the desired results. Therefore, we would like to put forward questions regarding the proposed procedure:

- Regarding the relationship between the proposed procedure and the already agreed-upon provisional procedure (COSI, Nov 19). It was agreed that the provisional procedure is to be followed for two years after which its effectiveness will be assessed.
  - How can these two procedures coexist?
  - By following the provisional procedure, voluntary MS' competent national authorities are well in progress of entering the latest FTFs list, yet the proposal mentions 1000 FTFs of which Europol is aware of that have not been entered into SIS yet. Are there still remaining lists of FTFs that Europol had received from third-countries that have not been entered into SIS?

– Regarding the added value of Europol's alerts.

  ◦ Given the fact that Europol's alerts would be informational and would technically require no actions by the MS, apart from informing the SIRENE bureau of the fact that a person has been identified, what would be the added operational value of Europol's alerts?

  ◦ As of right now, SIS alerts are tied to specific actions that MS decide upon when entering a person into SIS. In the proposed procedure, MS themselves will have to decide on how to proceed with a person who was the subject of an alert. How does this ensure the appropriate level of handling throughout all MS that should be applied to persons who are deemed a terrorist threat?

– Regarding the information that is received exclusively by Europol.

  ◦ What are the third-countries/third-parties that Europol receives information from, that MS do not?

– Regarding the criteria for ensuring the trust-worthiness of the third-party and data.

  ◦ What would be the criteria that Europol would follow in order to ensure the trust-worthiness of the source of information and the data received?

  ◦ What rules will Europol follow to ensure that the information received is reliable and not being used for political persecution?

- Regarding the consultations with MS.

Prior consultation with the Member States before the alert is entered into SIS - which channel will be used for consultation (SIENA or ....) with ENU?

NETHERLANDS

Please see below the written comments of the Netherlands of the LEWP of 22 February.

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

– General discussion regarding block 4: enabling Europol to enter data into the Schengen Information System

1) *Do you agree that there is an operational need to make verified third-country sourced information on terrorists and other criminals available to frontline officers (border guards and police officers) in order to detect those persons when they seek to cross EU external borders or when they are being checked within the EU?*

2) *If so, do you agree that the Schengen Information System is the right tool to make this information available to frontline officers (border guards and police officers)? If not, what alternative solution would you propose?*

- As we said during the JHA Council in January, the last IXIM and LEWP, the Netherlands – also following consultations with our operational experts - is not convinced that there is an operational need and/or that the possibility for Europol to enter alerts on suspected third-country nationals in SIS is the right solution. The proposed solution has no added value to the already existing information channels. In the Netherlands frontline officers have adequate access to the information available in systems, including those of Interpol. The solution in our view is to allow MS themselves to remedy the bottleneck of information on suspected third-country nationals in SIS. We see a solution in further cooperation with Interpol.
- The proposal is a fundamental change to the SIS system and poses serious questions about ownership of data, quality of information, fundamental rights of individuals, and a possible conflict with national law and investigations.
- We have a number of important questions we would like to raise:

1) How would Europol decide which information it receives from third countries to consider for inclusion in the SIS? Would the third countries themselves indicate whether the information is intended for e.g. analysis purposes or the SIS? Or would Europol decide what to do with the information it receives?

2) Is there not a risk that third countries would start sending a lot of information to Europol for inclusion in the SIS, i.e. that Europol would in fact be working on behalf of a third country?

3) Who would be responsible for the result of an action?
4) How many resources would Europol need to carry out this task? How much time would Europol need to include an alert about one person in the SIS?
5) Why should Europol be allowed to put information in the SIS that Member States cannot put in themselves? Why should Europol be able to do something that Member States are not?
6) What would be the added value of these alerts if Interpol notices have also been issued for the same people?
7) And last but not least, what would be the added value of having this information at the border, if no action has to be taken?

Before the proposal amending the SIS regulation is further assessed in the IXIM working party, the Netherlands is of the opinion that first clarity is needed on what the problem regarding the 'information gap' around suspect/criminal third country nationals is exactly.

We refer to the Joint Statement by the EU Home Affairs Ministers on the recent terrorist attacks in Europe of 13 November 2020. In that statement it is mentioned that we are striving for a process involving Europol for reviewing relevant information relayed by third countries and analysing it and that it is up to the competent national authorities to enter it into the SIS, to the extent that this is legally possible. The Ministers did not declare that it should be Europol who enters SIS alerts.

- It would not be wise to start negotiating the proposal to amend the SIS Regulation when we do not know what the problem is exactly and where the gap is. We are not convinced that the current proposed solution is the right way to go, and have concerns regarding unwanted effects and precedents. This could best be discussed in a dedicated format. Therefore we would like to propose to change the IXIM meeting planned by the Presidency on 18 March into an LEWP meeting to explore what the problem is and what solution is possible and necessary. Follow-up meetings could be planned if necessary to discuss this further. Only after conclusions have been reached should IXIM start technical, article by article discussions on the Commission's SIS proposal.

POLAND

Polish position as regards amendments to 2016/794 Regulation under block 4: enabling Europol to enter data into the Schengen Information System

1) Do you agree that there is an operational need to make verified third-country sourced information on terrorists and other criminals available to frontline officers (border guards and police officers) in order to detect those persons when they seek to cross EU external borders or when they are being checked within the EU?

Poland is of the opinion that the defined security gap has to be adequately addressed and information about any potential threats to the security of EU should be available to law enforcement officers. Bearing in mind that protecting Europeans from terrorism and organised crime is one of our strategic priorities, the instruments providing access to that information to frontline officers seem to be the most effective and increasing the probability of identifying/controlling the person posing the risk.

2) If so, do you agree that the Schengen Information System is the right tool to make this information available to frontline officers (border guards and police officers)? If not, what alternative solution would you propose?

Poland generally supports the direction of changes proposed in the SIS in relation to Europol. The extension of the SIS to alerts entered by Europol is in line with the EU's efforts to date in the area of redesigning the architecture of large-scale EU information systems to support the security of citizens of the Member States. In the opinion of our experts, possibly SIS is the best available tool to make information available to frontline officers.

At the same time, we believe that a balanced approach to changes in SIS is necessary, emphasizing in particular the need to maintain the supporting role of Europol and the need to assess the added value that these changes can bring in relation to the costs and practical consequences for SIS end users. To this end:

1) The added value of the new category of the SIS alert will depend to a large extent on the quality of information provided by third countries to Europol, therefore it is of utmost importance to set effective verification mechanism in terms of credibility, accuracy, complexity and respect of fundamental rights of individuals. The question is, if Europol has resources to conduct such verification in an appropriate manner, in case of large quantity of data and necessity to check every information case-by-case.

2) The disclosure of information based on a hit should depend on the type of crime and only after obtaining the consent of the Member State that owns the alert. From an operational point of view, it is also important to precisely define the actions to be taken after the hit on the basis of the alert.

3) We believe that the effective implementation of possible changes requires that the European Commission, eu-LISA and Europol coordinate activities in this area so that any changes for national users do not require the launch of separate sub-projects carried out in individual bodies and services. The implementation of the changes related to Europol coincides with the SIS Recast projects already carried out by eu-LISA and the implementation of interoperability of large-scale systems.

There are also a number of connections between this draft Regulation and other EU legislation on large-scale EU information systems. In particular, an evaluation of the provisions at Union level relating to the VIS and ETIAS is necessary to determine whether the new category of SIS alerts should be processed automatically in ETIAS and VIS.

In technical terms, we have to bear in mind risks such as: the relationship between the preparations that eu-LISA has to make for the Central SIS and the preparations Europol has to conduct for establishing the technical interface for transmitting data to the SIS; potential problems that eu-LISA might face in managing the changes presented in this proposal due to the other changes currently being introduced (e.g. introduction of the Entry / Exit System, ETIAS and updates of SIS, VIS and Eurodac); the lack of ICT resources, which results in delays in making the necessary changes and upgrades to the main system.

SLOVENIA

With reference to the Informal videoconference of the members of the LEWP on 22. 2. 2021, the point 8: Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation - General discussion regarding block 4: enabling Europol to enter data into the Schengen Information System, please find bellow the position of Republic of Slovenia.

Answers to your questions:

1. *Do you agree that there is an operational need to make verified third-country sourced information on terrorists and other criminals available to frontline officers (border guards and police officers) in order to detect those persons when they seek to cross EU external borders or when they are being checked within the EU?*

YES

2. *If so, do you agree that the Schengen Information System is the right tool to make this information available to frontline officers (border guards and police officers)? If not, what alternative solution would you propose?*

YES

Also, please find bellow the comment of Slovenia expressed at the last LEWP meeting on 22. 2. 2021:

Slovenia supports the Proposal since a gap in the access to information provided to Europol by third countries has been identified and considers that the solutions put forward in the Regulation adequately address the identified gap and ensure an effective functioning of law enforcement authorities.

Slovenia assesses the Proposal as necessary since it gives an active role to Europol, through which Europol will be able to fill the gap related to entries into the SIS in cases, when MS are not able to enter the alert themselves, and what is more, with Europol SIS alerts we will be able to prevent an undetected entry / travel of persons posing a threat to the internal security of the EU.

SIS represents the most effective possibility for alerts to be in real-time at disposal to all end-users and we are of the opinion that it is of utter importance for Europol to have the possibility to enter information alerts into the system in cases linked to terrorism and forms of crime, which affect a common interest covered by a Union policy.

We believe that, in relation to the entry of Europol SIS alerts, appropriate safeguards have been built in and we support prior consultation, involving the sharing of information on the person concerned with MS.

Access to INTERPOL databases via FIND system is very important for us but we think that this can't be seen as an alternative to the proposed system.

In particular this is very important for us since Slovenia is a transit country and an area of all types of flows, both legal as well as illegal, situated on the Balkan route which is one of the most important entry points for illegal migration to the EU. We believe that with Europol SIS information alerts, we could enhance EU response to threats and make an important added value to the security of the entire EU, especially of those MS that are most at risk in relation to terrorist criminal offences.

We realize that this will give Europol additional tasks and competencies and will also represent the increase of work of frontline police officers and SIRENE Bureaus in particular, but we will »gladly accept« this since we strongly believe that this will result in a significant increase in the security of all EU citizens.

Security of our citizens is our primary concern and we strongly believe that there is no efficient alternative to this proposal!

SPAIN

Follow-up comments to the last LEWP meeting (22/02/2021)

SPANISH POINT OF VIEW REGARDING THE NEXT QUESTIONS:

1) Do you agree that there is an operational need to make verified third-country sourced information on terrorists and other criminals available to frontline officers (border guards and police officers) in order to detect those persons when they seek to cross EU external borders or when they are being checked within the EU? **YES**

2) If so, do you agree that the Schengen Information System is the right tool to make this information available to frontline officers (border guards and police officers)? If not, what alternative solution would you propose? **NO**

ALTERNATIVE PROPOSAL

Relating the fact that Europol could entry alerts in SIS with information on persons received from third countries, and international organisations on foreign terrorist fighters, but also on persons involved in organised crime or serious crime we are studying this issue, we don't see it very clear if this is the appropriate procedure to provide such information to the States and for meet the target pursued. And we keep studying it because, as we have already said several times, it is a new proposal that radically changes the system established so far, since we are facing a competence exclusively of the Member States.

Further, our experts informed us that the proposal may generate some issues as the following:

1. The Europol´s capacity to solve urgently the hit subsequent to an alert generate us many doubts a priori.

2. The ability to solve those hits is frequently based on the quality of the data or on the availability of biometric data. This should be required to Europol if it is the case.

3. Alert proposals would be limited to settings that may not imply coercive measures, namely, by only providing information to the officer receiving the alert and generating intelligence (via CE/CD - Art. 36 Decision). This means that subsequent actions to take are not specified.

4. In relation to the IO regulation, once the system becomes operational, EUROPOL should carry out the manual verification in case of a yellow link with its setting in SIS, like the rest of the SIRENE Offices. We believe that the resolution of the link will be complicated.

That aside, we are currently exploring another way to meet the target that EUROPOL proposes to eliminate possible intelligence gaps, for example, taking advantage of the capabilities offered by Interoperability, through the two EU Regulations that regulates it.

Thus, we could use **QUEST**, **EIS** or a specific database created "ad hoc" by Europol, which should be fed with the data contained in the Europol files about people whose "alerts" were intended to be included. The Agency would make it available to member states within the framework of Interoperability.

During our study, we have found several benefits over the inclusion by Europol of alerts in SIS, such as follows:

1. Costs or changes to be made in legislation, infrastructure or competences would be minimal.

2. With the full implementation of IO, the aim pursued (that the Police receives an alert or alarm upon identification both at the border and within the territory) would be resolved, giving rise to the operational actions required by the situation.

3. The introduction of data through QUEST does not generate identity links to be solved by IO.

4. The expiry date of an alert will not be pre-set by the SIS regulation (art 53 (4), which is so restrictive and establishes generally limits requested alerts to 1 year duration.

5. When a TCN is arranging ETIAS and VIS in order to be authorized to travel to the EU, a link would be generated which, depending of the further review, could lead to a refusal of authorization or visa, respectively.

6. We would not overload the SIS, which has a different nature linked to the Police action on the basis of verified information, with alerts created on information which not always will be verified.

7. The transmission of communication would be faster and lighter, because a communication intermediary would be erased. Regarding the Commission's proposal (alert in SIS), the communication of a hit must be directed from the discovering point to its national SIRENE Office which, in turn, must communicate the hit to Europol and the most logical would be that Europol informs to the law enforcement of that country.

At the same time, a potential boost of a closer collaboration agreement with **Interpol** could be considered, also in the access to the news that be generated.

Apart from that, at national level, It could be implemented that the automatic communication of a detected hit -based on the IO through QUEST by Europol,- requires a specific action to be carried out by the frontline officer.

Spain considers that this proposal is suitable with the development of a voluntary procedure in which MS can enter alerts in SIS on the base of FTFs lists provided by other States. Moreover, all

these persons would be recorded in interoperability regardless of entries in SIS referring to some of them.

Finally, we believe that we should be encouraged to continue exploring other ways to achieve the proposed goals.

Regarding the creation of a working group, which focuses on the EUROPOL alerts on SIS, the handling of these matters should be under LEWP or IXIM, depending on the decision of Portugal Presidency.

5. COMMENTS RECEIVED AFTER THE MEETING ON 8 MARCH 2021

5.1. FOLLOW UP /ADDITIONAL WRITTEN COMMENTS ON BLOCKS 1, 3, 4, 5 AND 7

BELGIUM

Written contribution of Belgium following the LEWP meeting of 8 March 2021 on the revision of the Europol mandate, namely on blocks 1, 3, 4, 5 and 7.

In addition to a confirmation of our position already expressed during the meeting, this contribution contains two specific text proposals to further improve the text in relation to Europol's cooperation with private parties, as well as an important reflection on the correct interpretation of data submitted to Europol for research and innovation purposes.

Block 1

- We support the Dutch comment regarding the reporting on Europol's cooperation with private parties of Article 7(12) and believe it would be better suited to have the content of this paragraph mentioned in a new paragraph in Article 26. Contrary to the existing paragraph 11 of Article 7, there is no direct relationship with the obligations for Europol National Units. If we carefully align this provision with the obligation towards the Joint Parliamentary Scrutiny Group in Article 51(3)(f) and take into account the necessary elements based on its resemblance to Article 7(11), this could then for example become paragraph 11 of Article 26 as follows: *"Europol shall draw up an annual report to the Management Board about the number of cases in which Europol issued follow-up requests to private parties or own-initiative requests to Member States of establishment for the transmission of personal data in accordance with Article 26 and Article 26a, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks. The annual report shall be drawn up on the basis of the quantitative and qualitative evaluation criteria defined by the Management Board and shall be sent to the European Parliament, the Council, the Commission and national parliaments."*

- In relation to including a reference to private parties in the first sentence of Article 23(6) we welcome the explanation of the Commission. The first condition ("*if necessary for preventing and combating crime falling within the scope of Europol's objectives and in accordance with this Regulation*") however seems to be addressed at Europol. The second condition (*"if the recipient gives an undertaking that the data will be processed only for the purpose for which they were transferred*") would then ensure that private parties only process the information for the intended purpose. We thus still wonder if private parties should be added also to this list. We believe this would ensure that private parties do not use the received information for other

purposes (such as commercial purposes) and that legal certainty and data protection would be preserved in a better and clearer way. We thus propose the following change in Article 23(6): *"Without prejudice to Article 30(5), personal data shall only be transferred by Europol to Union bodies, third countries**, ~~and~~** international organisations **and private parties** if necessary for preventing and combating crime falling within the scope of Europol's objectives and in accordance with this Regulation, and if the recipient gives an undertaking that the data will be processed only for the purpose for which they were transferred."*

Block 3

We noted the interpretation by the Commission with regard to Article 18(2)(e) and Article 18(3a), stating that all information that will be provided by the Member States for other purposes and even all information provided by the Member States in the past for other purposes can be used by Europol for research and innovation purposes. However, as also raised by the Netherlands, we are of the opinion that this does not coincide with the intentions of the legislator as regards purpose limitation and with how purpose limitation has been functioning in practice. When providing information to Europol, Member States always have to indicate the purpose for which the information is provided to Europol. It is an established practice within Europol, that only after the consent of the owner of the information, the information can be used for another purpose. This means that in practice information provided to Europol in the past will not be able to be used by Europol for research and innovation purposes without the explicit consent of the owner of the information. Hence, on the basis of the current drafting of the text, Europol will only be able to use information sent to Europol for research and innovation purposes according to Article 18 (2)(e).

The above explained current interpretation is just fine for us as we do not want Europol to be able to use personal data for research and innovation other than those data that have been sent to Europol for that particular purpose. Therefore, we would welcome if our interpretation could be confirmed by the Council's Legal Service.

Block 4

Belgium reaffirms its position as shared in our previous own written comments. We equally reaffirm our support to the French and Greek non-paper. We want to thank the Presidency for its decision to cancel the scheduled IXIM meeting in order for the LEWP to further discuss block 4. We will provide the Presidency with written comments by 26 March as requested during the LEWP meeting of 16 March.

Block 5

As regards Europol's cooperation with third countries, Belgium welcomes the introduced possibility for Europol to conduct a self-assessment. We believe indeed that the existing possibilities should be enlarged and we believe that Europol does have relevant experience in this regard, which would enable it to benefit from such a provision.

Block 7

Belgium confirms their support for deleting the proposed change to Article 6.

BULGARIA

Bulgarian contribution to thematic blocks 1, 5 and 7 of the draft Regulation amending Regulation (EU) 2016/794 as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation (doc. WK 757/2021 REV 2)

Bulgaria would like to thank to the Presidency for organizing the intensive and fruitful discussions in the last months, allowing us to achieve significant progress on the provisions of the draft Regulation. The above mentioned thematic blocks contain the necessary amendments on some of the most important aspects of the activity of Europol. Therefore we appreciate the possibility to send written comments in addition to the position already expressed during the last meetings of LEWP. It is of crucial importance to have a mutual consent on these key provisions.

General comments

Is there difference between "competent authorities of the Member States" (see art.2 (a)) and the term "national law enforcement authorities" used in the proposal of the Commission only in recitals 29, 30, 34 and 38?

We suggest to use one and the same term namely "competent authorities of the Member States"

Recital 14 has to be brought in line with article 6 and our proposal is:

To strengthen the support and mutual cooperation between the the competent authorities of the Member States, Europol should be able to request Member States to initiate, conduct or coordinate criminal investigations into a crime falling within the scope of its objectives. Europol should inform Eurojust of such requests.

Recital 34

We need clarifications what is meant under private parties – only private parties with seat in MS or even private parties under the jurisdiction of third countries (both with operational/strategic agreement or without agreement with Europol). We try to understand from practical point of view how this exchange will take place

Concerning the last 2 sentences

"Where Member States use the Europol infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, they may decide whether to involve Europol in such exchanges or not. If it is not involved, Europol should not have access ~~Where Member States use the Europol infrastructure for exchanges of personal~~ **to data on crimes falling outside the scope of** ~~the~~ **its objectives** ~~of Europol, Europol should not have access to that data~~."

following questions arose. What happens when the crime falls in the scope but Europol is not involved in the information exchange – does it mean that despite that Europol would have access to these data.

And also: If Europol is involved in information exchange on crimes falling outside the scope of its objectives does it means that Europol will have the right to process these data including personal data.

To what data the access restriction/permission should be – to all kind of data or only to personal data? What the general rule should be?

Article 2 Definitions

Letter (p) 'administrative personal data' means all personal data processed by Europol apart from operational data ~~those that are processed to meet the objectives laid down in Article 3~~;

Considering the fact that there is no specific definition of „operational personal data" and this term is used in the draft amedments proposed by the Commission togheter with the term "personal data" and taking into account the refference made in Art. 27 a, para 3, namely *„References to 'personal data' in this Regulation shall be understood as references to 'operational personal data', unless indicated otherwise"*, we are on the opinion that it should be a clarification of this term. Therefore we propose the following wording:

(p) 'administrative personal data' means all personal data processed by Europol apart from operational **personal** data **listed in Annex II**.

Comments on blocks 1, 5 and 7

Block 1: Enabling Europol to cooperate effectively with private parties

Relevant articles	Proposed texts	BG comments
• Article 26(2) [amended]	2. Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 in order to identify all national units concerned, as referred to in point (a) of paragraph 1. Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the national units concerned. Europol may forward the personal data and relevant results from the processing of that data necessary for the purpose of	Would Europol be able to identify ALL national units during the initial assessment of the provided information?

	establishing jurisdiction in accordance with Article 25 to contact points and authorities concerned as referred to in points (b) and (c) of paragraph 1. ~~Once~~ **If Europol cannot identify any national units concerned, or has already** ~~Europol has identified and~~ forwarded the relevant personal data to all the **identified** respective national units concerned**~~, or~~ and** it is not possible to identify further national units concerned, it shall erase the data, unless the national unit, contact point or authority concerned resubmits the personal data to Europol in accordance with Article 19(1) within four months after the transfer takes place."	
	"2a. Any cooperation of Europol with private parties shall neither duplicate nor interfere with the activities of Member States' financial intelligence units established pursuant to Directive (EU) 2015/849 of the European Parliament and of the Council, and shall not concern information that is to be provided to financial intelligence units for the purposes of that Directive."	We support the proposed new paragraph 2a.
• Article 26(6a) [new]	"6a. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, ~~under their applicable laws~~ **in accordance with their national legal frameworks**, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned.	We propose „**national legal frameworks**" everywhere to be replaced by „**national law**" as this term is used in the Regulation
• Article 26(6b)	6b. Europol's infrastructure may be	The paragraph should be

[new]	used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws. In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data.	brought in line with recital 34.

Block 5: Strengthening Europol's cooperation with third countries

	Proposed texts	BG comments
• Article 25(5) [amended]	**(-a) In paragraph 1, point (a) is replaced by the following:** "(a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision') **or in the absence of such a decision, appropriate safeguards have been provided for or exist in accordance with paragraph 4a of this Article, or in the absence of both an adequacy decision and of such appropriate safeguards, a derogation applies pursuant to paragraph 5 or 6 of this Article**;	We fully support the newly proposed texts on the model of Eurojust, which provide more flexibility in personal data exchange with third countries. With regards to para 4a (b) we need clarification who will take the decision that appropriate safeguards exist - the Executive Director or the MB on a proposal of the Executive Director, or the MB will confirm the conclusion made by the
	"4a.	

	In the absence of an adequacy decision, Europol may transfer operational personal data to a third country or an international organisation where: **(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or** **(b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data."**	Executive Director? What will be the role of the DPO in this regard?

Block 7: clarifying that Europol may request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

	Proposed texts	BG comments
• Article 6(1) [amended]	In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the ~~Member State or~~ Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation."	We fully support reinstatement of the current wording of art 6 of Europol Regulation (EU) 2016/794

CZECH REPUBLIC

CZ comments – amendment to Europol Regulation blocks 1, 3 and 7

CZ proposes only very limited following changes to wk 757/2/2020 REV 2:

Block 1

Article 26a(5)

Technical change is necessary to align this provision with Art. 26(6a):

6a. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, ~~under their applicable laws~~ **in accordance with their national legal frameworks**, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned.

Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives.

Block 3

Recital 11

As indicated at the last meeting, CZ proposes to include text about the necessity of adequate funding for innovation and research at Europol. In addition, we are uncertain whether mere assistance with identifying key research themes really constitutes a conflict of interests (what about Member States that would assist the Commission by proposing key research themes?):

(11) In order to help EU funding for security research to develop its full potential and address the needs of law enforcement, Europol should assist the **Member States and the** Commission in identifying key research themes, **and the Commission in** drawing up and implementing the Union framework programmes for research and innovation that are relevant to Europol's objectives. When

Europol assists the Commission in (identifying key research themes,) drawing up and implementing a Union framework programme, it should not receive funding from that programme in accordance with the conflict of interest principle. **Therefore, it is necessary to ensure adequate and reliable funding of research and innovation efforts at Europol in order to enable it to support law enforcement authorities of the Member States.**

Article 4(4a)

This paragraph should be corrected so as to exclude assistance to Member States in drawing up and implementing Union research programmes:

4a. Europol shall assist the Member States and the Commission in identifying key research themes. Europol shall assist ~~the Member States and~~ the Commission in drawing up and implementing the Union framework programmes for research and innovation activities that are relevant to achieve the objectives set out in Article 3. When Europol assists the Commission in (identifying key research themes,) drawing up and implementing a Union framework programme, the Agency shall not receive funding from that programme. Europol may engage with relevant projects of such Union framework programmes and disseminate the results of that research to the Member States in accordance with Article 67.

Block 7

Recital 14

This recital should be deleted in light of deletion of amendment to Art. 6(1) on request to initiate a criminal investigation to single Member State.

(end of file)

FRANCE

NOTE DE COMMENTAIRES DES AUTORITÉS FRANÇAISES

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leurs commentaires écrits suite à la réunion de groupe LEWP du 8 mars 2021 s'agissant de la révision du règlement d'Europol *(5397/21, 5527/21 REV3, 5388/21 REV2, WK 757/21 REV2).*

Ces commentaires sont accompagnés du document « ***Annexe – Propositions d'amendements_révision Règlement EUROPOL*** » intégrant des propositions d'amendements.

- **Concernant le bloc thématique n°1 (permettre à Europol de coopérer efficacement avec les acteurs privés) :**

Reference in proposal COM(2020) 796 final	
Proposition de la présidence portugaise	**Commentaires des autorités françaises**
Article 1(2)(a)(III) du règlement (UE) 2016/794 est modifié comme suit à l'article 4 : Article 4 is amended as follows: (iii) point (m) is replaced by the following: "(m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States **and upon their request**, the coordination of law enforcement authorities' response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;";	Pas de commentaire.
Article 1(2)(a)(IV) du règlement (UE) 2016/794 prévoit de nouvelles dispositions à l'article 4 : Article 4 is amended as follows:	Pas de commentaire.

(iv) the following points (q) to (r) are added: […] (u) support, **upon their request,** Member States' actions in preventing the dissemination of online content **in an online crisis situation, in particular by providing private parties with the information necessary to identify relevant online content.** ~~**Related to terrorism or violent extremism in crisis situations, which stems from an ongoing or recent real-world event, depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and aims at or has the effect of seriously intimidating a population, and where there is an anticipated potential for exponential multiplication and virality across multiple online service providers**~~.	
Article 7 (12) **Europol shall draw up an annual report to the Management Board on the personal data exchanged with private parties pursuant Articles 26 and 26a on the basis of quantitative and qualitative evaluation criteria defined by the Management Board including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks. The annual report shall be sent to the European Parliament, the Council, the Commission and national parliaments;**	**Les autorités françaises remercient la présidence pour l'intégration de cette disposition complète et détaillée.** **Afin d'être le plus précis possible et d'éviter tout risque de mauvaise interprétation, la France propose un amendement à cet article (voir document en pièce jointe).**
Article 1(5)(a)(i) du règlement (UE) 2016/794 est modifié comme suit à l'article 18 : Article 18 is amended as follows: (a) paragraph 2 is amended as follows: (i) point (d) is replaced by the following wording: "(d) facilitating the exchange of	Pas de commentaire.

information between Member States, Europol, other Union bodies, third countries, international organisations and private parties;"	
Article 1(12)(a) du règlement (UE) 2016/794 est modifié comme suit à l'article 26 : *Article 26 is amended as follows :* (a) paragraph 2 is replaced by the following "2. Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 in order to identify all national units concerned, as referred to in point (a) of paragraph 1. Europol shall forward the personal data and any relevant results from the processing of that data necessary for the purpose of establishing jurisdiction immediately to the national units concerned. Europol may forward the personal data and relevant results from the processing of that data necessary for the purpose of establishing jurisdiction in accordance with Article 25 to contact points and authorities concerned as referred to in points (b) and (c) of paragraph 1. ~~Once~~ **If Europol cannot identify any national units concerned, or has already** ~~Europol has identified and~~ forwarded the relevant personal data to all the **identified** respective national units concerned, ~~or~~ **and** it is not possible to identify further national units concerned, it shall erase the data, unless the national unit, contact point or authority concerned resubmits the personal data to Europol in accordance with Article 19(1) within four months after the transfer takes place."	Les autorités françaises remercient la Présidence pour les précisions apportées à cette proposition équilibrée.
Article 1(12)(b) du règlement (UE) 2016/794 est modifié comme suit à l'article 26 : Article 26 is amended as follows (b) paragraph 4 is replaced by the following: "4. If Europol receives personal data from a	Pas de commentaire.

private party in a third country, Europol may forward those data only to a Member State, or to a third country concerned with which an agreement on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 TFEU has been concluded or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation. Where the conditions set out under paragraphs 5 and 6 of Article 25 are fulfilled, Europol may transfer the result of its analysis and verification of such data ~~with~~ **to** the third country concerned."	
Article 1(12)(c) du règlement (UE) 2016/794 est modifié comme suit à l'article 26 : Article 26 is amended as follows (c) paragraphs 5 […] are replaced by the following: "5. Europol may transmit or transfer personal data to private parties on a case-by-case basis, where it is strictly necessary, and subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67, in the following cases: (a) the transmission or transfer is undoubtedly in the interests of the data subject, ~~and either the data subject has given his or her consent~~; or (b) the transmission or transfer is absolutely necessary in the interests of preventing the imminent perpetration of a crime, including terrorism, for which Europol is competent; or (c) the transmission or transfer of personal data which are publicly available is strictly necessary for the performance of the task set out in point (m) of Article 4(1) and the following conditions are met: (i) the transmission or transfer concerns an individual and specific case; (ii) no fundamental rights and freedoms of the data subjects concerned override the public interest necessitating the	Pas de commentaire.

transmission or transfer in the case at hand; or (d) the transmission or transfer of personal data is strictly necessary for Europol to inform that private party that the information received is insufficient to enable Europol to identify the national units concerned, and the following conditions are met: (i) the transmission or transfer follows a receipt of personal data directly from a private party in accordance with paragraph 2 of this Article; (ii) the missing information, which Europol may refer to in these notifications, has a clear link with the information previously shared by that private party; (iii)the missing information, which Europol may refer to in these notifications, is strictly limited to what is necessary for Europol to identify the national units concerned.	
Article 1(12)(c) du règlement (UE) 2016/794 est modifié comme suit à l'article 26 : Article 26 is amended as follows (c) paragraphs […] 6 are replaced by the following: 6. With regard to points (a), (b) and (d) of paragraph 5 of this Article, if the private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, the transfer shall only be authorised by the Executive Director if the transfer is: (a) necessary in order to protect the vital	Pas de commentaire.

interests of the data subject or another person; or (b) necessary in order to safeguard legitimate interests of the data subject; or (c) essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or (d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences for which Europol is competent; or (e) necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence for which Europol is competent. Personal data shall not be transferred if the Executive Director determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer referred to in points (d) and (e). Transfers shall not be systematic, massive or structural."	
Article 1(12)(d) du règlement (UE) 2016/794 prévoit de nouvelles dispositions à l'article 26 : (d) the following paragraphs 6a […] are inserted: "6a. Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, ~~under their applicable laws~~ **in accordance with their national legal frameworks**, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for	Les autorités françaises remercient la présidence pour cette précision. Elles accordent une importance particulière à ce que **le cadre légal établi au sein des Etats membres s'applique strictement aux échanges avec les parties privées**.

Europol with a view to identifying the national units concerned. Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives.	
Article 1(12)(d) du règlement (UE) 2016/794 prévoit de nouvelles dispositions à l'article 26 (d) the following paragraphs […] 6b are inserted: 6b. Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws. In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data."	
Article 1(12)(e) du règlement (UE) 2016/794 supprime les dispositions suivantes à l'article 26: (e) paragraphs 9 and 10 are deleted;	Pas de commentaire.
Article 1(13)(d) du règlement (UE) 2016/794 prévoit les dispositions suivantes à l'article 26 : (13) the following Article 26a is inserted: *"Article 26a*	Les autorités françaises saluent **l'ajout du terme « online » qui, en lien avec la définition proposée à l'article 2**, permet de préciser le type de crise dont il est question.

Exchanges of personal data with private parties in <u>online</u> crisis situations 1. Europol may receive personal data directly from private parties and process those personal data in accordance with Article 18 to prevent the dissemination of online content related to terrorism or violent extremism in **<u>online</u>** crisis situations as set out in point (u) of Article 4(1). 2. If Europol receives personal data from a private party in a third country, Europol may forward those data only to a Member State, or to a third country concerned with which an agreement on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 TFEU has been concluded or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation. Where the conditions set out under paragraphs 5 and 6 of Article 25 are fulfilled, Europol may transfer the result of its analysis and verification of such data ~~with~~ **<u>to</u>** the third country concerned. 3. Europol may transmit or transfer personal data to private parties, on a case-by-case basis, subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67, where the transmission or transfer of such data is strictly necessary for preventing the dissemination of online content related to terrorism or violent extremism as set out in point (u) of Article 4(1), and no fundamental rights and freedoms of the data subjects concerned override the public interest necessitating the transmission or transfer in the case at hand. 4. If the private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, the transfer shall be authorised by the Executive Director. 5. Europol may request Member States, via	

their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, under their applicable laws, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol for preventing the dissemination of online content related to terrorism or violent extremism as set out in point (u) of Article 4(1). Irrespective of their jurisdiction with regard to the dissemination of the content in relation to which Europol requests the personal data, Member States shall ensure that the competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives. 6. Europol shall ensure that detailed records of all transfers of personal data and the grounds for such transfers are recorded in accordance with this Regulation and communicated upon request to the EDPS pursuant to Article 40. 7. If the personal data received or to be transferred affect the interests of a Member State, Europol shall immediately inform the national unit of the Member State concerned."	

- **Concernant le bloc thématique n°3 (renforcer le rôle d'Europol en termes de recherche et d'innovation) :**

Reference in proposal COM(2020) 796 final	
Proposition de la Présidence	**Commentaires des autorités françaises**
Article 1(2)(a)(IV) du règlement (UE) 2016/794 prévoit de nouvelles dispositions à l'article 4 : Article 4 is amended as follows: (iv) the following points (q) to (r) are added: […] (t) proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States,	Pas de commentaire.

~~and~~ implement its research and innovation activities regarding matters covered by this Regulation, including **in** the development, training, testing and validation of algorithms for the development of tools, **and disseminate the results of these activities to the Member States in accordance with Article 67, and contribute to the coordination of activities of Union agencies established on the basis of Title V of the TFEU in the field of research and innovation within their mandates in close cooperation with Member States**.	
Article 1(2)(d) du règlement (UE) 2016/794 prévoit de nouvelles dispositions à l'article 4 : Article 4 is amended as follows: (d) the following paragraphs 4a […] are inserted: "4a. Europol shall assist **the Member States and** the Commission in identifying key research themes~~,~~. **Europol shall assist the Member States and the Commission in** drawing up and implementing the Union framework programmes for research and innovation activities that are relevant to achieve the objectives set out in Article 3. When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, the Agency shall not receive funding from that programme. **Europol may engage with relevant projects of such Union framework programmes and disseminate the results of that research to the Member States in accordance with Article 67.**	Pas de commentaires.
Article 1(2)(d) du règlement (UE) 2016/794 prévoit de nouvelles dispositions à l'article 4 : Article 4 is amended as follows: (d) the following paragraphs […] 4b are inserted: ~~4b. Europol shall support the screening of specific cases of foreign direct investments~~	Les autorités françaises accueillent **favorablement la suppression de l'article dont le lien avec les activités d'Europol en matière d'appui aux États membres n'est pas clairement établi**.

~~into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council* that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security.~~	
Article 1(5)(a)(ii) du règlement (UE) 2016/794 prévoit de nouvelles dispositions à l'article 18 : Article 18 is amended as follows: (a) paragraph 2 is amended as follows: (ii), the following points (e) and (f) are added: "(e) research and innovation regarding matters covered by this Regulation for the development, training, testing and validation of algorithms **for the development of tools and for other research and innovation activities relevant to achieve the objectives set out in Article 3**;	Pas de commentaire.
Article 1(5)(b) du règlement (UE) 2016/794 prévoit de nouvelles dispositions à l'article 18 : (b) the following paragraph 3a is inserted: "3a. **If necessary to reach the objectives of Europol's research and innovation projects, P**processing of personal data for the purpose of research and innovation as referred to in point (e) of paragraph 2 shall be performed **only** by means of Europol's research and innovation projects with clearly defined objectives, duration and scope of the personal data processing involved, in respect of which the additional specific safeguards set out in Article 33a shall apply."	Les autorités françaises estiment que **la dimension collaborative de la recherche et de l'innovation devrait autoriser la réalisation effective du « *processing* » des données par Europol et les Etats membres dès lors que les garanties de protection des données personnelles sont réunies.** En outre, les autorités françaises s'interrogent sur l'utilisation exclusive des moyens d'Europol et proposent de **retirer le terme « *only* » afin de laisser ouvert le champ des possibles.**

Article 1(19) du règlement (UE) 2016/794 prévoit de nouvelles dispositions à l'article 33 : the following Article 33a is inserted: *"Article 33a* **Processing of personal data for research and innovation** 1. For the processing of personal data performed by means of Europol's research and innovation projects as referred to in point (e) of Article 18(2), the following additional safeguards shall apply: a) any project shall be subject to prior authorisation by the Executive Director, based on a description of the envisaged processing activity setting out the necessity to process personal data, such as for exploring and testing innovative ~~new~~ **technological** solutions and ensuring accuracy of the project results, a description of the personal data to be processed, a description of the retention period and conditions for access to the personal data, a data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome, and the measures envisaged to address those risks;	

- **Concernant le bloc thématique n°5 (renforcer la coopération d'Europol avec les États tiers) :**

Reference in proposal COM(2020) 796 final	
Proposition de la Présidence portugaise	**Commentaires des autorités françaises**
Considérant 24 Serious crime and terrorism often have links beyond the territory of the Union.	**La France estime qu'il convient de modifier le considérant 24 en fonction de la modification de l'article 25 tel que présentée par la présidence portugaise.**

Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation.	
Article 1(11)(a) du règlement (UE) 2016/794 prévoit les modifications suivantes à l'article 25 : Article 25 is amended as follows: (a) In paragraph 1, point (a) is replaced by the following: (a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision') **or in the absence of such a decision, appropriate safeguards have been provided for or exist in accordance with paragraph 4a of this Article, or in the absence of both an adequacy decision and of such appropriate safeguards, a derogation applies pursuant to paragraph 5 or 6 of this Article**;	**Les autorités françaises remercient vivement la présidence portugaise pour l'intérêt porté aux commentaires des délégations et d'Europol sur la prise en compte du régime d'autres agences JAI en matière de coopération avec les Etats tiers.** **Toutefois, les autorités françaises précisent que cette modification du cadre d'échange avec les Etats tiers doit absolument s'accompagner d'un renforcement du contrôle du Conseil d'administration.** **Ainsi, il conviendrait que le Conseil Affaires Etrangères non seulement décide des arrangements de travail et des arrangements administratifs conclus par l'agence (article 11r) mais également qu'il puisse autoriser Europol à échanger des données personnelles au terme du paragraphe 4a de l'article 24 tel que proposé par la présidence.** **Les autorités françaises proposent un amendement à la proposition de la présidence (cf : pièce jointe).**

- **Concernant le bloc thématique n°7 (clarifier la possibilité pour Europol de demander l'ouverture d'une enquête sur un crime concernant l'intérêt commun dans une politique de l'Union) :**

Reference in proposal COM(2020) 796 final	
Proposition de la Commission	**Commentaires des autorités françaises**
Considérant One of Europol's objectives is to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combatting forms of crime which affect a common interest covered by a Union policy. To strengthen that support, Europol should be able to request the competent authorities of a Member State to initiate, conduct or coordinate a criminal investigation of a crime, which affects a common interest covered by a Union policy, even where the crime concerned is not of a cross-border nature. Europol should inform Eurojust of such requests.	Au regard de la proposition satisfaisante de la présidence portugaise sur l'article 6, les autorités françaises proposent de **supprimer ce considérant**.
Article 1(3) du règlement (UE) 2016/794 prévoit la modification suivante à l'article 6 : in Article 6, paragraph 1 is replaced by the following: "1. In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the ~~Member State or~~ Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation."	Les autorités françaises se félicitent de cette suppression et remercient la Présidence portugaise pour la prise en compte des remarques faites par la délégation française.

Annexe – Propositions d'amendements_révision Règlement EUROPOL

Note de commentaires des autorités françaises
à la suite de la réunion du groupe LEWP du 8 mars 2021

Propositions d'articles - (bloc 1 parties privées et bloc 5 relations avec les Etats tiers)

En complément de ses commentaires sur les blocs 1, 3, 5 et 7, les autorités françaises proposent ci-dessous plusieurs amendements aux propositions de la Présidence portugaise.

Relations entre Europol et les parties privées

Les autorités françaises sont satisfaites du déroulement des discussions sur ce point et de la reprise de certaines de ses propositions.

Les autorités françaises sont également satisfaites des dernières propositions de la Présidence portugaise et accueillent très favorablement la proposition de la délégation hollandaise visant à permettre au Conseil d'administration de l'agence de produire des **lignes directrices** afin d'encadrer l'échange de données avec les parties privées.

Dans la continuité de ses précédentes contributions, elles soumettent à la Présidence les propositions d'article suivante :

Article 11 (v) Échanges de données à caractère personnel avec les parties privées (nouveau) :

Version FR *: « adopte des lignes directrices sur la réception et l'échange de données entre Europol et les parties privées ».*

Version EN : " *adopt guidelines on the receipt and exchange of data between Europol and private parties* ».

Article 23 paragraphe 4 bis échange de données à caractère personnel avec les parties privées (nouveau) :

Version FR : *« sans préjudice des articles 26 et 26a du présent règlement et après validation du Conseil d'administration, Europol peut conclure des protocoles d'entente avec les parties privées. Ces protocoles n'autorisent pas l'échange de données à caractère personnel et ne lient ni l'Union ni*

ses États membres.

Europol communique systématiquement aux États membres l'ensemble des protocoles d'ententes conclus avec les parties privées, pour information et validation par le Conseil d'administration ».

Version EN : " *Without prejudice to articles 26 and 26a and after the agreement of the Management Board, Europol may conclude memoranda of understanding with private parties. Such memoranda shall not authorise the exchange of personal data and shall not be binding on the Union or its Member States.*

Europol shall systematically communicate to the Member States all memoranda of understanding concluded with private parties for information and validation by the Management Board ".

Article 11 (r) Fonctions du Conseil d'administration (amendement) :

Version FR *: « r) Autorise la conclusion d'arrangements de travail, d'arrangements administratifs et* ***de protocoles d'entente avec les parties privées*** *conformément à l'article 23 paragraphe 4 et 4bis, et à l'article 25, paragraphe 1 ».*

Version EN: " r) *Decide upon working arrangements, administrative arrangements and memoranda of understanding with private parties in accordance with Article 23, paragraphs 4 and 4a, and Article 25, paragraph 1".*

Amendement de la proposition de la présidence portugaise (article 7 (12))

"Europol shall draw up an annual report to the Management Board on the personal data ***received*** *and exchanged with private parties pursuant Articles 26 and 26a on the basis of quantitative and qualitative evaluation criteria defined by the Management Board including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks. The annual report shall be sent to the European Parliament, the Council, the Commission and national parliaments".*

Coopération entre Europol et les Etats tiers

Les autorités françaises se félicitent du bon déroulement des discussions sur ce point et de l'amendement apporté par la Présidence à la proposition de la Commission.

Toutefois, et afin d'assurer à l'agence une plus grande efficacité opérationnelle et stratégique, les autorités françaises proposent les amendements suivants :

- **Article 7 (13) Fonctions du Conseil d'administration (nouveau) :**

Version FR :« *Europol rédige un rapport annuel portant sur la nature et le volume des données personnelles fournies à Europol et échangées avec les États tiers sur la base des critères d'évaluation quantitatifs et qualitatifs fixés par le CAE. Ce rapport annuel est transmis au parlements nationaux, au Parlement européen, au Conseil, et à la commission* ».

Version EN : " *Europol shall draw up an annual report to the Management Board on the personal data received and exchange with third countries on the basis of quantitative and qualitative evaluation criteria defined by the Management Board. The annual report shall be sent to the national parliaments, the European Parliament, the Commission, the Council and the Commission*."

Amendement de la proposition de la présidence (article 25.4a)

[…]

4a. In the absence of an adequacy decision, Europol may, ***after authorization of the Management Board****, transfer operational personal data to a third country or an international organisation where:*

(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or

(b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data.

GERMANY

Germany's follow-up comments to the LEWP meeting on 8 March 2021 (Revision of the Europol Regulation) – Thematic bloc 4

Following up on the discussion on thematic bloc 4 at the last LEWP meeting, Germany would like to raise the following questions:

- Which persons or lists should be covered by the proposal?
- Under which conditions would the proposal enable Europol to enter persons, including those on certain lists, into the SIS?
- On what basis/criteria would Europol decide which information from third countries should be entered with the effect of an information alert?
  For example, would Europol readily propose to MS that lists from Russia or China be entered into the SIS as information alerts by Europol? (At INTERPOL, we have Articles 2 and 3 of the INTERPOL Constitution to prevent an abuse by member countries.)
- What would be the added value of the new types of alerts, rather than relying on existing categories of alerts (entered by MS)?
- In light of Article 88 TFEU, which provides for *"support and strengthen[ing] action by the Member States' police authorities and other law enforcement services and their mutual cooperation"*, we would find it advisable to seek an opinion of the CSG legal service to confirm compliance, i.e. of the Commission's or any other alternative proposal, with primary Union law.

We would be very pleased to receive short and comprehensible answers to these questions.

Germany's follow-up comments to the LEWP meeting on 8 March 2021 (Revision of the Europol Regulation) – Thematic blocs 1, 3, 5 and 7

Please find below Germany's written comments on the second revised version of the text of the Commission proposal (changes to the provisions pertaining to thematic blocs 1, 3, 5 and 7). Further comments may be raised following ongoing scrutiny of the proposal.

On a general note, Germany would very much welcome if Europol could continuously be present in the meetings. In our view, delegations would benefit from seeking Europol's expertise and advice in the ongoing discussions. Against the background that Europol is also continuously invited at Ministerial Council level, we do not see any reasons why the participation of an agency should not be possible nor any legal obstacles.

Thematic bloc 1: cooperation with private parties

Article 2(r):

Germany welcomes that the definition has been aligned in line with our previous comments.

Article 4(1)(m):

We suggest the following amendments (underlined) to the version in WK 757/21 Rev.2:

> "the coordination of the competent authorities of the Member States' ~~law enforcement authorities'~~ response to cyberattacks and~~,~~ the taking down of terrorist content online constituting such forms of crime, and".

Moreover, the exact role of Europol with respect to the new TCO Regulation (not adopted yet, as stressed by COM in the Working Party) remains to be determined. The second amendment here would help in this respect, as it clarifies that any relevant cyberattacks or terrorist content online would have to constitute a Europol crime. This is the exact language used now, later in the sentence after "internet content".

Article 26(2):

We thank for the revision of that provision, as contained in WK 757/21 Rev.2.

With regard to the fourth sentence, we would appreciate an explanation why the obligation to delete would not take immediate effect after the transfer to all concerned units has been completed.

Article 26(6a):

We welcome the revised version of this provision as in WK 757/21 Rev.2.

Article 26a:

As a general observation, after the only slight revisions in WK 757/21 Rev.2 it remains unclear what the supporting task of Europol would be, including the relationship to the current tasks under Article 4(1)(m). The provision would also raise various issues about its exact scope. Should electronic evidence fall under it, this may have undesirable implications vis-à-vis the draft TCO Regulation and harbor contradictions to the E-Evidence dossier.

Thematic bloc 3: research and innovation

Article 4(4a):

While we welcome that the changes foresee greater involvement of the Member States, we maintain our view that the proposed new Article 4(4a) should be deleted and would like to refer to our previous comments.

From our point of view, the fundamental question is what role Europol should play in the field of innovation. Should it support the Member States with concrete projects? Or should it take on a more

strategic role for the EU and the Commission? This question has to be answered on the basis of the needs of the national law enforcement authorities.

Following our own assessment in Germany but also the position of other MS on this matter, the main need clearly is in the area of supporting the national law enforcement authorities with concrete innovation projects. At the last meeting of the Management Board, Europol itself emphasised that it sees the role of its Innovation Lab primarily in the implementation of concrete projects for the law enforcement authorities of the Member States and highlighted the importance of EU funding in order to bridge budgetary gaps. Only when it is ensured that Member States' law enforcement authorities receive the best possible support in the area of innovation can further tasks be considered.

Article 4(4b):

Germany welcomes the deletion of this provision in line with our previous comments.

Article 18(3a):

The revised version in WK 757/21 Rev.2 is acceptable to Germany.

Article 33a(2):

Point (a) of Article 33(1) already foresees that for each individual project the necessity to process personal data is to be assessed carefully. In that context, the newly introduced Article 33(2) is rather of an advisory character. With that in mind, we think that this would be better placed in the corresponding Recital. Besides, we would like to ask to limit the phrase to "synthetic" and "anonymized" data. Personal data (such as "pseudonymized data") may be used where it is necessary and proportionate.

Thematic bloc 5: cooperation with third countries

Article 25(1)(a), (4a) and (8):

Germany welcomes that our proposal has been included in the text in line with our previous comments. We would like to point out that the amendment should also be reflected in all other provisions that refer to the possibilities for structural exchanges of personal data with third countries foreseen by Article 25, e.g. Articles 26(1)(c), 26(4), 26a(2) and 26a(4).

Schengen-associated countries:

In line with our previous comments, we maintain the view that the revision of the Europol Regulation would be a good opportunity to put the Schengen-associated countries on an equal footing with Member States, considering that they have the same level of data protection in the JHA

field as the Member States do. In that regard, the Schengen acquis ensures the highest degree of conformity.

We take note of the Commission's and the CLS's position arguing that the Europol Regulation is not part of the Schengen acquis. We are not fully convinced of this argument and would like to understand better whether and where the Commission and the CLS see the specific legal hurdles that would stand in the way of putting Schengen-associated countries on an equal footing with Member States.

Thematic bloc 7: ability to request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

Germany welcomes the deletion of the proposed amendment to Article 6. This follows the Member States' clear rejection of such amendment, expressed again at the last LEWP meetings. We would like to point out that the deletion must be reflected in Recital 14 accordingly. To that end, we suggest that the wording of Recital 11 of the current Europol Regulation be retained:

> *"Europol should be able to request Member States to initiate, conduct or coordinate criminal investigations in specific cases where cross-border cooperation would add value. Europol should inform Eurojust of such requests."*

LITHUANIA

In accordance to the last informal videoconference of the LEWP meeting on 08/03/2021, please be advised that we do not have any additinal remarks or suggestions to those that we have sent you on 15/02/2021.

Nevertheless, we would kindly like to ask you to analyze our remarks and wording suggestions that we proposed in our earlier position, in case it could be taken into account.

NETHERLANDS

Comments the Netherlands on blocs 1, 3, 4, 5 and 7 of the Europol Regulation following the LEWP of 8 March 2021

- Enabling Europol to cooperate effectively with private parties, strengthening Europol's role on research and innovation, enabling Europol to enter data into the Schengen Information System, strengthening Europol's cooperation with third countries and clarifying that Europol may request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

- We would like to thank the Presidency for the new version of the text. We are pleased to see that a number of the changes we had asked for have been included. We understand that with such a complicated proposal, it takes time to take all the comments on board and to present a new text. It also takes time for the Member States to study all the changes that have been proposed and any new thematic blocs that are put on the agenda. We would therefore like to ask you to please send us the agenda and the new version of the proposal at an earlier stage next time, so that we have sufficient time to prepare.

- We would very much appreciate it if you could include our scrutiny reservation on the proposal in a footnote.

Bloc 1 Enabling Europol to cooperate effectively with private parties

General questions

- We have a couple of general remarks and questions about the articles and recitals of bloc 1 on private parties.

- Thank you very much for taking on board our drafting suggestion for article 23 para 7, to make sure that private parties can only forward personal data they have received from Europol with Europol's permission.

- During the LEWP of 8 March, Belgium asked whether "private parties" should be added not only in article 23, para 7 but also in the first sentence of para 6. We think this might be a logical addition. We understand art 23 para 6 to mean that Europol needs to determine whether sharing information with another organisation is necessary for preventing and combating crime. This does not necessarily mean that the organisation receiving the information should have the prevention of or fight against crime as a task too. It seems logical that Europol should make this determination regardless of the type of organisation it intends to share the information with. We would therefore like to propose adding "private parties" to the first sentence of art 23 para 6 too:

> "Without prejudice to Article 30(5), personal data shall only be transferred by Europol to Union bodies, third countries ~~and~~ international organisations and private parties if necessary for preventing and combating crime falling within the scope of Europol's objectives and in

accordance with this Regulation, and if the recipient gives an undertaking that the data will be processed only for the purpose for which they were transferred."

- Since the LEWP of 8 March, we have realised that under article 18 para 7, the MB already adopts guidelines about processing of information for the purposes mentioned in art 18 para 2. Looking at paragraph 2, these guidelines also seem to cover information exchange with private parties and the processing of data for research and innovation. There therefore seems no need for separate guidelines.

- Recital 25 refers to "private parties providing cross-border services", whereas articles 26 and 26a talk about private parties in general. We would like to suggest that the words "providing cross-border services" are deleted from recital 25, to make sure there is no confusion about the scope of articles 26 and 26a. Recital 26 already explains that one of the main reasons for introducing these changes the use by criminals of the cross-border services of private parties, so this will remain clear, even if we delete these words in recital 25:

> "To support Member States in cooperating with private parties ~~providing cross-border services~~ where those private parties hold information relevant for preventing and combatting crime, Europol should be able to receive, and in specific circumstances, exchange personal data with private parties."

- There seems to be a small mistake in recital 32:

> "Transmissions should relate to Europol disclosing personal data <u>to</u> ~~with~~ national units, private parties or other recipients established in the Union, while transfers should relate to Europol disclosing personal data to private parties, public authorities or bodies established in third countries or to international organisations, in accordance with the applicable rules."

- We do not completely understand the new text of recital 34:

> "Where Member States use the Europol infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, they may decide whether to involve Europol in such exchanges or not. If it is involved, Europol should not have access to data on crimes falling outside the scope of its objectives."

The first and the second sentence seem to contradict each other. Or are we reading this wrong?

Article 7 para 12

- Thank you for also mentioning art 26a in para 12 of art 7.

- We are just wondering whether the article on national units is the right place for this provision? Not all information exchange with private parties takes place through the national units. Maybe it could be included in article 26 on Exchanges of personal data with private parties as a new paragraph 9?

- Art 51 para 3 sub f seems to be about a similar report on the same topic for the JPSG, but it is described differently there. That could suggest that Europol needs to draw up two similar, but different reports on the same topic. Should art 51 para 3 sub f be brought in line with article 7 para 12?

- The word “to” seems to be missing in art 7 para 12:

> “Europol shall draw up an annual report to the Management Board on the personal data exchanged with private parties pursuant to Articles 26 and 26a on the basis of quantitative and qualitative evaluation criteria defined by the Management Board, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks.”

Article 26(2)

- In reply to our question in the LEWP of 8 March about whether the MS where a company is established would be considered a “member state concerned” under art 26 para 2, Europol said something along the lines that this would create an additional burden for both Europol and the recipient and that they would therefore not advise it. However, in a document for the Working Group on Corporate Matters of the Europol MB on 11-12 February (EDOC#1151374v5), Europol writes:

> “The addition of the “seat Member State” of a private party as mandatory recipient of the notification (via its ENU) of personal data that Europol receives directly from the private actors may also be considered. The new paragraph 2 of Article 26 requires Europol only to forward the data to Member States concerned in terms of content; these States are often other than the State in which the private party has its (main) seat or a legal representative. The discussions of the Council Conclusions clearly showed that the seat Member State has an operational need to be informed about suspected criminal conduct detected by a private actor on its territory. Such insertion would also be consistent with the new proposed paragraph 6a, according to which Europol may request the “seat MS” of the private party to obtain personal data from them under certain conditions.”

These two statements do not seem to be completely aligned. What would Europol’s advice be? And in order to get an idea of the additional burden, we were wondering if Europol could tell us how often it expects to receive data from private parties directly under art 26 para 2?

- Since it is currently not clear what it would entail for the “seat Member State” to always be informed about data from private parties in their territory, or conversely what the consequences would be if the “seat Member State” would not be informed, we would like to suggest that rules are drawn up to determine when the “seat Member State” should be informed. The question is whether we need to include something about this in the text of the Regulation itself or whether we can include those rules in the guidelines on processing of information that will be established by the MB under article 18, para 7?

Article 26(6a)

- We have a further question to the Commission regarding article 26 paragraph

5 sub d and paragraph 6a and recitals 30 and 31: should we understand paragraph 5 sub d to be the exception to and/or the specialised version of paragraph 6a? Do we understand correctly that:

> - when Europol receives data from Member States, third countries, international organisations or private parties, but it needs additional information to identify the member states concerned and it thinks that a private party has information that can help it identify those member states, it would normally ask a member state to obtain the additional data from that private party under art 26 para 6a (if the private party is established / has a legal representative in that MS);
>
> - but if the private party which Europol thinks has information that can help it identify those member states is the same private party that supplied the original information, Europol can inform that private party directly that the information received is insufficient to identify the MS concerned under art 26 para 5 sub d?

Is that how these two paragraphs relate to each other?

- In recital 31, the –s seems to be missing from "international organisations" in the first line.

- Recital 32 stipulates that "To ensure that Europol does not keep the data longer than necessary to identify the Member States concerned, time limits for the storage of personal data by Europol should apply." To make sure that it is clear that this recital does not refer to paragraph 6a of article 26, but only to paragraph 2, we would like to suggest the following amendment to the text:

> "To ensure that Europol does not keep the data it has received directly from private parties longer than necessary to identify the Member States concerned, time limits for the storage of personal data by Europol should apply."

Article 26a

We think it is important that in a crisis situation, as formulated in point u of article 4(1), Europol can directly exchange information with a private party to prevent the dissemination of terrorist content. Nonetheless, some safeguards should be put in place to avoid duplication of efforts and interference with investigations in Member States (A). The TCO Regulation (which is currently under negotiation) contains such safeguards, so the safeguards for Europol could be similar to those in recital 36 and article 14 paragraph 1 of the Regulation on TCO. We would therefore like to suggest including some text similar to that in the TCO Regulation here. In addition, we would like the recitals to clarify the difference between the referrals under art 26a of the Europol Regulation and the removal orders under the TCO Regulation, similar to the clarification in recital 40 of the TCO Regulation (B).

A) Avoiding duplication of efforts and interference with investigations

To avoid duplication of efforts and interference with investigations, we would like to propose a new recital 35a, similar to recital 36 of the TCO Regulation:

> "In order to avoid duplication of effort and possible interferences with investigations and to minimise the burden to the hosting service providers affected, Europol should exchange information, coordinate and cooperate with the competent authorities before transmitting or transferring personal data to private parties to prevent the dissemination of online content related to terrorism or violent extremism. Where Europol is informed by a competent authority of a Member State of an existing transmission or transfer, it should not transmit or transfer personal data concerning the same subject matter."

We would also like to propose a new article 26a paragraph 4a, similar to article 14 para 1 of the TCO Regulation:

> "Europol shall exchange information, coordinate and cooperate with the competent authorities with regard to the transmission or transfer of personal data to private parties under paragraphs 3 or 4 of this Article, in particular to avoid duplication of effort, enhance coordination and avoid interference with investigations in different Member States."

B) Making sure that the difference between removal orders and referrals is clear

The Europol Regulation would only apply to referrals (i.e. the transmission or transfer of personal data to prevent the dissemination of online content). The competence to send out removal orders stays with the competent authorities in line with the TCO Regulation that is under negotiation. Recital 40 of the TCO Regulation clarifies the different competences:

> "Referrals by Member States and Europol have proven to be an effective and swift means of increasing hosting service providers' awareness of specific content available through their services and enabling them to take swift action. Such referrals, which are a mechanism for alerting hosting service providers of information that could be considered to be terrorist content for the provider's voluntary consideration of the compatibility of that content with its own terms and conditions, should remain available in addition to removal orders. The final decision on whether to remove the content because it is incompatible with its terms and conditions remains with the hosting service provider. This Regulation should not affect the mandate of Europol as laid down in Regulation (EU) 2016/794 of the European Parliament and of the Council[1] . Therefore, nothing in this Regulation should be understood as precluding the Member States and Europol from using referrals as an instrument to address terrorist content online."

We would like to propose that in order to make sure that the difference is also made clear in the Europol Regulation, a text is included in the recitals of the Europol Regulation that mirrors this recital 40. This text could be added to recital 35:

[1] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

"[Nothing in this Regulation should be understood as precluding the Member States and Europol from using removal orders as laid down in Regulation 2021/…

on addressing the dissemination of terrorist content online as an instrument to address terrorist content online.]"*

*Between square brackets, since the TCO regulation is still being negotiated.

Bloc 3: Strengthening Europol's role on research and innovation

Article 33a

- Thank you very much for following the Belgian suggestion to include some text that there is a preference for synthetic/anonymised data.

- In the Netherlands, there is currently discussion whether under our national law data that has been collected in the course of criminal investigations can be used for the aim of research and innovation. This question has not been settled yet, but will hopefully be clarified in future.

- When it comes to the role of the Management Board regarding projects for research and innovation, para 1 sub b now stipulates that it will be informed prior to the launch of such projects. When it comes to the bigger, more substantial of these projects, we would like it if the Management Board would not just be informed, but consulted. The guidelines drawn up under article 18 para 7 could be used to determine which projects the MB should be consulted on, and where informing the MB should be enough. We would like to propose the following text:

"~~the Management Board and~~ the EDPS shall be informed prior to the launch of the project. The Management Board shall be either consulted or informed prior to the launch of the project, in accordance with criteria laid down in the guidelines, referred to in article 18, paragraph 7."

In order to further explain this, we would like to propose amending recital 39 as follows (in yellow):

"Europol should inform the European Data Protection Supervisor prior to the launch of its research and innovation projects that involve the processing of personal data. Europol should either consult or inform the Management Board prior to the launch of the project, in accordance with criteria such as the risks to all rights and freedoms of data subjects, including of any bias in the outcome, the measures envisaged to address those risks and the scope of the project. For each project, Europol should carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of

personal data and all other fundamental rights, including of any bias in the outcome. This should include an assessment of the appropriateness, **necessity and proportionality** of the personal data to be processed for the specific purpose of the project, **including the requirement of data minimisation**. Such an assessment would facilitate the supervisory role of the European Data Protection Supervisor, including the exercise of its corrective powers under this Regulation which might also lead to a ban on processing. The development of new tools by Europol should be without prejudice to the legal basis, including grounds for processing the personal data concerned, that would subsequently be required for their deployment at Union or national level."

Bloc 4: Enabling Europol to enter data into the Schengen Information System

- We would like to thank the chair for putting the subject of enabling Europol to enter data into SIS on the agenda of this LEWP.

- We can fully support the non-paper presented by France. This non-paper is a good starting point for further discussions.

- We think it is important to first get clarity on the extent of this problem, on where this information gap is.

- Then, discussion needs to take place on which solution would be most suitable. Next to amending SIS, several other options have been suggested by Member States.

- Only after conclusions on this are reached, should IXIM start technical discussions.

- We would therefore like to suggest to continue discussions on the exchange of third country-sourced information in dedicated LEWP meetings. The planned IXIM meeting on 18 March could be changed into an LEWP meeting for this purpose. This could be done in a similar setting as the LEWP Major Sports Events meetings.

- The meetings could be attended by experts from the relevant ministries and LEA.

- We hope you are willing to take this suggestion into consideration.

POLAND

PL comments on blocks 1,3,4,5,7 of Europol regulation

On page 3 of doc. 5388/2/21 REV 2, recitals

Whereas:	*Comment* PL suggest adding in the preamble the following motive : Europol's new legal framework fully respects the principles enshrined in the art. 4.2 of the Treay on the European Union as well as recognizes that national security remains the sole responsibility of each Member State. Since the objective of this Reguation is to strenghten action by the Member States' law enforcement services and their mutual cooperation in preventing and combating serious crime and terrorism Europol's institutional role has to be carefully balance in order to guarantee a neccessary level of benefits for the Member States while maintaining and respecting the very essence of their exclusive competence in the area of national security.

On page 7 of doc. 5388/2/21 REV 2, recital 12

~~(12) It is possible for the Union and the Members States to adopt restrictive measures relating to foreign direct investment on the grounds of security or public order. To that end, Regulation (EU) 2019/452 of the European Parliament and of the Council[7] establishes a framework for the screening of foreign direct investments into the Union that provides Member States and the Commission with the means to address risks to security or public order in a comprehensive manner. As part of the assessment of expected implications for security or public order, Europol~~	Comment PL supports deleting this provision.

~~should support the screening of specific cases of foreign direct investments into the Union that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes.~~	

On page 24 of doc. 5388/2/21 REV 2, Article 4

(r) enter data into the Schengen Information System, in accordance with Regulation (EU) 2018/1862 of the European Parliament and of the Council*, following consultation with the Member States in accordance with Article 7 of this Regulation, and under authorisation by the Europol Executive Director, on the suspected involvement of a third country national in an offence in respect of which Europol is competent and of which it is aware on the basis of information received from third countries or international organisations within the meaning of Article 17(1)(b);	*Comment* PL position as regards entering data into SIS by Europol has been sent on 3 March. PL remains ready to discuss technical details on IXIM as regards, above all, implementation issues in the context of current ongoing changes into SIS and verification of information from third countries.

On page 25 of doc. 5388/2/21 REV 2, Article 4

~~4b. Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council* that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security.~~	*Comment* PL supports deleting this provision

On page 26 of doc. 5388/2/21 REV 2, Article 5

"1. In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the ~~Member State or~~ Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation."	*Comment* PL supports deleting this amendment

On page 26 of doc. 5388/2/21 REV 2, Article 7

"12. Europol shall draw up an annual report to the Management Board on the personal data exchanged with private parties pursuant Articles 26 and 26a on the basis of quantitative and qualitative evaluation criteria defined by the Management Board, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks. The annual report shall be sent to the European Parliament, the Council, the Commission and national parliaments;"	*Comment* In PL opinion including specific examples of cases should be further examined in order to aviod dislosure of operational details of certain cases.

On page 33 of doc. 5388/2/21 REV 2, Article 25

(-a) In paragraph 1, point (a) is replaced by the following: "(a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision') **or in the absence of such a decision, appropriate safeguards have been provided for or exist in**	*Comment* PL supports the amendment. Additionaly, in the Eurojust regulation there is a provision which stipulates conditions when Eurojust may transfer operational data to third countires (art 56 (1)). Among the others, the authorisation of a transfer from the competent authority of Members State is mandatory. PL suggests to include this obligation to Europol regulation as well. **Suggested wording of new paragraph 1a of article 25:** « Where the operational personal data to be

accordance with paragraph 4a of this Article, or in the absence of both an adequacy decision and of such appropriate safeguards, a derogation applies pursuant to paragraph 5 or 6 of this Article;"	transferred in accordance with paragraph 1 of this article have been transmitted or made available to Europol by a Member State, Europol shall obtain prior authorisation for the transfer from the relevant competent authority of that Member State in compliance with its national law, unless that Member State has authorised such transfers in general terms or subject to specific conditions.
(-a *bis*) A new paragraph 4a. is inserted	
"4a. In the absence of an adequacy decision, Europol may transfer operational personal data to a third country or an international organisation where:	In the case of an onward transfer to another third country or international organisation by a third country or international organisation, Europol shall require the transferring third country or international organisation to obtain the prior authorisation of Europol for that onward transfer. »
(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or	
(b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data."	

ROMANIA

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

Additional written comments on blocks 1, 3 and 5

- **Block 1: enabling Europol to cooperate effectively with private parties**

- Art. 4 (1) (m). With regard to the support of Member States' actions in the fight against online crime, it is important to highlight *on a case by case basis*.

- Regarding **the transfer personal data to private parties established outside the EU on a case-by-case basis, where it is strictly necessary, and subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and only in the cases regulated by Art 26 (5) (a-d).** In this context, we agree this initiative to restricted the transfer of personal data only in the specific cases and **we underline the same restriction should aplly accordingly to private parties established within the EU**.

- **Block 3: strengthening Europol's role on research and innovation**

-Art. 4 paragraph 1 (4a). We support FR position (doc.5527/21). In our opinion, the wording from paragrapf 4a is missleading because creates the image that Europol is the only Agency that supports COM and MSs for identifying main innovation themes in the security field. Besides Europol, there are other JHA Agencies that could support these efforts.

- The scope of the research and innovation activities should be better defined in the Europol Regulation.

- **Block 5: strengthening Europol's cooperation with third parties**

- Art 25 paragraph 4a. For the text coherence, the distinction between personal data and operational personal data should be highlighted. In the Directive (EU) 2016/680, chapter V

(Transfers of personal data to third countries or international organisations), the term used is personal data.

-Art. 25 paragraphs 5 and 6. Additional information / clarifications are needed on the meaning of "*categories of transfers*", as well distinction "*from set of transfer*".

SLOVENIA

With reference to the Informal videoconference of the members of the LEWP on 16. 3. 2021, regarding the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation **- block 4 and questions written in the Summary of discussions, please find bellow answers of Republic of Slovenia.**

1.	Do you totally agree with the legal text of article 4, 1, r)?	**YES**
2.	Should this article 4, 1, r) have a more general and/or revised formulation? The MS that think so, please send us written text proposals (wording) to this article 4, 1, r).	**NO**
3.	Should we include new article(s) with alternative solutions?	**NO**
4.	Do you think that this article 4, 1, r) should be deleted?	**NO**

5.2. WRITTEN COMMENTS ON THEMATIC BLOCK 2

BELGIUM

Written contribution BELGIUM concerning block 2 (enabling Europol to process large and complex datasets) – LEWP meeting 08.03/2021

- Belgium considers this bloc one of thé most important issues of the Europol Regulation recast. We appreciate that the European Commission is clearly also determined to find a sound solution for the current interpretation of the EDPS on Europol's possibilities to process datasets. It will be especially important to make sure that:
    - Firstly, the new articles will leave no room for further interpretation problems, especially towards the EDPS. We do not want a new EDPS decision challenging the possibilities for Europol.
    - Secondly, the solutions make sense from a practical operational perspective and it is clear how to fit these solutions in the current existing dataflows to Europol, especially when sending Europol data for operational analysis purposes.
- While the explanation of the Commission during the LEWP meeting has provided some more clarity, we still have open questions and doubts with regard to the relevant articles for block 2. We need more time to further look into several issues and this is why we want to enter **a scrunity reservation** at this time.
- However, we want to use this opportunity to indicate what issues we still have and want to ask a few questions for further consideration and or clarification:

1. **The new concept of an "investigative case file":**
    - Definition in article 2 (q)
        - Do we really need the terminology of "datasets"? There is no definition of a "dataset" in the Regulation and this might pose a risk of difference of interpretation between the EDPS and Europol when applied in practice. Would a reference to "data" not be sufficient?
        - While the Commission's response to our question if the definition would also cover the pro-active phase of an investigation was reassuring, we still contemplate whether or not it would not be advisable to explicitly clarify this in a recital. Again, to avoid future interpretation issues for the EDPS.

- The necessity of using the concept of an "investigative case file"
  It is not clear for us how this new concept would work in practice, also taking into account how the feeding op Analysis Projects is currently organised. The introduction of this concept consequently means that it will be necessary to describe the concept more in detail on the practical use of it by Member States. We have a lot of questions in this regard. The MS would be required upon sending the data to indicate themselves that this concerns an investigative case file. That would probably mean that MS already have to assess themselves that the data they send contains data outside the categories of data listed in Annex II. So, in other words, would MS only use this specific concept when sending data when they already have assessed themselves that they are sending data outside Annex II. Or would Europol – upon verifying the data – also be able to qualify the received data as an investigative case file?
  This is absolutely not clear for us at this time and we would welcome further clarification on this. This unclarity is also a consequence of the definition as the definition does not contain a reference to the fact that the data sent does or might contain data outside Annex II.
  In this context and depending further clarification, we are not convinced that we need the concept of an investigative case file. It could be sufficient to integrate (part) of the definition in the text of article 18a. The advantage of this would then be that there is no need to further specify practical (future) procedures to enable the use of an investigative case file.

2. The "rationale" behind the 2 new possibilities inserted in article 18.5a and article 18a

The explanation of the Commission was confusing for us. The Commission stated that article 18.5a would be a "subset" of article 18a. The meaning of this is not clear for Belgium.

Our understanding of the proposal (in our criminal law system) would be the following: if we have the possibility to process data outside Annex II according to our system, Europol would be able to process the data too provided that Europol's support is necessary for our investigation. Or in other words each time a MS sends Europol data outside of the categories listed in Annex II and Europol's support is crucial for the MS's investigation Europol will be allowed to process these data. It is important for us if the Commission and/or the Council's Legal Service would confirm this explicitly as this is crucial for our analysis to decide whether or not the proposal reassures Europol's analytical support for the Member States for the future.

3. Article 18.5a – prior authorisation of the EDPS to extend the one year period

Taking into account the current experiences of cooperation with the EDPS, the EDPS would probably be asking Europol to introduce this a few months ahead of the expiration of the one year period. We assume however that this would not suspend the one year period and whatever the outcome Europol would still be able to keep the data for the maximum period of one year? We would welcome if the Commission could confirm this interpretation.

4. Article 18a : some questions for clarification

- Article 18a.1 states "Where necessary for the support of a specific criminal investigation (…)". Who will decide on the necessity part? Is this something to be clarified in the conditions to be specified by the MB and the EDPS? Does the Commission have a particular view on this? Is this "where necessary" the same as the Europol assessment mentioned in article 18a.1 (b)? If not, could the Commission clarify?
- Could the Commission explain how Europol would have to provide a credible assessment provided for in article 18a.1 (b)? In practice, if the MS clearly indicates that it needs Europol support, would Europol not be expected to confirm this?

5. Article 18a. 4

We currently consider the role of the EDPS to go too far, as the EDPS is given a role in an operational live processing of information. We will probably propose to delete this role for the EDPS.

BULGARIA

Bulgarian contribution to the draft

Regulation amending Regulation (EU) 2016/794, as regards the processing by Europol of multiple datasets (Thematic block 2)

General comments:

First of all, Bulgaria appreciates the overall purpose of this thematic block to properly reflect the decision of the EDPS on the processing of multiple datasets by Europol. We believe that the proposed approach successfully mitigates the risks related to this processing. The proposed provisions regulate in details the possible exemptions by processing multiple datasets and in the same time contain the necessary guarantees for the personal data protection, which should be done in a proportionate manner and to be limited to the strictly necessary purposes. In our opinion the draft provisions ensure a high level of cooperation and consultation between Europol and the EDPS and we could express our principle support.

Comments text by text:

Concerning **the new letter (q) of Article 2** containing definition of "investigative case file" we would like to ask the Commission for additional clarification whether a scenario is envisaged in which other EU agencies, such as OLAF and Frontex can provide datasets in support of criminal investigation or the way to provide such data will be through the MS concerned or through EPPO.

Regarding Article 18 (5) we could support the proposed text and we have only a small technical remark. The wording of Letter B of Annex II should be updated and letter (f) of para 2 should also be added.

Annex II

*B. Categories of personal data and categories of data subjects whose data may be collected and processed for the purpose of analyses of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information as referred to in points (b), (c), (d) and **(f)** of Article 18(2).*

On the new Article 18(5a) Bulgaria would like to ask for clarification from the Commission and Europol (from practical perspective) regarding the new para 5a and the already existing para 6 and to be sure that there will be no duplication or contradiction with this text considering the temporary processing of data and the deadlines envisaged.

As far as we understand para 5a is regulating the temporary processing of data, received by Europol in order to determine whether these data fall within the categories of data and categories of data subjects listed in Annex II. These data could be collected and processed for the purposed of para 2, points a) to d) and f) and the maximum period for this temporary processing of personal data is 1 year with a possible prolongation.

Paragraph 6[1] is also provided for temporary processing of data for the purpose of determining whether these data are relevant to Europol's tasks and, if so, for which of the purposes referred to in paragraph 2. But the maximum period in this provision is 6 months.

Our questions are: When Europol receives personal data for temporary processing, it will be done under which provision and how will be calculated the maximum periods? Can these temporary data processing under para 5a and para 6 be performed simultaneously or they have to be done one after another? Which one has to be first and whether the outcome of the one temporary processing will influence on the initiation of the second one?

Regarding the new Article 18a Bulgaria has the following comments:

On para 1 a) taking into account that EPPO as a Union body is covered by Art. 17, para 1, point b) we propose the wording "pursuant to point a) of Article 17 (1)" to be deleted because the reference is to proving of data by the Member States through the Europol National Units.

We also have concerns about the limitation that the data provided with an investigative case file can be processed only for the purpose of operational analysis pursuant to point (c) of Article 18(2) but not for example for cross-checking under art. 18 (2) (a) in order to identify connections or other relevant links with data already stored in Europol data bases or even with other on-going investigations in other MS or third countries operational (18 (2) (d)).

On para 3, second sentence we are on the opinion that any Member State should have the possibility, when identifying that data provided by an investigative case file and the outcome of their analysis are related to on-going criminal investigation on its territory, to request Europol to store the investigative case file and the outcome of its operational analysis with the preliminary consent of the Member State provided this investigative case file.

We propose the following sentence to be added after the second one:

In case where an on-going related criminal investigation in another Member State is identified during processing of data from investigative case file provided by a Member State or the EPPO pursuant to paragraph 1, this another Member State, with the prior consent of the provider of this investigative case file, may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going.

[1] 6. Europol may **temporarily process data** for the purpose of determining whether such **data are relevant to its tasks** and, if so, for **which of the purposes referred to in paragraph 2**. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data, in particular with respect to access to and use of the data, as well as time limits for the storage and deletion of the data, which may not exceed **six months**, having due regard to the principles referred to in Article 28

We would also like clarification from the Commission and Europol, if during the processing of these data connections and links are identified with data already collected and stored in the operational analysis projects under art.18 (3), whether these data could be transferred and stored in these analysis projects or this will be subject of additional regulation from the MB.

On para 4 of article 18a

We will be grateful to receive more information by the Commission on the process of informing EDPS by Europol when the Agency receives investigative case file by a third country. What kind of information will be exactly provided to the EDPS and will it be enough, in order to allow EDPS to take a decision that there are preliminary indications that these data are collected in disproportioned manner or in violation of the fundamental rights.

If such a decision is taken, Europol should not only be prohibited to process them, but it should also delete/erase them.

We would also like to have clarification if this information providing to EDPS could be interpreted as asking approval for data processing and what would happen if Europol has started data processing and later on the EDPS take a decision that these data are collected in disproportioned manner or in violation of the fundamental rights and meanwhile Europol has identified valuable links. Also what happens in case of urgency?

We would like also to receive the opinion of the Europol on these questions.

Last sentence of para 4 and the wording "**It shall be shared only within the Union**", we believe that an amendment is needed taking into account that the data received by a third country and the outcome of their operational analysis should be shared with the Member States which investigations are supported (both Member State provider of this investigative case file and Member states with on-going related criminal investigation). In a scenario when the third country provided the data has initiated its own parallel investigation, Europol should also have the right to share the outcome of the operational analysis with this third country operational with the prior consent of the provider of this investigative case file.

Our proposal for this last sentence is

"It shall be shared only with the Member States and third countries concerned with the prior consent of the provider of this investigative case file. "

As a final remark, we would like to express our opinion that Europol should participate fully in the LEWP meetings on the new Europol Regulation, in order to provide timely responses to Member States' questions and to be aware of the direction of the discussions.

CZECH REPUBLIC

CZ comments on Europol recast – bloc 2

CZ shares the opinion of other delegations that further systemic interference with processing big data based on EDPS data protection concerns should be prevented or minimized. Therefore, CZ proposes the following:

Article 2(q)

This definition, in particular the words "in the context of an on-going criminal investigation", may cause problems, because it does not explicitly address certain situations, such as when the dataset is acquired:

- before the investigation, such as when cyber security authority finds stolen dataset in the course of response to cyberattack, and then the police starts investigation,

- in the context of non-criminal investigation of legal person for (a criminal) offence and subsequently used in criminal investigation of natural person.

CZ proposes to broaden the definition in order to prevent future restrictive interpretation, or at least to provide further clarification in recital 17.

Article 18(5a)

We understand the explanations of the Commission to mean that this is a "pre-check procedure" and (legally) yields no analytical results. Thus we refrain from regulating such results. However, the last subparagraph is probably too strict. The Europol should be given the option to delete (in agreement with the provider of data) the superfluous part of the data (i.e. data in excess of Annex II), where it is feasible (e.g. data collated from multiple sources or files, which are clearly separable). If that is already intended, it should be clarified in a recital.

Article 18a(2)

Word "file" is missing in the first line.

We understand the explanations of the Commission that the link to particular criminal investigation is crucial to establish limits for processing of categories of data and data subjects in excess of Annex II and duration of processing, which necessarily restricts the standard forms of processing to operational analysis pursuant to Art. 18(2)(c). However, we believe that at least limited instances of "cross-checking" of the file against the data already held by Europol could be enabled if requested and justified by the file provider due to possible operational value. Hence, the last sentence could read: "… they were provided **unless the Member State or EPPO that provided an investigative**

case file requests, in exceptional and duly justified cases, to carry out processing referred to in Art. 18(2)(a).”

Article 18a(4)

We appreciate the explanation of the Commission that the role (veto, in fact) given to EDPS should raise the bar for third countries. However, we regard is as a kind of slippery slope, which is contrary to the core supervisory responsibilities of EDPS. Europol must remain responsible for the processing it controls. There is no reason to give the EDPS an executive responsibility.

Given the proliferation of foreign advanced law enforcement technologies available for many developing third countries, it is in the long-term interests of the EU not to dissuade such third countries from cooperating with Europol.

CZ may accept the notification of EDPS as such, inter alia because it does not lead to delays in processing of investigative case file by Europol.

(end of file)

FRANCE

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leurs commentaires écrits suite à la réunion de groupe LEWP du 8 mars 2021 s'agissant de la révision du règlement d'Europol *(5397/21, 5527/21 REV3, 5388/21 REV2, WK 757/21 REV2) :*

- **Concernant le bloc thématique n°2 (permettre à Europol de traiter des ensembles de données importants et complexes) :**

Les autorités françaises rappellent accueillir favorablement les dispositions permettant à Europol de traiter des données obtenues auprès de parties privées, des données de masse ou des données obtenues dans le cadre d'enquêtes de grande ampleur répondant à des enjeux opérationnels centraux. Elles garantissent la pérennité du modèle de fonctionnement de l'agence dans le cadre des obligations posées par le CEPD, vis-à-vis du règlement 2016/794. Les autorités françaises souhaitent cependant faire état des commentaires ci-dessous.

Reference in proposal COM(2020) 796 final	
Proposition de la Commission	**Commentaires des autorités françaises**
Article 1(1)(c) prévoit un nouvel article 2 (q) dans le règlement (UE) 2016/794 *Article 1* Regulation (EU) 2016/794 is amended as follows: (1) Article 2 is amended as follows: […] (c) the following point (q) is added: "(q) 'investigative case file' means a dataset or multiple datasets that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation, in accordance with procedural requirements and safeguards under the applicable national criminal law, and submitted to Europol in support of that criminal investigation."	Les autorités françaises estiment nécessaire de préciser dans cette définition la nécessité, pour le dossier d'enquête des États-tiers, d'être **manifestement lié** à une enquête d'un ou de plusieurs États membres.
Article 1(5)(c) amende l'article 18(5) dans le règlement (UE) 2016/794 *Article 1* Regulation (EU) 2016/794 is amended as follows: […]	

Reference in proposal COM(2020) 796 final	
Proposition de la Commission	**Commentaires des autorités françaises**
(5) Article 18 is amended as follows: […] (c) paragraph 5 is replaced by the following: "5. Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II."	
Article 1(5)(d) prévoit un nouvel article 18(5a) dans le règlement (UE) 2016/794 *Article 1* Regulation (EU) 2016/794 is amended as follows: […] (5) Article 18 is amended as follows: (d) the following paragraph 5a is inserted: "5a. Prior to the processing of data under paragraph 2 of this Article, Europol may temporarily process personal data received pursuant to Article 17(1) and (2) for the purpose of determining whether such data comply with the requirements of paragraph 5 of this Article, including by checking the data against all data that Europol already processes in accordance with paragraph 5. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Europol may only process personal data	Pas de commentaire

Reference in proposal COM(2020) 796 final	
Proposition de la Commission	**Commentaires des autorités françaises**
pursuant to this paragraph for a maximum period of one year, or in justified cases for a longer period with the prior authorisation of the EDPS, where necessary for the purpose of this Article. Where the result of the processing indicates that personal data do not comply with the requirements of paragraph 5 of this Article, Europol shall delete that data and inform the provider of the data accordingly."	
Article 1(6) prévoit un nouvel article 18(a) dans le règlement (UE) 2016/794 *Article 1* Regulation (EU) 2016/794 is amended as follows: […] (6) The following Article 18a is inserted: *"Article 18a* Information processing in support of a criminal investigation 1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where: (a) a Member State or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2); and (b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded. 2. Europol may process personal data contained in an investigative case for as long as it supports the on-going specific criminal investigation for which the investigative case	Les autorités françaises saluent l'initiative de la Commission européenne et sa proposition. Toutefois, elles s'interrogent sur le caractère restreint du paragraphe 1 limité à l'analyse opérationnelle. Il semble tout à fait envisageable de permettre à Europol de traiter des données dans le cadre de dossiers d'enquêtes à **des fins d'analyse opérationnelle, mais également de recoupement**.

Reference in proposal COM(2020) 796 final	
Proposition de la Commission	**Commentaires des autorités françaises**
file was provided by a Member State or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided. 3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State. That Member State may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a related criminal investigation are on-going in another Member State. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such	

Reference in proposal COM(2020) 796 final	
Proposition de la Commission	**Commentaires des autorités françaises**
data. Such personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process. 4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, or the EDPS, reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union.”;	

- **Concernant le bloc thématique n°4 (permettre à Europol de traiter des ensembles de données importants et complexes) :**

Les autorités françaises réaffirment leur opposition à ce qu'Europol puisse se voir confier un rôle d'alimentation dans le SIS et se réfèrent à leur «Non-papier » transmis en début de semaine en ce qui concerne les solutions alternatives proposées.

Par ailleurs, les autorités françaises rappellent qu'elles souhaitent qu'un examen complémentaire des solutions alternatives soit conduit en LEWP, ceci pouvant même être fait dans cette enceinte en lieu et place de la réunion IXIM prévue le 18 mars prochain. Elles précisent également que les discussions techniques ne peuvent commencer qu'une fois que les États membres seront parvenus à des conclusions sur ce point.

GERMANY

Germany's follow-up comments to the LEWP meeting on 8 March 2021 (Revision of the Europol Regulation) – Thematic bloc 2

Please find below Germany's written comments on thematic bloc 2 following the last LEWP meeting on 8 March 2021. Further comments may be raised following ongoing scrutiny of the proposal.

Germany welcomes that the legislative proposal addresses this very important issue. As we all know, it has become urgent to address Europol's ability to process big data in accordance with relevant data protection principles since the EDPS' decision on the big data challenge. As the Ministers have expressed in their Declaration on the Future of Europol, it is of key importance to Member States that Europol will be able to continue to support Member States in this regard.

We support the fundamental approach of the proposal and generally agree with the provisions brought forward. At the same time, the processing of large and complex datasets (beyond the limitations of Art. 18(5) and Annex II) raises questions concerning data protection and fundamental rights and must strictly be limited to what is necessary and proportionate to achieve the objectives covered by Europol's mandate.

Below you will find a few specific comments and questions:

Article 2(q):

We wondered whether it should read *„the competent authorities of a Member State, the EPPO or the competent authorities of a third country"*.

Furthermore, we suggest phrasing it *„under the applicable Union law and national criminal law"*, as e.g. the EPPO acts upon legal instruments under Union law.

On a more general note, we would appreciate an explanation what the term *"investigative case file"* means exactly. In the context of Article 18a, *"personal data from an investigative case file"* seems more fitting.

Article 18(5):

What is the purpose of the introductory amendment (*"Without prejudice to Article 8(4) and 18a, categories…"*)? Article 8(4) specifies only that Liaison Officers may use Europol infrastructure for exchanging information between their Member States and the liaison officers of other Member States, third countries and international organisations without involving Europol.

Article 18(5a):

Why does paragraph 5a in its first sentence refer to Article 17(1) and (2)? Paragraph 6 does not contain such a restriction or specification to the sources of information mentioned in Article 17. What purpose does the reference serve?
We would also appreciate a clarification on the relationship of Article 18(5a) and Article 18a. In particular, with regard to Article 18(5a) it would be of interest to know whether the checking of data against other data processed by Europol is a feasible method to fulfil the purpose set out in the first part of the provision.

Furthermore, a clarification on the relationship between Article 18(5a) and Article 18(6) would be appreciated.

The second sentence concerns the establishment of further conditions related to the processing under the first sentence. A similar provision can be found in the second sentence of paragraph 6, whereby the latter refers not only to *"conditions relating to the processing of such data"*, but more specifically to *"conditions relating to the processing of such data, in particular with respect to access and use of the data, as well as time limits for the storage and deletion of the data"*. Is there a reason why there is no complete alignment between these provisions?

We welcome the maximum period of one year foreseen in the third sentence, as it is reasonable and corresponds with the time limits in our national legislation. We would appreciate an explanation, though, why paragraph 6 provides for a shorter maximum time period than paragraph 5a.

As the processing powers only serve the purpose of determining compliance with paragraph 5, why does the third sentence refer to *"where necessary for the purpose of this Article"*? This should rather read *"...of this paragraph"*.

The fourth sentence sets out that in the event of deletion of the data Europol shall inform the provider of the data accordingly. In our view, this obligation does not make sense in cases where Europol has retrieved the information from publicly accessible sources including the Internet pursuant to Article 17(2). Who would be the addressee of such notification in this case?

We have noticed that while the new Article 18a stipulates that the data shall be functionally separated (cf. paragraph 2 third sentence and paragraph 3 third sentence), Article 18(5a) does not contain such requirement. From a data protection perspective, the separation of categorised and non-categorised data would presumably make sense and would certainly be welcomed by the EDPS in particular.

Article 18(6):

In view of the fact that Article 28 is to be deleted, the reference in the second sentence to Article 28 should either be deleted or replaced by a reference to Article 4 of Regulation (EU) 2018/1725 (Principles relating to processing of personal data).

Article 18a(1):

It should be ensured that Art. 18a is applied on an exceptional basis and thus prevent the risk of the exception becoming the rule. Therefore, the provisions should lay down certain conditions that must be met to apply the derogation from Art. 18(5), such as scale, complexity, type or importance of the investigations.

Regarding point (b), it is not clear what the test behind *„that it is not possible“* entails. Does this mean technical impossibility? Would Europol have to arrange that the *„case file“* is processed in a way that categories of personal data that do not comply with the requirements of Article 18(5) are filtered out to the greatest extent possible? Will processing be permissible on a provisional basis then?

Against the background that our national law enforcement authorities also see a need for support as foreseen by Article 18a in the area of preventing crime, why does Article 18a(1) specifically refer to cases of Article 18(2) point (c)?

Eventually, Article 18a(1) concerns the general question of cooperation between Europol and EPPO. From our point of view, it does not make sense to deal with individual aspects of this topic outside the context of the underlying general issue. May we therefore suggest that all questions related to the EPPO be dealt with comprehensively in the context of thematic bloc 6. To that end, Germany enters a scrutiny reservation on all EPPO related aspects of the proposal.

Article 18a(2) and (3):

The provisions are partly redundant and could also be combined in an extended paragraph 2. The current paragraph 4 could then be renumbered as paragraph 3. The reference to paragraph 3 in paragraph 4 would have to be adapted accordingly.

Our proposal for wording for an extended provision based on paragraph 2:

> *“2. Europol may process personal data contained in an investigative case for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by a Member State [or the EPPO] in accordance with paragraph 1, and only for the purpose of supporting that investigation. Upon request of the Member State [or the EPPO] that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond that storage period, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State or in a related criminal investigation in another Member State based on the outcome of the operational analysis of Europol and provided by the requesting Member State to the other Member State in accordance with national law.*
> *The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data.*
> *Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be processed where necessary and proportionate for the support of the specific criminal investigation for which they were provided or for the*

purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process."

On the bracketing of EPPO, see the above commentary. Whether EPPO is to be included should be revisited when discussing thematic bloc 6.

Article 18a(4):

The part after *„with which ...“* could be aligned with the order used in Article 25(1).

The relationship of the third sentence (*"Europol shall verify .."*) and the fourth sentence (*"Where Europol ..."*) remains unclear. If the processing is already prohibited where preliminary indications of disproportionality or fundamental rights violations exist, the higher threshold in the former sentence may be unnecessary. If this was the case, both sentences could be combined into one sentence along the requirements in what is now the latter sentence.

The last sentence should read *"... be processed by Europol where necessary and proportionate..."* (cf. above drafting proposal).

LITHUANIA

We would like to mention that we do not have any general remarks/comments on the thematic block 2 of the Revision of Europol Regulation.

NETHERLANDS

Comments the Netherlands on bloc 2 of the Europol Regulation following the LEWP of 8 March 2021

- Enabling Europol to process large and complex datasets

We are still studying this thematic bloc, so these are only some preliminary questions. We reserve the right to make further comments at a later stage.

Article 18(5a)

- What is the difference between checking the data against data already held by Europol and cross-checking the data?

- How are the pre-analysis under art 18 para 5a and the analysis under art 18a connected? Do you foresee that personal data that has been subject to a pre-analysis under art 18 para 5a and is found to contain data that does not comply with annex II, will always be resubmitted under art 18a?

Article 18a

Paragraph 2

- The word "file" seems to be missing from the first sentence: "Europol may process personal data contained in an investigative case [file?] for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by a Member State or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation."

- What does "functionally separated from other data" mean? Does it mean that the data will not be cross-checked against those other data?

Paragraph 3

Part of the first sentence reads: “for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process”. The second sentence contains the same words, but without the word “sole”. Is that intentional?

Paragraph 4

Article 18a para 4 says that if a third country provides an investigative case file to Europol, Europol needs to verify that “there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights.” Could the Commission explain why this requirement of compliance with fundamental rights has been included here? Does Europol also have to check for fundamental rights when it receives personal data from third countries under other provisions of the Regulation like article 23 para 5?

POLAND

PL comments on block 2 of Europol regulation

On page 27 of doc. 5388/2/21 REV 2, Article 18

"5. Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in **points (a) to (d) and (f) of** paragraph 2 are listed in Annex II."	Comment: In PL opinion it would be reasonable to discuss these amendment within Block 8: strengthening the data protection framework applicable to Europol
"5a. Prior to the processing of data under paragraph 2 of this Article, Europol may temporarily process personal data received pursuant to Article 17(1) and (2) for the purpose of determining whether such data comply with the requirements of paragraph 5 of this Article, including by checking the data against all data that Europol already processes in accordance with paragraph 5.	Comment: PL supports the EDPS remark and question as regards the need for further clarification of relation between new para 5a and exiting para.6 in terms of differences between temporary data processing discribed in both para. PL would appreciate some more explanation by what other means Europol may determine if data comply with requirements of art. 18(5). « Including by checking... » suggests that this is not the only way.
Europol may only process personal data pursuant to this paragraph for a maximum period of one year, or in justified cases for a longer period with the prior authorisation of the EDPS, where necessary for the purpose of this Article. Where the result of the processing indicates that personal data do not comply with the requirements of paragraph 5 of this Article, Europol shall delete that data and inform the provider of the data accordingly."	Comment: In case of data obtained form MS, PL suggests adding the consent of data provider (MS) for extending the processing period. Including neccessity and proportionality assessment before the prolongation could be considered.

On page 28 of doc. 5388/2/21 REV 2, Article 18a

"Article 18a **Information processing in support of a criminal investigation**	Comment: Bearing in mind the siginficant impact of these amendment to the whole data processing rules and data protection framework applied to Europol, it is worth to take EDPS opinion into consideration and explore the possibility to accomodate its remarks.
(b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded.	Comment: PL needs further explanation as regards when carring out the operational analysis of the investigative case file, without processing personal data that does not comply with the requirements of Article 18(5), might tke place. A practical example would be appreciated.

On page 29 of doc. 5388/2/21 REV 2, Article 18a

Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided.	Comment: How it will be implemented in terms of practical and technical aspects ? A practical example would be appreciated. Are these data going to be stored in separated repository ?
3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State.	Comment: Does the pre-analysis procedure (temporary processing) set in art 18 (5a) as regards determining compliance with requirements from art. 18(5) apply? Or is the intention that this provision guarantees legal basis for storage purposes only without any Europol access to it?.
That Member State may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a	Comment: Are these data going to be stored in the same repository ? Question to Europol : what technical means are

related criminal investigation are on-going in another Member State.	at Europol's disposal to guarantee that ? PL suggests reformulating the last part of the sentence as follows : « as long as judicial proceedings following a related criminal investigation are on-going in **requesting Member State** or another Member State. »

On page 30 of doc. 5388/2/21 REV 2, Article 18a

the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, or the EDPS, reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it.	Comment: The considered Member State or Member States should be informed as well. Further clarification is needed. It will be very difficult to verify in practice. How Europol will conduct such verification and are there appropriate tools at its disposal ? What if Europol reaches the conclusion that amount of personal data is disproportionate, however the data set contains crucial data for further criminal investigation in MS ? PL suggests exploring a possibility of including the provision regarding requesting a third country to narrow the scope of data.

ROMANIA

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

Block 2

From the point of view of personal data protection, due to the extension of EUROPOL's competences, a large volume of personal data will be processed. In order to ensure legal transparency and guarantees of processing in compliance with the principles of data protection, RO proposes that the terms used in the field of data protection to be defined, namely "personal data", "data subject", "genetic data", "processing of personal data", "transfer of personal data", " personal data breach".

Keeping these definitions is important, given the challenges of big data processing, reported in detail in the EDPS opinion. The purpose is to enable Europol to analyze such data, while respecting personal data, and it is therefore important that there are clear rules and references regarding data protection.

In the same context, **RO suggests that the definition of biometric data to be added.** So, at **art 1 (1) a new d) point to be introduced** as follows:

„(d) the following point (r) is added:

„(r) biometric data 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

We consider that the proposed regulation should be completed with an article on keeping a register of personal data processing, in order to align these provisions with current practice in the field of personal data protection.

Art 18 (5a). Additional information is needed on the cases when Europol may request extension of the maximum period of 1 year. RO sustains EDPS opinion 4/2021 on Art 18 (5a) when Europol

regulation should provide sufficient safeguards to ensure that the derogations under Art 18 (5a) and Article 18a would not in reality become the rule.

Art 18a (2) the third subparagraph. RO underlines that the processing of personal data outside of those listed in Annex II should be performed in compliance with the general principles and obligations laid down in Regulation (EU) 2018/1725.

SPAIN

BLOCK 2:ENABLE Europol to Process large and complex datasets			
article	**COMENTARIO DELEGACIÓN ESPAÑOLA**	**SPANISH DELEGATION COMMENTS**	***texto***
2q	Parece razonable que los estados miembros, el EPPO y terceros estados puedan introducir datos que se consideren de interés. Convendría aclaración sobre la implementación de este último punto.	It seems reasonable that EPPO, member states and third states can enter data that are considered to be of interest. Clarification on the implementation of this last point would be welcome.	***(q) 'investigative case file' means a dataset or multiple datasets that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation, in accordance with procedural requirements and safeguards under the applicable national criminal law, and submitted to Europol in support of that criminal investigation.***
18. 5	El texto: "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II." debería decir "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II."	The text: "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II." should be modified as follows: "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II."	***CWithout prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II.***

BLOCK 2:ENABLE Europol to Process large and complex datasets			
article	**COMENTARIO DELEGACIÓN ESPAÑOLA**	**SPANISH DELEGATION COMMENTS**	***texto***
18. 5a	No hay comentarios. Se considera adecuado	No comments. It is considered appropriate	***5a. Prior to the processing of data under paragraph 2 of this Article, Europol may temporarily process personal data received pursuant to Article 17(1) and (2) for the purpose of determining whether such data comply with the requirements of paragraph 5 of this Article, including by checking the data against all data that Europol already processes in accordance with paragraph 5.***
18a	Se entiende que los datos obtenibles públicamente se podrán tratar, aún no siendo de los del Anexo II. Se propone aclarar este punto.	It is understood that publicly available data may be processed, even if they are not Annex II data. It is proposed to clarify this point.	***Páginas 20-21 del doc. Wk00757***

SWEDEN

Sweden's first preliminary comments to Block 2, Europol handling of Big Data. We reserve ourselves the right to come back with more at a later stage.

General

SE considers Article 18 to be one of the most important articles of Regulation as it regulates how personal data may be handled in Europol's operational activities. Europol's support for Member States has evolved in recent years from primarily being a more reactive intelligence exchange to also include more direct operational support in ongoing, high-priority cases. The proposal needs to be clear and the use of language harmonised in order to avoid ambiguities.

Article 1(1)(c) — new Article 2(q) Definition of the new concept of "investigative case file".

The concept should be broadened to include active intelligence matters. A broader definition of the concept better corresponds to operational needs and Europol's mandate. Broadening to include intelligence matters is important in order to support Europol and Member States' work with operational task forces and distinguishes the concept from future initiatives concerning a Case Management System for Joint Investigation Teams (JIT).

Article 1(5)(c) — Revised Article 18(5)

SE can support the proposal that "investigative case files" should be exempted from the requirements of Annex II.

Article 1(6) – new article 18a

SE can accept the article. However, it should be considered to harmonise the language between Articles 18(5a), 18a and also 20(2a) (note 20(2a) question block 9) to give a better understanding.

6. COMMENTS RECEIVED AFTER THE MEETING ON 12 APRIL 2021

6.1. FOLLOW UP /ADDITIONAL WRITTEN COMMENTS ON BLOCKS 1, 2, 3, 5 AND 7

BELGIUM

Written comments following LEWP meeting of 12 April

Following the LEWP meeting of 12 April, Belgium would like to submit written comments in relation to block 2, block 3 and block 5.

Block 2: enabling Europol to process large and complex datasets

Preliminary comments

- Following our earlier written contribution on block 2, Belgium would like to repeat that we consider this bloc one of thé most important issues of the Europol Regulation recast. In that context, the aim of this bloc should be, firstly, to leave no room for further interpretation problems as we do not want a new EDPS decision challenging the possibilities for Europol. Secondly, the solutions have to make sense from a practical operational perspective and it must be clear how to fit these solutions in the dataflows from MS to Europol.

- Taking into account the above and the answers by the Commission (which have again contributed to more confusion) to some of our questions contained in our earlier written contribution, we unfortunately are still not convinced that the proposals contained in Article 18(5a) and Article 18a are sufficiently clear both from the perspective of leaving no room for interpretation and practical feasibility. **Therefore, we are not able to lift our scrutiny reservation on this block.**

- The text of Article 18(5a) and Article 18a is meant to provide a solution for the EDPS admonishment of September 2020. As the EDPS mentioned in its opinion on the amendment of the Europol Regulation "the processing of large datasets has thus become an important part of the work performed by Europol to produce criminal intelligence". The recent operations like "Encrochat" and "SKY EEC" have only further confirmed this evolution. A more and more analytically led manner for investigations becomes even more prominent. In that context – as was already confirmed by the Europol Management Board – Belgium wants to ensure that Europol is fully able to continue to support the Member States in order to analyse complex and large amounts of unprocessed data. This means **that Belgium wants Europol to be allowed, to the maximum extent, to process data outside of Annex II in order to support our criminal investigations.**

The relation between Article 18(5a) and Article 18a

- The possibility as described under Article 18(5a) was described by the Commission (during the LEWP meeting of 12 April) as the "first test", implicating that this should always be the first step before applying Article 18a. Belgium does not agree to this, as we believe that in most cases Europol will receive data in the context of a criminal investigation and thus Article 18a would have to apply immediately. This also makes more sense as – when applying the logic of the Commission – applying Article 18(5a) as "a first test" would end up in the deletion of all of the data outside Annex II (unless there is a "justified case with prior authorisation of the EDPS") after one year. The latter is difficult to align with the regime contained in Article 18a. **For Belgium this means that Article 18a – as in reality Europol will receive the data in the case of a criminal investigation – will in reality have to be applied first in most cases and would thus be the rule and the "first test" in Article 18(5a) would not have to be applied.**

We therefore are of the opinion that **Article 18(5a) would only be applied** when data is sent to Europol **when there is no (or not yet) a criminal investigation or in cases Europol would receive data from private parties or publicly available sources without a link to criminal investigations.**

Belgium believes that the current text of Article 18(5a) and Article 18a would have to be amended to reflect that logic. As we would very much welcome a debate and/or confirmation on the above first, at this stage we have not yet suggested a text amendment in this regard.

The new concept of an "investigative case file"

- As already mentioned in our previous written contribution on block 2 and as mentioned during the LEWP meeting of 12 April, **Belgium is not at all convinced that we need the concept of an "investigative case file" and a definition of the concept**. As we understand it, the underlying rationale of Article 18a is that Europol should be allowed to process data outside Annex II if this is in support of a criminal investigation of a Member State or third "trusted" country (or EPPO). Defining and using the concept of an "investigative case file" only creates interpretation problems (for instance the Commission said it would not apply to intelligence gathering – for us that is exactly one of the most important reasons for asking Europol to support us in analysing data) and creates the need to further define a whole procedure (who decides on the creation?, when does it apply: only when it is very likely that it contains data outside of Annex II?, how does it relate to other procedures with regard to sending data for operational analyses?...).
- With regard to the definition in Article 2(q): do we really need the terminology of "datasets"? There is no definition of a "dataset" in the Regulation and this might pose a risk of difference of interpretation between the EDPS and Europol when applied in practice. Would a reference to "data" not be sufficient?
- As to the proposal to add "or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2)", Belgium is of the opinion that Europol should indeed be able to cross-check the data to the data that is already in its possession. However, we do not support the proposed addition as it can easily be read to mean that the data should be inserted into the Europol Information System, which is of course not feasible as that would mean that the EIS would contain data outside of Annex II (which largely passes the kind of data that can be inserted into the EIS). Belgium believes that the proposed wording to Article 18a(2) is sufficient.

- Some of the wording in Article 18a(1) is not clear to us as to what it means in reality.
  - Article 18a(1) states "Where necessary for the support of a specific criminal investigation (…)". Who will decide on the necessity part? Is this something to be clarified in the conditions to be specified by the MB and the EDPS? Does the Commission have a particular view on this? Is this "where necessary" the same as the Europol assessment mentioned in Article 18a(1)(b)? If not, could the Commission clarify?
  - Could the Commission explain how Europol would have to provide a credible assessment provided for in Article 18a(1)(b)? In practice, if the MS clearly indicates that it needs Europol's support, would Europol not be expected to confirm this?

- **Pending all of the above and pending some further clarifications, Belgium for now – as a first draft proposal – suggests to:**
  - **Delete Article 2(q):**

~~*"(q) 'investigative case file' means a dataset or multiple datasets that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation* **related to one or more Member States**~~*, in accordance with procedural requirements and safeguards under the applicable* ~~**Union law or** *national criminal law, and submitted to Europol in support of that criminal investigation."~~

  - **Amend Article 18a(1) as follows:**

"1. ~~**Where necessary for the support of a specific criminal investigation,**~~ *Europol may process personal data outside the categories of data subjects listed in Annex II where:*

(a) a Member State or the EPPO ***in accordance with procedural requirements and safeguards under applicable national or Union law*** *provides* ***for the purpose of operational analysis*** ~~**an investigative case file**~~ ***data*** *to Europol* ***for Europol's support of a[n ongoing] criminal investigation*** *[within the mandate of Europol]* ***[related to one or more Member States]*** ~~**pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2), or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2)**~~*; and*

(b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded."

Commented [VOF(1]: We suggest to delete this as for the moment it is not clear to us by whom and how this should be assessed. We also wonder if this makes sense taking into account the text of Article 18a(1)(b).

Commented [VOF(2]: We have adapted and incorporated the definition of the investigative case file. See our comments supra.

Commented [VOF(3]: We have a preference to delete « ongoing » as we want make to make sure that data collected in the proactive stage of an investigation (gathering of criminal intelligence) is also included.

Commented [VOF(4]: This could be deleted for Belgium. However, since we are not sure what is intended by the addition, we have not done so. Would the reference to Europol's mandate not be sufficient?

Commented [VOF(5]: "Pursuant to point (a) of Article 17(1)" is redundant as the text already states that is a MS that provides the data to Europol. Following the comment of Bulgaria during the LEWP this was indeed only relevant for MS in the text suggested by COM and the Presidency.

Commented [VOF(6]: "Pursuant to point (c) of Article 18 (2)" is also redundant as it stated earlier that the data is provided to Europol for the purpose of operational analysis.

Commented [VOF(7]: We have left the text as it is, but we would still like to know how this would work in reality (see our comment supra).

Article 18a(4)

Belgium is grateful for the deletion of the EDPS as already foreseen in the latest version of the working document. Belgium indeed does not agree with the Commission that this would not lead to a prior authorisation by the EDPS. We remain by our position that we do not want the EDPS to be given a role in an operational live processing of information. Therefore we would also suggest to delete the sentence "Where a third country provides an investigative case file to Europol, the EDPS shall be informed."

Block 3: Europol's role regarding research and innovation

Different interpretation of the impact of adding Article 18(2)(e)

As expressed in our earlier written comments and during the last meeting, we have a different interpretation than the Commission and the Council's Legal Service on the repercussions of including a new purpose in Article 18(2)(e). We do not believe that information provided by the Member States for specific other purposes can be used by Europol for research and innovation purposes. This does not coincide with the intentions of the legislator as regards purpose limitation, with how the text stands right now and with how purpose limitation has been functioning in practice.

Based on the detailed procedure of Article 19(1) and proven by established practice, Member States always have to indicate the purpose for which the information is provided to Europol. Only after the consent of the owner of the information, the information can be used for another purpose. This means that in practice information provided to Europol in the past will not be able to be used by Europol for research and innovation purposes, because the information provided in the past will not have the determined purpose of research and innovation. Europol will thus have to apply the procedure of Article 19(1) to request the use for another purpose and will have to await explicit consent of the owner of the information. Also when Member States provide information to Europol in the future, everything will depend on the purpose that is determined by the Member State. Member States may of course decide in their practice to always add the purpose of research and innovation when they provide information to Europol.

Seeing as Article 19(1) is very clear and explains how purpose determination functions, Belgium does not see any room for interpreting the text otherwise. Article 18(2)(e) thus only provides an extra option to be chosen by Member States when they provide Europol with information. Any phrasing in a recital constituting another way of interpreting Article 18(2)(e) – for example, reading the adding of Article 18(2)(e) as superseding the functioning Article 19(1) – would not coincide with the operative part of the Regulation.

Block 5: Europol's cooperation with third countries

Self-assessment by Europol as a structural way of cooperating with third countries

As explained during the meeting of 12 April, we welcome the possibility for a self-assessment by Europol as copied from the Eurojust Regulation in art. 25(4a)(b). We do have some remarks, which we list below together with the requested changes to the text.

- Firstly, we prefer to focus on the self-assessment by Europol, namely current art. 25(4a)(b). The Presidency's proposal also indicates another solution in art. 25(4a)(a) on "appropriate safeguards that are provided for in a legally binding instrument". We know this is a copy from the Eurojust Regulation, but as indicated during the last meeting we do not see at this point the added value in copying this first half of art. 58(1). On the other hand, we do

believe that – following Europol's experience in this regard – a self-assessment as proposed in art. 25(4a)(b) would create added value for certain third countries. **In art. 25(4a) we thus propose to delete art. 25(4a)(a)**. Consequently, in art. 25(1)(a) we also propose to delete the reference to this part of art. 25(4a), namely the words "have been provided for or".
As a result art. 25(4a)(b) remains and for clarity reasons we believe we should enter the whole remaining sentence of art. 25(4a)(b) in art. 25(1)(a) itself, so that art. 25(4a) can be deleted. In this way, art. 25(1) will clearly enumerate the four structural ways for Europol to cooperate with third countries:

- Art. 25(1)(a) explains adequacy decisions ánd the self-assessment alternative to it.
- Art. 25(1)(b) explains the international agreements.
- Art. 25(1)(c) explains the existing cooperation agreements.

The enumeration of structural possibilities in art. 25(1) is then followed by two derogations described in art. 25(5) and art. 25(6). **In art. 25(1)(a) we would thus also suggest to delete the reference to paragraphs 5 and 6** for clarity reasons. In this art. 25(1) the structural possibilities are listed; so the new self-assessment does have a place in there, but the derogations do not. We consider the current text to be clear and correct; paragraphs 5 and 6 read 'By way of derogation from paragraph 1', so a repetition in art. 25(1)(a) is not necessary. We do understand this formulation has been copied from the Eurojust Regulation, but we ask not to interfere unnecessarily with the current logic of the Europol Regulation in this matter.
These comments result in the following text proposal for art. 25(1)(a):
*"(a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision') **or in the absence of such a decision, Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data** ~~**appropriate safeguards have been provided for or exist in accordance with paragraph 4a of this Article, or in the absence of both an adequacy decision and of such appropriate safeguards, a derogation applies pursuant to paragraph 5 or 6 of this Article**~~**;**"*

- Certain changes are necessary to further incorporate the newly proposed self-assessment by Europol in the current functioning of Europol. **It would be useful for Europol to be able to conclude administrative arrangements with the third country after such self-assessment. And, we think that the Management Board should be informed about transfers on the basis following such self-assessment.** These are two activities that are also taking place following adequacy decisions. For adequacy decisions, these activities are listed in the last sentence of art. 25(1) and in art. 25(2). According to us the clearest option is thus to streamline the text in art. 25(1) and (2) to include transfers on the basis of Europol's self-assessment.
  Thus we believe the final sentence of art. 25(1) should read:
  "*Europol may conclude administrative arrangements to implement such agreements**, ~~or~~ adequacy decisions **or assessments***."
  Thus we think art. 25(2) should read:
  "*The Executive Director shall inform the Management Board about exchanges of personal data on the basis of adequacy decisions **or assessments** pursuant to point (a) of paragraph 1.*"

- We have to be realistic: the European Parliament is sensitive to Europol's possibilities to cooperate with third countries. We believe we thus should carefully align the EDPS' involvement here with what is written in the Eurojust Regulation. **We thus propose to add a sentence stating that Europol should inform the EDPS of such self-assessment (as in art. 58(2) of the Eurojust Regulation)**, for example as a new art. 25(7a) or in the existing art. 25(7):
  "The Executive Director shall inform the EDPS about categories of transfers following assessments pursuant to point (a) of paragraph 1."

- As explained this text proposal goes hand in hand with no longer needing and thus deleting art. 25(4a):
  ~~"4a. In the absence of an adequacy decision, Europol may transfer operational personal data to a third country or an international organisation where:~~
  ~~(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or~~
  ~~(b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data."~~

- As a further result of the amendments above also the first sentence of art. 25(8) would have to be amended to ensure a streamlined text:
  "Where a transfer is based ***on the assessment pursuant to point (a) of paragraph 1 or*** *on paragraph* ***~~4a or~~*** *5, such a transfer shall be documented and the documentation shall be made available to the EDPS on request."*

If the Presidency prefers to keep the current structure and thus to keep the self-assessment by Europol in a separate paragraph 4a, please find below an alternative to accommodate our comments above:

- To accommodate our comment not to refer to the derogations in the list of structural options, we propose to amend art. 25(1)(a):
  "(a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision') ***or in the absence of such a decision, appropriate safeguards ~~have been provided for or~~ exist in accordance with paragraph 4a of this Article, ~~or in the absence of both an adequacy decision and of such appropriate safeguards, a derogation applies pursuant to paragraph 5 or 6 of this Article;~~*** *"*

- To accommodate our proposal to delete the option of "appropriate safeguards provided for in legally binding instruments" and to include the possibility for Europol to create administrative arrangements and the reporting obligation to the Management Board, we propose to amend art. 25(4a):
  "4a. In the absence of an adequacy decision, Europol may transfer operational personal data to a third country or an international organisation where~~:~~
  ~~(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or~~

~~*(b)*~~ *Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data.*
Europol may conclude administrative arrangements to implement such assessments. The Executive Director shall inform the Management Board and the EDPS about exchanges of personal data on the basis of such assessments."

- Next to this a clerical amendment is proposed to first sentence of art. 25(8):
*"Where a transfer is based on paragraph**s** 4a or 5, such a transfer shall be documented and the documentation shall be made available to the EDPS on request."*

CZECH REPUBLIC

CZ comments – amendment to Europol Regulation blocks 1, 3, 5 and 7

Pursuant to request by the Presidency, CZ comments on WK 757/2020 REV 3 as follows:

Bloc 1

Article 1(m)

We have been able to consult this provision with our cyber security agency only after the meeting. It must be taken into account that there are other channels for coordination of responses to cyber incidents/attacks including large scale attacks, in particular CSIRTs' Network and CyCLONe Platform. Our cyber security agency points out that, pursuant to EU and national rules, there is no EU competence as regards the coordination of their reactions and does not see the role for Europol in this respect. The situation is not helped by broad definition of "competent authorities" in the Article 2(a) of the Europol Regulation. Therefore CZ needs to ask the Presidency to either:

a. *revert to "law enforcement authoritites":*

(m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States **and upon their request**, the coordination of **law enforcement** ~~**competent**~~ authorities'response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;

b. use the term "support" instead of "coordination":

(m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States **and upon their request**, the ~~**coordination**~~ **support** of ~~**law enforcement**~~ **competent** authorities'response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;

c. separate the "cyber-security part" from "combating computer crime part" by using Annex I:

(m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States **and upon their request**, the **coordination** of ~~**law enforcement**~~ **competent** authorities'response to ~~**cyberattacks**~~ **computer crime**, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;

Article 23(6)

CZ supports the inclusion of "private parties" to the first sentence. The purposes of prevention and combating crime may require processing by private parties, even though theirs is not such competence (see e.g. LED recital 11). To prevent confusion with legal grounds for processing, CZ proposes this wording:

6. Without prejudice to Article 30(5), personal data shall **not** ~~**only**~~ be transferred by Europol to Union bodies, **private parties,** third countries and international organisations **unless** ~~**if**~~ necessary for preventing and combating crime falling within the scope of Europol's objectives and in accordance with this Regulation, and if the recipient gives an undertaking that the data will be processed only for the purpose for which they were transferred. …

N.B. In further discussions of Article 24, the relationship between these two provisions will need to be taken into account.

Articles 26(6a) and 26a(5)

These provisions should both refer to Member State law by the same terms. CZ is flexible with regard to "national law", "legal frameworks" or something similar.

Article 26(11)

CZ accepts this location, but prefers previous wording in Art. 7(12), as it gave the Management Board more flexibility. CZ is flexible as to explicit inclusion of „data received from private parties".

Bloc 2

Article 2(q), recital 17

CZ believes that the definition of "investigative case file" should be broadened. We understand that an explicit link to national criminal proceedings is necessary for delimitation of these situations. However, the current wording "... a Member State ... acquired in the context of an on-going criminal investigation ..." is too restrictive. For example, if a cyber-security authority acquires a dataset during response to cyberattack, it is attributed to Member State, but there is no on-going criminal investigation yet to provide the context. Therefore, we propose to add the words "or used":

(q) 'investigative case file'means a dataset or multiple datasets that a Member State, the EPPO or a third country acquired **or used** in the context of an on-going criminal investigation **related to one or more Member States**, in accordance with procedural requirements and safeguards under ~~the~~ applicable **Union law or** national criminal law, and submitted to Europol in support of that criminal investigation.

The same change should be made to the fourth sentence of recital 17.

Bloc 3

Recital 11

As indicated at the two last meetings, CZ proposes to include text about the necessity of adequate funding for innovation and research at Europol:

(11) In order to help EU funding for security research to develop its full potential and address the needs of law enforcement, Europol should assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation that are relevant to Europol's objectives. When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, it should not receive funding from that programme in accordance with the conflict of interest principle. **Therefore, it is necessary to ensure adequate and reliable funding of research and innovation efforts at Europol in order to enable it to support law enforcement authorities of the Member States.**

Article 18(2) and Article 19(1)

For the reasons of legal certainty, CZ prefers explicit text to decide on the ability of Europol to process "historic" operational personal data transmitted with certain other purpose according to Art. 19(1). As there are several solutions possible (legal ground, prohibition, opt-in, opt-out etc.), CZ believes that general discussion should precede drafting.

Bloc 5

Article 25

CZ believes that the text of Art. 25 is well balanced and informing EDPS should be left for trilogues.

Block 7

Recital 14

CZ is flexible as regards insertion of the recital 11 of the Europol Regulation currently in force:

(11) Europol should be able to request Member States to initiate, conduct or coordinate criminal investigations in specific cases where cross-border cooperation would add value. Europol should inform Eurojust of such requests.

(end of file)

FINLAND

Finland's written comments on articles 4 (t), 18(2)(e), 18(5a) and bloc 8.

Article 4(1)(t)

(t) ~~proactively~~ monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States, **and** implement its research and innovation activities regarding matters covered by this Regulation, including **in** the development, training, testing and validation of algorithms for the development of tools, **and disseminate the results of these activities to the Member States in accordance with Article 67, and contribute to the coordination of activities of Union agencies established on the basis of Title V of the TFEU in the field of research and innovation within their mandates in close cooperation with Member States**;

As per reasoning provided during LEWP 12th April.

Article 18(2)(e)

In view of the concerns expressed by the EDPS in his opinion, we draw attention to the drafting proposal we sent to the Presidency already earlier:

"(e) research ~~**and innovation regarding matters covered by this Regulation**~~ for the development, training, testing and validation of algorithms for the development of tools **necessary for activities which fall within the scope of Chapter 5 of Title V of Part Three TFEU, covered by this Regulation**;

Reasons:

The EDPS has considered that the proposed new processing purpose is too broadly defined. We believe that our drafting proposal would respond to this concern and would also help to avoid possible conflicts with the requirements set out in TFEU and Regulation (EU) 2018/1275, including particularly requirements relating to the purposes of processing of personal data and the rights of the data subject. The concept of innovation is not used in that Regulation, whereas research is already a recognised purpose of further processing in data protection legislation. Innovation is also easily linked with commercial activities, but it is not in our understanding what is sought. Even if the concept of innovation was left in the text, it would be important to the research and innovation activities more clearly to the tasks of Europol as proposed by the EDPS, instead of objectives. Those tasks are essentially based on Chapter 5 of Title V of Part Three TFEU.

Article 18(5a)

While the proposed new processing purpose is based on prior views expressed by the EDPS, there are still further concerns expressed in the opinion of the EDPS concerning wording proposed by the Commission. We find that it would be useful to further define the situations in which this derogation from the main rule may be resorted to. We propose redrafting as follows:

5a. Prior to the processing of data under paragraph 2 of this Article, Europol may temporarily process personal data received pursuant to Article 17(1) and (2) for the purpose of determining whether such data comply with the requirements of paragraph 5 of this Article, **where it is impossible to establish the relevance of all data and functionally separate unnecessary data immediately**, including by checking the data against all data that Europol already processes in accordance with paragraph 5.

~~Europol may only process personal data pursuant to this paragraph for a maximum period of one year.~~ **Personal data processed pursuant to this paragraph must be deleted without delay where it has been established that it is not necessary for a specific criminal investigation.** ~~or~~ In justified cases, **personal data may be processed** for a longer period **only** with the prior authorisation of the EDPS, where necessary for ~~the purpose of this Article~~ **a specific criminal investigation and where it is impossible to functionally separate the unnecessary data**. Where the result of the processing indicates that personal data do not comply with the requirements of paragraph 5 of this Article, Europol shall delete that data and inform the provider of the data accordingly **where relevant.**

Reasons: In addition to the concerns expressed by the EDPS, we point out that one year is a rather long period of time in view of the principles of data minimisation and storage limitation set out in Article 4 of Regulation (EU) 2018/1725. It should be noted that the processing of big data may involve even large numbers of persons that have no link with the suspected criminal offence. However, we understand that the operational need of storing large and complex datasets is related to the fact that it takes time to establish the relevance and to functionally separate unnecessary data. As a main rule, the processing of data relating to persons with no link to a specific criminal offence, that is either planned or has taken place, is not permitted under the data protection legislation. There may also be risks relating to the proposed period of storage without separating the data in view of the prior views of the ECJ despite that those views have concerned different situations. In view of the impact on the fundamental rights of not only criminal suspects but also other persons, including the victims, it would be more appropriate to underline the main rule of deleting the unnecessary data without delay (Article 4(1)(e) of Regulation (EU) 2018/1725). A more efficient pre-analysis would also be better in line with the interests of crime prevention and criminal investigations. Furthermore, we agree with the EDPS in that the relationship with the proposed paragraph 5a and paragraph 6 is not clear. It would be useful to try and clarify it.

******

As regards to bloc 8, we have some questions, that we hope the Commission would have a chance to reflect during its presentation.

****

Article 26(6)

We propose the following modifications to Article 26(6):

Article 26

~~Exchanges of personal data~~ Cooperation with private parties

[…]

6a. Transmissions or transfers **referred to in paragraphs 5 and 6** shall not be systematic, massive or structural.

~~6a.~~ **6b.** Europol may request Member States, via their national units, to obtain personal data from private parties, which are established or have a legal representative in their territory, ~~under their applicable laws~~ **in accordance with their national ~~legal frameworks~~ laws**, for the purpose of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view to identifying the national units concerned.

Irrespective of their jurisdiction over the specific crime in relation to which Europol seeks to identify the national units concerned, Member States shall ensure that their competent national authorities can lawfully process such requests in accordance with their national laws for the purpose of supplying Europol with the information necessary for it to fulfil its objectives.

~~6b.~~ **6c.** Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws. In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data.

Reasons:

The EDPS considers in his opinion that the prohibition of systematic, massive or structural transfers should apply to any transfers of data to private parties. It is clear that when the law enforcement authorities request personal data or evidence from the private entities, it may sometimes be necessary to even request large volumes of data or the data may be in a structural form. However, even in that case the requests should be limited to what is necessary, and as a main rule, systematic, massive or structural requests should be avoided. In any case, the last sentence of paragraph 6, as worded, appears to concern data transfers to private entities and not data requests. Even at the EU level, it should be exceptional to transfer or transmit operational personal data to any private parties. On occasion, limited data may be transmitted to reason the request for personal data or evidence. It is hard to see how such data transmissions could be systematic, massive or structural.

The title of Article 26 could be aligned with its contents, e.g. by replacing "exchanges of personal data" with "requests of data from and transmissions of data to private parties". (Alternatively, "cooperation with private parties" that is used in proposed paragraph 2a could be used and would cover all situations.) It is not customary to speak of data exchange with private parties.

Article 33a

We submitted last week a drafting proposal for Article 18(2)(e). For reasons of consistency, we would also propose the following wording for Article 33a:

Article 33a

Processing of personal data for research **~~and innovation~~**

1. For the processing of personal data performed by means of Europol's research **~~and innovation~~** projects as referred to in point (e) of Article 18(2), the following additional safeguards shall apply:

Reasons:

The EDPS has considered that the proposed new processing purpose is too broadly defined. As an option - that we proposed for Article 18(2)(e) - the term "innovation" could be left out as the concept of "research" together with the contents of the Article would already cover the same. The concept of innovation is not used in Regulation (EU) 2018/1275, whereas research is already a recognised purpose of further processing in data protection legislation. If the concept of innovation was left in the text, it would be important to be more precise and link the research and innovation activities more clearly to the tasks of Europol as proposed by the EDPS, instead of objectives. Those tasks are essentially based on Chapter 5 of Title V of Part Three TFEU.

Observations relating to the provisions on data protection

We welcome the alignments with Regulation (EU) 2018/1275 proposed by the Commission. It is important to ensure a consistent data protection framework within the EU. However, it seems that the alignment is not in all places systematic. There are still some provisions where it may be unnecessary to duplicate the provisions of Regulation (EU) 2018/1275 in the Europol Regulation, such as Article 37a that has been proposed to be deleted by the EDPS. We have noticed duplication of provisions e.g. in Article 30, paragraph 2 (whereas paragraph 4 of that Article is proposed to be deleted, apparently for reasons of duplication). In any case, it is important to maintain all those additional safeguards set out in Article 30 that are not included in Regulation (EU) 2018/1275. Article 32 also raises the question of whether it is necessary to repeat the principle of data security even if it is only by means of referring to Article 91 of Regulation (EU) 2018/1275, given that the Member States are already bound by the identical provisions in the LED and its implementing legislation (whereas in Article 34, the requirement of notifying the EDPS has been deleted as it is already regulated by Regulation (EU) 2018/1275). We would welcome a clarification on whether Article 32 is meant to impose on Member States an obligation that is additional to the requirements imposed by the LED. The different approaches in different Articles might lead to confusion as to which provisions apply. It is important to ensure that the regime in Regulation (EU) 2018/1275, Chapter IX, applies in full.

Article 43

The EDPS has called for the harmonisation of the powers set out in Article 43 with the general powers of the EDPS in Article 58 of Regulation (EU) 2018/1275, and suggested that paragraphs 3 and 4 be deleted. We would welcome the Commission's clarification as to whether Article 58 would automatically become applicable through such a change? For the reasons of transparency and consistency of the data protection framework, it would be useful to harmonise the supervisory powers. To be able to form a view, however, we would also welcome clarity as regards the applicability of the provisions of Regulation (EU) 2018/1275 on administrative sanctions. Do they apply to EU agencies? In the light of Article 58 and recital 81, it is not apparent. According to recital 81 of that Regulation,

"*The fines should aim at sanctioning the Union institution or body — rather than individuals — for non-compliance with this Regulation, to deter future violations of this Regulation and to foster a culture of personal data protection within the Union institutions and bodies.*" The Regulation is silent on agencies as regards the applicability of administrative fines.

FRANCE

NOTE DE COMMENTAIRES DES AUTORITÉS FRANÇAISES

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leurs commentaires écrits suite à la réunion de groupe LEWP du 12 avril 2021, s'agissant des blocs suivants :

- *Bloc 1 - Permettre à Europol de coopérer de manière effective avec les parties privées*
- *Bloc 3 - Renforcer le rôle d'Europol en matière de recherche et d'innovation*
- *Bloc 5 - Renforcer la coopération d'Europol avec les États tiers*
- *Bloc 7 - Clarifier le fait qu'Europol puisse demander l'ouverture d'une enquête sur un crime affectant un intérêt commun couvert par une politique de l'Union*
- *Bloc 2 - permettre à Europol de traiter des ensembles de données complexes*

S'agissant du bloc 1 : Coopération avec les parties privées

Concernant le nouvel article 26 (11) relatif à la production d'un rapport sur les échanges entre Europol et les parties privées, les autorités françaises relèvent la modification profonde du texte qui avait fait pourtant l'objet d'un consensus en séance. Les autorités françaises s'interrogent sur les raisons de ces modifications et s'opposent à cette proposition d'article.

Commentaires détaillés :

Considérant nouveau	En lien avec leur proposition ci-dessous, les autorités françaises proposent la rédaction du considérant suivant : ***"In order to ensure Europol's effectiveness as a hub for information exchange, clear obligations should be laid down requiring Private parties to provide Europol with the data necessary for it to fulfil its objectives.*** ***Europol should increase the level of its support to Member States, so as to enhance mutual cooperation and the sharing of information.*** ***Given the nature of the new tasks of Europol regarding privates parties, the Management Board should be given the necessary information regarding the data exchanged between Europol and Private Parties. Europol should submit an annual report to the Management Board on the information provided by Private parties".***

Article 26 (11) *11. Europol shall draw up an annual report to the Management Board about the number of cases in which Europol issued follow-up requests to private parties or own initiative requests to Member States of establishment for the transmission of personal data in accordance with Article 26 and Article 26a, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks. The annual report shall be drawn up on the basis of the quantitative and qualitative evaluation criteria defined by the Management Board and shall be sent to the European Parliament, the Council, the Commission and national parliaments.*	Les autorités françaises accueillent favorablement cette proposition. Toutefois, pour la bonne information des Etats membres et la bonne conduite des échanges entre Europol et les parties privées elles proposent de compléter cette proposition d'article comme suit : *Europol shall draw up an annual report to the Management Board* ***including the number of personal data received and exchanged with private parties****, number of cases in which Europol issued follow-up requests to private parties or own initiative requests to Member States of establishment for the transmission of personal data in accordance with Article 26 and Article 26a, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks.* *The annual report shall be drawn up on the basis of the quantitative and qualitative evaluation criteria defined by the Management Board and shall be sent to the European Parliament, the Council, the Commission and national parliaments.* Toutefois, comme proposé par la Commission lors du dernier LEWP du 12 avril 2021, et sous réserve de l'approbation de la Présidence, la France pourrait également soutenir l'ancienne version du texte – article 7 (11).

Propositions d'articles :

Nous renouvelons nos propositions d'articles, que nous souhaiterions présenter plus en détail : ainsi, afin de garantir la totale transparence de l'activité d'Europol avec les parties privées et renforcer le rôle des États-membres, la délégation française propose un mécanisme pérenne permettant aux États-membres de prendre connaissance et de valider tous les protocoles d'entente (Memorandum of understanding - MoU) que l'agence signe avec les partenaires privées, la France soumet à la Présidence les propositions d'article suivante :

- **<u>Article 11 (v) Échanges de données à caractère personnel avec les parties privées (nouveau) :</u>**

Version FR *: « adopte des lignes directrices sur la réception et l'échange de données entre Europol et les parties privées ».*

Version EN : " *adopt guidelines on the receipt and exchange of data between Europol and private parties* ».

<u>Argumentaire</u> : Les autorités françaises précisent que ces lignes directrices n'interfèreraient pas avec les capacités de l'agence d'échanger des données personnelles avec les parties privées telles que prévues par les futures dispositions de ce Règlement. Il s'agirait pour les États membres d'impulser une dynamique dans un champ d'action nouveau pour l'agence en réfléchissant collectivement aux conditions et à l'application opérationnelle de ces échanges (quelles informations peuvent être envoyées par les parties privées (article 26 paragraphe 2a notamment), quelles infrastructures de communication (article 26 paragraphe 6b)…).

Cela serait plus cohérent avec les conclusions du conseil du 2 décembre 2019 qui mentionne que « *tout régime régissant la transmission directe de données à Europol par des parties privées devrait être fondé sur une procédure de consentement des États membres qui pourrait prendre la forme d'une liste proposée par Europol, constituée des parties privées de la part desquelles Europol aurait besoin de recevoir des données à caractère personnel. Cette liste ferait régulièrement l'objet de décisions prises par le conseil d'administration d'Europol, qui représente les autorités nationales* ».

- **<u>Article 26 ter échange de données à caractère personnel avec les parties privées (nouveau) :</u>**

Version FR : *« sans préjudice des articles 26 et 26a du présent règlement et après validation du Conseil d'administration, Europol peut conclure des protocoles d'entente avec les parties privées. Ces protocoles n'autorisent pas l'échange de données à caractère personnel et ne lient ni l'Union ni ses États membres*

Europol communique systématiquement aux États membres l'ensemble des protocoles d'ententes conclus avec les parties privées, pour information et validation par le Conseil d'administration ».

Version EN : " *Without prejudice to articles 26 and 26a and after the agreement of the Management Board, Europol may conclude memoranda of understanding with private parties. Such memoranda shall not authorise the exchange of personal data and shall not be binding on the Union or its Member States.*

Europol shall systematically communicate to the Member States all memoranda of understanding concluded with private parties for information and validation by the Management Board ".

<u>Argumentaire :</u> Les autorités françaises précisent que la communication aux Etats membres des protocoles d'entente ne vise pas à empêcher Europol d'échanger des données personnelles avec les parties privées mais simplement à les informer des protocoles que l'agence peut éventuellement conclure avec les parties privées, dont certains sont classifiés.

La France a déjà demandé la communication des protocoles qui restent à ce jour sans suite. Ainsi, la France souhaite seulement disposer de ces **protocoles pour information** et sans interférer avec les possibilités d'échange de données entre l'agence et les parties privées.

- **Article 11 (r) Fonctions du Conseil d'administration (amendement) :**

Version FR *: « r) Autorise la conclusion d'arrangements de travail, d'arrangements administratifs et* ***de protocoles d'entente avec les parties privées*** *conformément à l'article 23 paragraphe 4 e, à l'article 25, paragraphe 1 et l'article 26 ter ».*

Version EN: " r) *Decide upon working arrangements, administrative arrangements and memoranda of understanding with private parties in accordance with Article 23, paragraphs Article 25, paragraph 1 and article 26b".*

S'agissant du bloc 3 : Renforcer le rôle d'Europol dans la recherche et l'innovation

Commentaires détaillés :

Considérant 40 ***Providing Europol with additional tools and capabilities requires reinforcing the democratic oversight and accountability of Europol. Joint parliamentary scrutiny constitutes an important element of political monitoring of Europol's activities. To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group with annual information on the use of these tools and capabilities and the result thereof.***	Afin de suivre et d'enrichir les travaux de l'agence, cette information annuelle doit être communiquée aux États membres. La France propose de modifier le considérant comme suit : « *To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group and the Member States with annual information on its use of these tools and capabilities and the result thereof* ».

S'agissant du bloc 5 : renforcer la coopération entre Europol et les États tiers

Commentaires détaillés :

Considérant 24 ***Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation.***	Les autorités françaises estiment qu'il convient de modifier le considérant 24 en fonction de la modification de l'article 25 telle que présentée par la présidence portugaise. Les autorités françaises précisent que cette proposition de rédaction s'inspire largement des considérants du règlement Eurojust (voir considérant 51 du règlement Eurojust). Soit la proposition suivante : ***Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation.*** ***Transfers not based on an adequacy decision or international agreement concludes by the EU should be allowed by the Management Board only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where Europol, after authorization of the Management Board, has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist.*** ***Such legally binding instruments could, for***

	example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. Europol should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, Europol should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, Europol should be able to require additional safeguards.
Article 1(11)(a)- Article 25(5)- Transfer of personal data to third countries and international organisations *Subject to any possible restrictions pursuant to Article 19(2) or (3) and without prejudice to Article 67, Europol may transfer personal data to an authority of a third country or to an international organisation, insofar as such transfer is necessary for the performance of Europol's tasks, on the basis of one of the following (a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision')* ***or in the absence of such a decision, appropriate safeguards have been provided for or exist in accordance with paragraph 4a of this Article, or in the absence of both an adequacy decision and of such appropriate safeguards, a derogation applies pursuant to***	**La France remercie vivement la présidence portugaise pour la prise en compte des commentaires des délégations et d'Europol sur le régime d'autres agences JAI en matière de coopération avec les États tiers.** **Toutefois, la France, précise que cette modification du cadre d'échange avec les États tiers doit absolument s'accompagner d'un renforcement du contrôle du Conseil d'administration.** **Ainsi, il conviendrait que le CAE non seulement décide des arrangements de travail et des arrangements administratifs conclu par l'agence (article 11r) mais également qu'il puisse autoriser Europol à échanger des données personnelles au terme du paragraphe 4a de l'article 25 tel que proposé par la présidence.** **La France propose donc un amendement à l'article 25.4.a (voir plus haut sur le CAE).**

paragraph 5 or 6 of this Article**; (b) an international agreement concluded between the Union and that third country or international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals;* *(c) a cooperation agreement allowing for the exchange of personal data concluded, before 1 May 2017, between Europol and that third country or international organisation in accordance with Article 23 of Decision 2009/371/JHA. Europol may conclude administrative arrangements to implement such agreements or adequacy decisions. 2. The Executive Director shall inform the Management Board about exchanges of personal data on the basis of adequacy decisions pursuant to point (a) of paragraph 1.* *3. Europol shall publish on its website and keep up to date a list of adequacy decisions, agreements, administrative arrangements and other instruments relating to the transfer of personal data in accordance with paragraph 1.* *4. By 14 June 2021, the Commission shall assess the provisions contained in the cooperation agreements referred to in point (c) of paragraph 1, in particular those concerning data protection. The Commission shall inform the European Parliament and the Council about the outcome of that assessment, and may, if appropriate, submit to the Council a recommendation for a decision authorising the opening of negotiations for the conclusion of international agreements referred to in point (b) of paragraph (1).* ***4a. In the absence of an adequacy decision, Europol may transfer operational personal data to a third country or an international organisation where: ***(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or (b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that***	

appropriate safeguards exist with regard to the protection of operational personal data. *5. By way of derogation from paragraph 1, the Executive Director may authorise the transfer or a category of transfers of personal data to third countries or international organisations on a case-by-case basis if the transfer is: (a) necessary in order to protect the vital interests of the data subject or of another person;* *(b) necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides;* *(c) essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country;* *(d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions; or* *(e) necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal sanction. Personal data shall not be transferred if the Executive Director determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer referred to in points (d) and (e). Derogations may not be applicable to systematic, massive or structural transfers.* *6. By way of derogation from paragraph 1, the Management Board may, in agreement with the EDPS, authorise for a period not exceeding one year, which shall be renewable, a set of transfers in accordance with points (a) to (e) of paragraph 5, taking into account the existence of adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. Such authorisation shall be duly justified and documented.* *7. The Executive Director shall as soon as possible inform the Management Board and the EDPS of the cases in which paragraph 5 has been applied.*	

*8. Where a transfer is based on paragraph **4a or** 5, such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.*	

Propositions d'articles :

Les autorités françaises se félicitent du bon déroulement des discussions sur ce point et de l'amendement apporté par la Présidence à la proposition de la Commission.

Toutefois et afin d'assurer à l'agence une plus grande efficacité opérationnelle et stratégique, elles proposent les amendements suivants :

- **Article 7 (13) Fonctions du Conseil d'administration (nouveau) :**

Version FR :« *Europol rédige un rapport annuel portant sur la nature et le volume des données personnelles fournies à Europol et échangées avec les États tiers sur la base des critères d'évaluation quantitatifs et qualitatifs fixés par le CAE. Ce rapport annuel est transmis au parlements nationaux, au Parlement européen, au Conseil, et à la commission* ».

Version EN : " *Europol shall draw up an annual report to the Management Board on the personal data received and exchange with third countries on the basis of quantitative and qualitative evaluation criteria defined by the Management Board. The annual report shall be sent to the national parliaments, the European Parliament, the Commission, the Council and the Commission.*"

- **Amendement de la proposition de la présidence (article 25.4a)**

[…]

*4a. In the absence of an adequacy decision, Europol may, **after authorization of the Management Board**, transfer operational personal data to a third country or an international organisation where:*

(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or

(b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data.

S'agissant du bloc 7 : capacité d'initiative d'enquête de l'agence Europol

Aucun commentaire de la part des autorités françaises.

S'agissant du bloc thématique 2 (permettre à Europol de traiter des ensembles de données complexes)

Commentaires détaillés :

article 2 (q) Definitions ***(q) 'investigative case file' means a dataset or multiple datasets that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation related to one or more Member States, in accordance with procedural requirements and safeguards under the applicable Union law or national criminal law, and submitted to Europol in support of that criminal investigation.***	Lors du dernier LEWP, la Suède a rappelé qu'Europol intervient en soutien des États membres lorsque deux ou plusieurs États sont impliqués (article 3 règlement Europol). À ce titre, la Suède a fait remarquer que les dossiers d'enquête (*investigative case files*) devaient eux aussi concerner deux ou plusieurs États membres. La France estime pertinente la remarque de la délégation suédoise. En conséquence, elle propose d'amender la définition des dossiers d'enquête en ce sens : *'investigative case file' means a dataset or multiple datasets that **two or more** Member State**s**, the EPPO or a third country acquired in the context of an on-going criminal investigation, in accordance with procedural requirements and safeguards under the applicable Union law or national criminal law, and submitted to Europol in support of that criminal investigation.*

Article 1(6) – article 18a information processing in support of a criminal investigation *1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where: (a) a Member State or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2),* ***or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2)****; and (b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded.* *2. Europol may process personal data contained in an investigative case* ***file in accordance with Article 18(2)*** *for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by a Member State or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided. 3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for*	En conséquence de ce qui précède, les autorités françaises proposent les modifications suivantes de cet article : ***Article 1(6) – article 18a information processing in support of a criminal investigation*** *1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where: (a)* ***two or more*** *Member States or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2), or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2); and (b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded.* *2. Europol may process personal data contained in an investigative case* file in accordance with Article 18(2*) for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by Member States or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation.* *The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Without prejudice to the processing of personal data*

*as long as the judicial proceedings related to that criminal investigation are on-going in that Member State. That Member State**, or, with its agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation,** may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the **sole** purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a related criminal investigation are on-going in **that** other Member State. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Such personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.*	*under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided.*
	3. Upon request of all the Member States or the EPPO that provided the investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in one of these Member States.
4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, reaches the conclusion that there are	*These Member States**,** or, with their agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation, may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the **sole** purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a related criminal investigation are on-going in **that** other Member State. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Such personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.*
	4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of

preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union.	*Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union.* *5. The Management Board adopt guideline further specifying the procedure for the implementation of the article.*

GERMANY

Germany's follow-up comments to the LEWP meeting on 12 April 2021: Revision of the Europol Regulation – Thematic blocs 1, 3, 5, 7 and 2

Please find below Germany's written comments on the third revised version of the text of the Commission proposal (changes to the provisions pertaining to thematic blocs 1, 3, 5, 7 and 2). Further comments may be raised following ongoing scrutiny of the proposal.

On a general note, we would like to reiterate our previous comments in expressing that Europol should continuously be present in the meetings. In our view, delegations would benefit from being able to seek Europol's expertise and advice in the ongoing discussions. Against the background that Europol is also continuously invited at Ministerial Council level, we do not see any reasons why the participation of an agency should not be possible nor any legal obstacles. We are confident that the legal framework allows for a satisfactory solution in the best interests of the Member States while taking due account of the concerns expressed by the Council Legal Service.

Thematic bloc 1: cooperation with private parties

Article 4(1)(m):

As stated before, the exact role of Europol with respect to the new TCO Regulation remains to be determined.

Therefore, Germany suggests to refer explicitly to the coordination of removal orders for terrorist content online by Member States authorities in accordance with Art. 14 of Regulation 2021/… [the TCO-Regulation], as this provision defines the supporting role of Europol regarding the taking down of terrorist content online.

Thus, Art. 4(1)(m) would read as follows:

> *"support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States and upon their request, the coordination of competent authorities' response to cyberattacks,* ***the coordination of removal orders for terrorist content online by Member States authorities in accordance with Art. 14 of Regulation 2021/… [the TCO-Regulation]*** *and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions.*

This amendment should be mirrored in the last sentence of recital 35 as follows:

> *Nothing in this Regulation should be understood as precluding the Member States* ***and Europol*** *from using removal orders as laid down in Regulation 2021/... on addressing the dissemination of terrorist content online as an instrument to address terrorist content online* ***or making use of the coordinative and cooperative role of Europol in accordance with Art. 14 of the Regulation 2021/…, when member states issue such a removal order***."

Moreover, the meaning of "cyberattacks" needs to be explained as this term is only used in this Article of the Europol Regulation without giving a definition. Is there a suitable definition of this term in Union law that the provision could refer to?

Article 4(1)(u):

Germany does not object to the amendments to the previous version, but would still appreciate an explanation as to what the exact action by Europol to support Member States will be, inter alia vis-à-vis Article 4(1)(m). Especially, in our view it remains unclear which information could be provided to which private parties with the aim of identifying relevant online content (as the referral of terrorist internet content to the online service providers concerned is already covered by Article 4(1)(m)).

Article 26(5):

Germany would appreciate an explanation why the provisions concerning the consent (and presumed consent) of the data subject have been deleted. The remaining criterion ("undoubtedly in the interests of the data subject") appears too vague.

Article 26(6a) and Recital 31:

Germany welcomes the amendments to Article 26(6a) and to the corresponding Recital 31. Nevertheless, it should be specified more clearly that there is no legal obligation for the Member States and for the private parties concerned to comply with requests made by Europol. Therefore, the following sentence should be added to the provision (or at least the corresponding Recital):

> *"This Article does not oblige neither Member States nor private parties to comply with a request made by Europol."*

Article 26(6b):

Article 26(6b) does not yet limit the mentioned use of Europol's infrastructure in any way. Therefore, the wording should be aligned with the comparable provision of Article 8(4) in order to clarify that while applying to crimes falling outside the scope of the objectives of Europol the use of Europol's infrastructure must still relate to preventing and combating crime. Thus, the provision should read as follows:

> "*6b. Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws,* ***also to cover crimes falling outside the scope of the objectives of Europol.*** *In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data.* ***All such exchanges of information shall be in accordance with applicable Union and national law.****"*

Article 26(11):

Germany agrees with moving the provision to Art. 26(11), but suggests to clarify that in principle, the required examples – insofar as they relate to personal data– should be anonymized. The provision would then read as follows:

> *"Europol shall draw up an annual report to the Management Board about the number of cases in which Europol issued follow-up requests to private parties or own-initiative requests to Member States of establishment for the transmission of personal data in accordance with Article 26 and Article 26a, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks.* ***In principle, these examples shall be anonymized insofar as personal data is concerned.****"*

Article 51 (3) (f) should be amended accordingly

Article 26a:

As a general observation, it still remains unclear what the supporting task of Europol would be, including the relationship to the current tasks under Article 4(1)(m). The provision would also raise various issues about its exact scope. Should electronic evidence fall under it, this may have undesirable implications vis-à-vis the draft TCO Regulation and harbor contradictions to the E-Evidence dossier.

Recital 32:

The first sentence in Recital 32 as proposed by the Presidency needs to reflect the different ways of receiving data from private parties. Therefore, the text should be amended as follows:

> *"To ensure that Europol does not keep the data* ***~~received directly~~ obtained*** *from private parties* ***directly or via the Member States*** *longer than necessary …"*

Thematic bloc 2: enabling Europol to process large and complex datasets

Article 18(5):

What is the purpose of the introductory amendment (*"Without prejudice to Article 8(4) …"*)? Article 8(4) specifies only that Liaison Officers may use Europol infrastructure for exchanging information between their Member States and the liaison officers of other Member States, third countries and international organisations without involving Europol.

Why was Article 18(2)(e) excluded from the scope of Article 18(5)? Article 18 establishes the regulatory model that the categories of personal data that may be processed for the purposes laid down in Article 18(2) are specified in Annex II. If differences between the purposes arise, these disparities are also addressed in Annex II, as the Annex distinguishes between different purposes of Article 18(2). Why does the proposal not follow this regulatory model, when it comes to research and innovation activities?

Article 18(5a):

Why does paragraph 5a in its first sentence refer to Article 17(1) and (2)? Paragraph 6 does not contain such a restriction or specification to the sources of information mentioned in Article 17. What purpose does the reference serve?
We would also appreciate a clarification on the relationship of Article 18(5a) and Article 18a. In particular, with regard to Article 18(5a) it would be of interest to know whether the checking of data against other data processed by Europol is a feasible method to fulfil the purpose set out in the first part of the provision.

Furthermore, a clarification on the relationship between Article 18(5a) and Article 18(6) would be appreciated.

The second sentence concerns the establishment of further conditions related to the processing under the first sentence. A similar provision can be found in the second sentence of paragraph 6, whereby the latter refers not only to *"conditions relating to the processing of such data"*, but more specifically to *"conditions relating to the processing of such data, in particular with respect to access and use of the data, as well as time limits for the storage and deletion of the data"*. Is there a reason why there is no complete alignment between these provisions?

We welcome the maximum period of one year foreseen in the third sentence, as it is reasonable and corresponds with the time limits in our national legislation. We would appreciate an explanation, though, why paragraph 6 provides for a shorter maximum time period than paragraph 5a.

As the processing powers only serve the purpose of determining compliance with paragraph 5, why does the third sentence refer to *"where necessary for the purpose of this Article"*? This should rather read *"...of this paragraph"*.

The fourth sentence sets out that in the event of deletion of the data, Europol shall inform the provider of the data accordingly. This obligation does not make sense in cases where Europol has retrieved the information from publicly accessible sources including the Internet pursuant to Article 17(2). Therefore, the obligation to inform the provider should expressly exclude Article 17(2) instead of referring to the *"relevant"* cases (as proposed by the Presidency in the current version).

We have noticed that while the new Article 18a stipulates that the data shall be functionally separated (cf. paragraph 2 third sentence and paragraph 3 third sentence), Article 18(5a) does not contain such requirement. From a data protection perspective, the separation of categorised and non-categorised data would presumably make sense and would certainly be welcomed by the EDPS in particular.

Article 18a(1):

Germany welcomes that the legislative proposal addresses this very important issue. As we all know, it has become urgent to address Europol's ability to process big data in accordance with relevant data protection principles since the EDPS' decision on the big data challenge. As the Ministers have expressed in their Declaration on the Future of Europol, it is of key importance to Member States that Europol will be able to continue to support Member States in this regard.

We support the fundamental approach of the proposal and generally agree with the provisions brought forward. At the same time, the processing of large and complex datasets (beyond the limitations of Art. 18(5) and Annex II) raises questions concerning data protection and fundamental rights and must strictly be limited to what is necessary and proportionate to achieve the objectives covered by Europol's mandate.

It should be ensured that Art. 18a is applied on an exceptional basis and thus prevent the risk of the exception becoming the rule. Therefore, the provisions should lay down certain conditions that must be met to apply the derogation from Art. 18(5), such as scale, complexity, type or importance of the investigations.

Regarding point (b), it is not clear what the test behind *„that it is not possible"* entails. Does this mean technical impossibility? Would Europol have to arrange that the *„case file"* is processed in a way that categories of personal data that do not comply with the requirements of Article 18(5) are filtered out to the greatest extent possible? Will processing be permissible on a provisional basis then?

The new insertion in Article 18a(1)(a) proposed by the Presidency aims at opening the scope of this Article to the purposes referred to in Article 18(2)(a). This aim is in line with calls from our national law enforcement authorities for support in the area of preventing crime. However, the proposed amendment raises several questions that should be addressed:

- Apart from the new addition, the wording of the whole Article remains focused on "investigative case files" (which refer to datasets "that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation") and their "operational analysis" (which refers to Art. 18(2)(c)). Therefore, Germany proposes to revise the wording in order to better clarify which conditions would apply to the newly inserted option. *"Exceptional and duly justified cases"* alone is not an appropriate criterion.
- As EPPO is not competent for the prevention of crime, EPPO could at most request an additional analyses pursuant to Article 18(2)(a)(i). Nevertheless, Article 18a(1) concerns the general question of cooperation between Europol and EPPO. From our point of view, it does not make sense to deal with individual aspects of this topic outside the context of the underlying general issue. May we therefore suggest that all questions related to the EPPO be dealt with comprehensively in the context of thematic bloc 6.

Article 18a(2) and (3):

We welcome that the Presidency adopted several details of the wording suggested by Germany. Nevertheless, the provisions are partly redundant and could also be combined in an extended paragraph 2. The current paragraph 4 could then be renumbered as paragraph 3. The reference to paragraph 3 in paragraph 4 would have to be adapted accordingly.

Our proposal for wording for an extended provision based on paragraph 2:

> *"2. Europol may process personal data contained in an investigative case file for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by a Member State [or the EPPO] in accordance with paragraph 1, and only for the purpose of supporting that investigation. Upon request of the Member State [or the EPPO] that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond that storage period, for the sole purpose of ensuring the veracity, reliability and traceability of*

the criminal intelligence process and only for as long as the judicial proceedings related to that criminal investigation are on-going [under the responsibility of EPPO] or in that Member State or in a related criminal investigation in another Member State based on the outcome of the operational analysis of Europol and provided by the requesting Member State to the other Member State in accordance with national law.
The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data.
Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be processed where necessary and proportionate for the support of the on-going specific criminal investigation for which they were provided or for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process."

On the bracketing of EPPO, see the above commentary. Whether EPPO is to be included should be revisited when discussing thematic bloc 6.

Germany is not in favour of the proposed addition to Article 18a(2), according to which Europol may process personal data contained in an investigative case file *"in accordance with Article 18(2)"*. The purpose of processing data within the scope of Article 18a is exhaustively defined in its first paragraph. The second paragraph only deals with the subject of time periods,

Article 18a(4):

The part after *„with which ..."* could be aligned with the order used in Article 25(1).

The relationship of the third sentence (*"Europol shall verify .."*) and the fourth sentence (*"Where Europol ..."*) remains unclear. If the processing is already prohibited where preliminary indications of disproportionality or fundamental rights violations exist, the higher threshold in the former sentence may be unnecessary. If this was the case, both sentences could be combined into one sentence along the requirements in what is now the latter sentence.

The last sentence should read *"... be processed by Europol where necessary **and proportionate**..."* (cf. above drafting proposal).

Thematic bloc 3: research and innovation

Article 4(4a) and (4b):

Germany can accept the revised version of paragraph 4a in general. Regarding the last sentence of the revised version, the relation between this provision and Article 4(1)(t) seems unclear and should be clarified as follows"

*"Europol may engage with relevant projects of such Union framework programmes **in accordance with Article 4(1)(t)**".*

If this proposal is taken on board, the rest of the sentence can be deleted because Art. 4(1)(t) already states that results of these activities shall be disseminated to the Member States in accordance with Article 67.

Germany welcomes the deletion of paragraph 4b in line with our previous comments.

Article 18(2)(e):

Article 18(2) aims at realizing the principle of purpose limitation, according to which the purposes for the processing of personal data shall be specified. Could the provision indicate more specifically the purposes for which data may be processed in the context of research and innovation? For example, the text could stay closer to the Commission's proposal by amending the original wording as follows:

> *"research and innovation regarding matters covered by this Regulation**, in particular** for the development, training, testing and validation of algorithms **and** for the development of **other** tools **relevant to achieve the objectives set out in Article 3.**"*

Moreover, Germany is confident that the interests of the competent authorities as "data owner" are duly taken into account. Yet we would appreciate if the Commission could explain how the proposal interacts with the interests of the "data owners" in more detail so we can ensure this is in line with the requirements of our law enforcement authorities.

Article 33a(2):

Point (a) of Article 33(1) already foresees that for each individual project the necessity to process personal data is to be assessed carefully. In that context, the newly introduced Article 33(2) is rather of an advisory character. With that in mind, we think that this would be better placed in the corresponding Recital. Besides, we would like to ask to limit the phrase to "synthetic" and "anonymized" data. Personal data (such as "pseudonymized data") may be used where it is necessary and proportionate.

Thematic bloc 5: cooperation with third countries

Article 25(1) and (4a):

Germany welcomes the revision of Article 25 in line with our previous comments. However, as we mentioned before, the amendment to Article 25 must be reflected accordingly in all other provisions that refer to the possibilities for structural exchanges of personal data with third countries foreseen by Article 25. This applies in particular to Articles 18a(4), 26(1)(c), 26(4), 26(6), 26a(2), 26a(4), 27(1)(c) and 27(2).

By way of example, Article 18a(4) should be amended as follows:

> *"Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision, or in the absence of such a decision, where appropriate safeguards have been provided for or exist, as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational*

analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports."

Article 25(8):

Germany does not object to the current proposal of making available certain information to the EDPS. Nevertheless, Germany would appreciate an explanation why the former paragraph 8 was deleted. Will the subjects not covered by the new paragraph 8 be covered by point (1) (e) of the new Article 39a in the future?

Thematic bloc 7: ability to request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

Germany welcomes the deletion of the proposed Recital 14. In order to avoid any doubt that Article 6 only applies to cross-border cases, the wording of Recital 11 of the current Europol Regulation should be retained.

We therefore agree to provisionally close thematic block 7 on the condition that the wording of the old Recital 11 is carried over into the new Recital 14. Thus, Recital 14 should read as follows:

"(14) Europol should be able to request Member States to initiate, conduct or coordinate criminal investigations in specific cases where cross-border cooperation would add value. Europol should inform Eurojust of such requests."

IRELAND

Ireland's current position in regards to the discussions on the Europol Regulation Recast, blocks 1-7. Ongoing amendments to the text may alter our positions.

(1) **Enabling Europol to cooperate effectively with private parties, addressing lack of effective cooperation between private parties and law enforcement authorities to counter the use of cross-border services, such as communication, banking, or transport services, by criminals;**

Allowing Europol to directly exchange personal data with private parties is a very contentious proposal. An Garda Síochána have data protection concerns regarding the legality of mass transfers of data. In addition, the means by which the data is transferred could result in implications to national security systems, if the use of these IT systems are intended for transferring the data. Quantifying the volume of data to be transferred is inconceivable and will undoubtedly place implications on current resources, if dependent on Europol National Units. The possible consequences of time delays in processing the data and the capacity for ENU's to carry out this function in a timely manner is also a matter for concern.

The views of the Data Protection Officers reflected in the proposal document would be appreciated and should be considered.

(2) **Enabling Europol to effectively support Member States and their investigations with the analysis of large and complex datasets, addressing the big data challenge for law enforcement authorities.**

Consideration should be given to Member States' IT capacity and capabilities for dealing with large data sets. The requirement for carrying out Data Subject Categorisation on large data sets, prior to submitting them to Europol will have an impact on resources, if it is intended to dependent on Europol National Units to carry out this function. In addition, the practicalities of carrying out a review on data sets received from private parties requires clarification.

(3) **Strengthening Europol's role on research and innovation, addressing gaps relevant for law enforcement.**

An Garda Síochána foresee the benefits arising out of Europol's intended role on research and innovation, however, further consideration should be given to what data is used. Data previously submitted may not be appropriate as a dataset for research. In addition this data may be of limited value and relevance and it may have been superseded or obsolete. To overcome this issue, consideration should be given to mandatory consultation with MS in advance of the use of such data.

(4) Enabling Europol to enter data into the SIS

An Garda Síochána are in agreement with Article 4,1,r remaining, with specific adjustments being made to its wording.

Information received by Europol from trusted Third Party Countries, concerning non-EU citizens posing risk of terrorist offences, should be made available to Member States, and should be entered into SIS by Europol where the Member State(s) concerned has not been identified, in adherence with SIS protocols. Alternatively information received by trusted Third Party Countries concerning identified Member State(s) should be forwarded to concerned Member State(s) for appropriate action according to SIS guidelines.

Information inputted into SIS by Europol should be limited to terrorist offences involving non-EU citizens only, at this time.

An Garda Síochána currently have procedures in place for entering non-EU FTF data onto SIS under Article 36 of the Council Decision 2007/533/JHA. An Garda Síochána are of the view that if further information is required to substantiate the inputting of a SIS alert, and Europol are in a position to obtain and provide such information, this information should be returned to the Member State, to whom the responsibility lies, for review and subsequent inputting into SIS, if deemed appropriate.

(5) **Strengthening Europol's cooperation with third countries in specific situations and on a case-by-case basis for preventing and countering crimes falling within the scope of Europol's objectives;**

It is considered a necessary advancement to extend cooperation beyond Member States, ensuring trusted third party countries adhere to agreements entered into with Europol.

(6) **Clarifying that Europol may request, in specific cases where Europol considers that a criminal investigation should be initiated, the competent authorities of a Member State to initiate, conduct or coordinate an investigation**

An Garda Síochána support Europol initiating investigations concerning the EU Budget.

(7) **Strengthening Europol's cooperation with the European Public Prosecutor's Office (EPPO).**

Ireland are not involved with the European Public Prosecutor's Office and as such An Garda Síochána in not in a position to provide any submission on these discussions.

ITALY

In order to actively contribute to the new drafting of the Europol Recast Proposal, echoing the Italian written contribution to the 28 January LEWP meeting, please find below our amended proposals of Recital 3 and 6:

Recital 3:

"These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal and structured organised criminal groups, such as mafia type, that engage in a wide range of criminal activities. As action at national level alone does not suffice to address these transnational security challenges, Member States' law enforcement authorities have increasingly made use of the support and expertise that Europol offers to counter serious crime and terrorism. Since Regulation (EU) 2016/794 became applicable, the operational importance of Europol's tasks has changed substantially. The new threat environment also changes the support Member States need and expect from Europol to keep citizens safe".

Recital 6:

"High-risk criminals play a leading role in criminal networks, such as mafia-type and other structured criminal associations, and pose a high risk of serious crime to the Union's internal security. To combat high-risk organised crime groups and their leading members, Europol should be able to support Member States in focusing their investigative response on identifying these persons, their criminal activities and the members of their criminal networks".

We deem it is of the utmost importance to recall in the Europol Regulation the threat posed by structured mafia-type organizations.

The reference proposed would be in full compliance with the Commission's Communication on the EU Strategy to tackle Organised Crime 2021-2025 and with the Policy Advisory Document on EU crime priorities for the period 2022-2025 (discussed during the COSI meeting of the 16 of April).

As a matter of fact, identifying and disrupting High- risk Criminal networks such as "mafia-type" (and of course the crimanals that play leading roles within the mentioned organizations) is the aim of the PAD first recommended priority.

NETHERLANDS

Europol Regulation

Comments of the Netherlands following the LEWP of 12 April 2021

Blocks 1, 3, 5 and 2

General comment:

- We would appreciate it very much if the scrutiny reservations of the MS could be included in footnotes.

Block 1 Enabling Europol to cooperate effectively with private parties

General questions

- We would like to thank you for deleting the words "providing cross-border services" in recital 25.

- During the LEWP of 8 March, Belgium asked whether "private parties" should be added not only in article 23, para 7 but also in the first sentence of para 6. We think this might be a logical addition. We understand art 23 para 6 to mean that Europol needs to determine whether sharing information with another organisation is necessary for preventing and combating crime. This does not necessarily mean that the organisation receiving the information should have the prevention of or fight against crime as a task too. It seems logical that Europol should make this determination regardless of the type of organisation it intends to share the information with. We would therefore like to propose adding "private parties" to the first sentence of art 23 para 6 too:

> "Without prejudice to Article 30(5), personal data shall only be transferred by Europol to Union bodies, third countries ~~and~~ international organisations and private parties if necessary for preventing and combating crime falling within the scope of Europol's objectives and in accordance with this Regulation, and if the recipient gives an undertaking that the data will be processed only for the purpose for which they were transferred."

Article 7 para 12

- Thank you for moving the text about the annual report on the personal data exchanged with private parties from article 7 para 12 to article 26 para 11.

Article 26 para 2

- Since it is currently not clear what it would entail for the "seat Member State" to always be informed about data from private parties in their territory, or conversely what the consequences would be if the "seat Member State" would not be informed, we would like to suggest that rules are drawn up to determine when the "seat Member State" should be informed. These could be included in the guidelines on processing of information that will be established by the MB under article 18 para 7.

Article 26 para 6b

- How does the Commission intend to handle the recommendations of the EDPS regarding the use of Europol's infrastructure for exchanges between MS and private parties?

Article 26a

- Thank you for including a reference to the TCO Regulation in recital 35. This helps to clarify the difference between the referrals under art 26a of the Europol Regulation and the removal orders under the TCO Regulation.

- The TCO Regulation also includes stipulations to avoid duplication of efforts by Europol and MS. In order to avoid duplication of efforts by Europol and the Member States regarding article 26a and to prevent interference with investigations, we would like to propose a new recital 35a and a new article 26a para 4a. The text we propose for recital 35a is similar to recital 36 of the TCO Regulation:

> "In order to avoid duplication of effort and possible interferences with investigations and to minimise the burden to the hosting service providers affected, Europol should exchange information, coordinate and cooperate with the competent authorities before transmitting or transferring personal data to private parties to prevent the dissemination of online content related to terrorism or violent extremism. Where Europol is informed by a competent authority of a Member State of an existing transmission or transfer, it should not transmit or transfer personal data concerning the same subject matter."

The text we propose for article 26a paragraph 4a is similar to article 14 para 1 of the TCO Regulation:

> "Europol shall exchange information, coordinate and cooperate with the competent authorities with regard to the transmission or transfer of personal data to private parties under paragraphs 3 or 4 of this Article, in particular to avoid duplication of effort, enhance coordination and avoid interference with investigations in different Member States."

Block 3: Strengthening Europol's role on research and innovation

Article 18 para 2 sub e

- In the Netherlands, there is currently discussion whether under our national law data that has been collected in the course of criminal investigations can be used for the aim of research and innovation. This question has not been settled yet, but will hopefully be clarified in future. We would just like to inform you about this, since it could have implications for the use of Dutch data for research and innovation by Europol.

- Belgium may have a point when it comes to changing the use of data that has been provided before by MS so that it can also be used for research and innovation, if you look at the text of art 19 para 1.

Article 33a

- What does research and innovation encompass? Is there a definition of research and innovation? Article 18 para 2 subpara e talk about research and innovation "for the development, training, testing and validation of algorithms for the development of tools". Art 4 para 1 sub t says that research and innovation include "the development, training, testing and validation of algorithms for the development of tools" and therefore seems to suggest that they could involve other activities too. Article 33a mentions: "exploring and testing innovative new technological solutions and ensuring accuracy of the project results". We were wondering if these formulations are clear enough or if by not defining more precisely what we mean with research and innovation, we run the risk that the EDPS will formulate a definition of its own and then say that certain innovation projects are not allowed? How does the Commission intend to handle the EDPS recommendation that "the scope of the research and innovation activities should be better defined in the Europol Regulation, e.g. by clearly linking those activities to the tasks of Europol, and further clarified in a binding document, for instance adopted by the Management Board of Europol, which could be subsequently updated, if necessary"?

- When it comes to the role of the Management Board regarding projects for research and innovation, para 1 sub b now stipulates that it will be informed prior to the launch of such projects. When it comes to the bigger, more substantial of these projects, we would like it if the Management Board would not just be informed, but consulted. The guidelines drawn up under article 18 para 7 could be used to determine which projects the MB should be consulted on, and where informing the MB should be enough. We would like to propose the following text:

> "~~the Management Board and~~ the EDPS shall be informed prior to the launch of the project. The Management Board shall be either consulted or informed prior to the launch of the project, in accordance with criteria laid down in the guidelines, referred to in article 18, paragraph 7."

In order to further explain this, we would like to propose amending recital 39 as follows (in yellow):

> "Europol should inform the European Data Protection Supervisor prior to the launch of its research and innovation projects that involve the processing of personal data. Europol should either consult or inform the Management Board prior to the launch of the project, in accordance with criteria such as the risks to all rights and freedoms of data subjects, including of any bias in the outcome, the measures envisaged to address those risks and the scope of the project. For each project, Europol should carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data and all other fundamental rights, including of any bias in the outcome. This should include an assessment of the appropriateness, **necessity and proportionality** of the personal data to be processed for the specific purpose of the project, **including the requirement of data minimisation**. Such an assessment would facilitate the supervisory role of the European Data Protection Supervisor, including the exercise of its corrective powers under this Regulation which might also lead to a ban on processing. The development of new tools by Europol should be without prejudice to the legal basis, including grounds for processing the personal data concerned, that would subsequently be required for their deployment at Union or national level."

Block 5 Strengthening Europol's cooperation with third countries

Article 25 para 4a / 5

- When it comes to the new para 4a subpara b, we agree with the Bulgarian comment that it would be useful to clarify who will decide whether appropriate safeguards exist, the Executive Director or the MB.

- How does the Commission intend to handle the EDPS recommendation that "the meaning of "categories of transfers", as well as the distinction from "sets of transfers", should be further defined and clarified in the Europol Regulation."?

Block 2: enabling Europol to process large and complex datasets

Article 18(5a)

- We previously asked about the difference between checking the data against data already held by Europol and cross-checking the data. We assume that one difference is that when the data is checked against Europol's existing data under art 18 para 5a, any hits cannot be used, since the purpose under this article is only to check if the data comply with the requirements of paragraph 5 of this Article. Is that correct?

- We agree with the German suggestion that it would be wise to stipulate that the data shall be functionally separated.

- How does the Commission intend to handle the recommendation by the EDPS that this article should be "limited to cases where the transfer by Member States to Europol and the subsequent processing of big datasets by the Agency is actually an objective necessity", to clarify what are "justified cases" for extending the period in which Europol can process the data and to clarify the relationship between the derogations in paras 5a and 6?

Article 18a paras 1 and 2

- What does the Commission intend to do with the EDPS recommendation that in order to prevent the risk of the exception becoming the rule, the Regulation should lay down certain conditions and/or thresholds, such as scale, complexity, type or importance of the investigations?

- Do we understand correctly that para 1 refers to large datasets that also include non-annex II data and para 2 refers to the minimised version of that dataset that only includes annex II data, i.e. that under para 2 only annex II data can be processed?

Article 18a para 3

- The first and second section of para 3, especially the last parts, are very similar. The different uses of the word "related" may cause some confusion:

> - in the first section, the word "related" is used to indicate the connection between the judicial proceedings and the criminal investigation:
>
> "and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State."
>
> - in the second section, however, the word "related" refers to the connection between the original and the other investigation and the word "following" is used to indicate the connection between the judicial proceedings and the criminal investigation:
>
> "and only for as long as judicial proceedings following a related criminal investigation are on-going in that another Member State."

In order to prevent confusion, we would like to suggest clarifying the text of the first section by replacing "related to" by "concerning". This way, the word "related" will only refer to the connection between the original and the other investigation:

> "3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings ~~related to~~ concerning that criminal investigation are on-going in that Member State."

(We could consider replacing the word "following" in the second section by "concerning" too. "Following" could be read to mean that the judicial proceedings come after the criminal

investigation in time, whereas "concerning" would more clearly indicate that the judicial proceedings are based on the criminal investigation:

> "That Member State, or, with its agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation, may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings following (or concerning?) a related criminal investigation are on-going in that other Member State.")

Article 18a para 4

- What should Europol share with the EDPS here, the complete investigative file, or just a short message that the file has been received?

- When the Commission negotiates a treaty with a third country or issues an adequacy decision so that Europol is allowed to exchange personal data with that country, does it also look at the situation regarding fundamental rights in that country?

- How is Europol meant to check if fundamental rights have been violated? This could be quite difficult. What if the file also contains data that the third country providing it has received from other countries?

- Can Europol share the outcome of the operational analysis with a third country when relevant? How does this work if an analysis is based on data from several Member States?

- How can we make sure that third countries do not share intelligence, but only information that has been acquired in the context of a criminal investigation as part of these case files?

POLAND

PL comments on block 2 of Europol regulation:

Art. 18a (4)

In the light of the discussion and explanation received from the Commission on the 12 April LEWP VTC, as regards processing by Europol personal data from a third country and verification if the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports and if there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights, PL suggest deleting the second element, namely verification of respect for fundamental rights. If we assume that third country, which is a party of an international agreement pursuant to Article 218 TFEU or a cooperation agreement in accordance with Article 23 of Decision 2009/371/JHA, or is subject of adequacy decision, is a trusted partner, which do not obtain personal data with violation of fundamental rights, there is no need to include a provision which stipulates the necessity to verify it by Europol.

Furthermore, PL still needs some more clarification as regards the term "manifestly disproportionate" and how Europol will conduct verification in practice and are there appropriate tools at its disposal? The involvement of EDPS in the process might be a challenge.

We would like to repeat once again our question what will happen if Europol reaches the conclusion that amount of personal data is disproportionate, however the data set contains crucial data for further criminal investigation in MS? PL suggests exploring a possibility of including the provision regarding requesting a third country to narrow the scope of data.

ROMANIA

Follow up LEWP 12 April 2021

- **Blocks 1, 3, 5 and 7**

Ro reiterates previous positions (written comments) on blocks 1, 3, 5 and 7.

Additionally,

In view of the above written comments, RO supports the deletion of recital no. 14, as well as the amendments brought to art. 6 para 1, respectively:

Art.6 (1) In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the ~~Member State or~~ Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation.

RO agrees the following wording of Art 4 (1) (m), respectively:

*Art 4 (m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States **and upon their request**, the coordination of ~~law enforcement~~ **competent** authorities' response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;*

Starting from RO's written comments on Art. 25 (4) and the amendment of Art. 2 lit. p) - "operational personal data" in the definition of administrative data - RO proposes the insertion of the definition of "operational personal data" in the content of Art. 2. This is needed for legal clarity and for making a clear distinction between "administrative personal data" and "operational personal data".

Regarding Art. 7 (12), RO supports the changes from point 12 by moving the provisions of this point within Art. 26 (11).

Art 7 (12). (provision moved to Article 26(11)) Europol shall draw up an annual report to the Management Board on the personal data exchanged with private parties pursuant Articles 26 and 26a on the basis of quantitative and qualitative evaluation criteria defined by the Management Board number of cases in which Europol issued notifications to private parties on missing information in accordance with point (d) of paragraph 5 of Article 26 or requests Member States to obtain personal data from private parties in accordance with paragraph 6a of Article 26, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks. The annual report shall be sent to the European Parliament, the Council, the Commission and national parliaments;

- **Block 2 – enabling Europol to process large and complex dataset**

Previous RO written comments, additional information / clarifications are needed on newly introduced phrase “where relevant" (art 18 (5a)), as this could create confusion in practice.

1) Art 18 (5a) (...) Europol may only process personal data pursuant to this paragraph for a maximum period of one year, or in justified cases for a longer period with the prior authorisation of the EDPS, where necessary for the purpose of this Article. Where the result of the processing indicates that personal data do not comply with the requirements of paragraph 5 of this Article, Europol shall delete that data and inform the provider of the data accordingly ***where relevant.***

SPAIN

Follow-up comments to the last LEWP meeting (12/04/2021)

EXAMINATION OF THE PROPOSAL REGARDING THEMATIC BLOCS 1 AND 3, 5 AND 7:

THEMATIC BLOCK 5: STRENGTHENING EUROPOL'S COOPERATION WITH THIRD COUNTRIES

Art.25.5: It is necessary to clarify the scope of the term "category of transfers". It is proposed to eliminate it from this article, indicating only the transmission of personal data "case by case", as the regulation itself states. It should be noted that this clarification is motivated by the fact that the inclusion of the term CATEGORY means adding the possibility of a massive authorization of transfers that can be included in the same group, so it is not considered incorrect.

FURTHER EXAMINATION OF THEMATIC BLOC 2: ENABLING EUROPOL TO PROCESS LARGE AND COMPLEX DATASETS

Art.2 q: It seems reasonable that EPPO, member states and third states can enter data that are considered to be of interest. Clarification on the implementation of this last point would be welcome.

18.5: The text: "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II." should be modified as follows: "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II."

18.5 a: No comments

18 a: It is understood that publicly available data may be processed, even if they are not Annex II data. It is proposed to clarify this point.

6.2. WRITTEN COMMENTS ON THEMATIC BLOCK 6

BELGIUM

Written comments of Belgium in relation to block 6

Belgium generally supports continuing to work on Article 20a. We do have some specific suggestions for certain paragraphs:

- Following the formulation in Article 102 of the EPPO Regulation, which clearly outlines that EPPO *requests* information or *asks* for Europol's support, we believe also in the Europol Regulation this way of functioning should be upheld. To this end, the words indicating the requirement of a request by the EPPO should be added to paragraph 2 of Article 20a. To streamline the paragraph further with what is written in Article 102 of the EPPO Regulation, we propose the following text for Article 20a(2):

*"Europol shall **actively** support the investigations and prosecutions of the EPPO and cooperate with it**, in particular** through **providing, at the request of the EPPO, relevant** **exchanges of** information and **by providing** analytical support."*

Although this is indeed not foreseen in the EPPO Regulation, we are open to support the inclusion of a hit/no-hit system for EPPO. Our preference would be to delete Article 20a(3) and to add EPPO to the relevant paragraphs of Article 21 (which would be paragraphs 1, 3, 4, 5, 6 and 7).

CZECH REPUBLIC

CZ comments – amendment to Europol Regulation bloc 6

Pursuant to the request by the Presidency, CZ proposes following changes to WK 757/2020 REV 3:

Bloc 6 (EPPO)

Article 20a(1)

The second sentence is not included in Article 102 or elsewhere in EPPO Regulation. We believe that it should focus on Europol only and refer to rules given in this regulation. This would also serve to provide stronger legal link to data ownership principle. Finally, the order of sentences should be changed:

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). To that end, they shall conclude a working arrangement setting out the modalities of their cooperation. In the framework of that relationship, Europol ~~**and the EPPO**~~ shall act within ~~**their respective**~~ **the** mandate**, restrictions** and competences **stipulated by this Regulation**.

Article 20a(2)

While it is true that recitals of EPPO Regulation refer to "active support" of EPPO by all Union bodies, the purpose of this provision is to provide for specific cooperation between the two bodies in particular and should closely reflect that of Article 102(2) of EPPO regulation. The part of sentence concerning analytical support should not be repeated as it is already included in Art. 18a(1)(a):

2. Where necessary for the purpose of its investigations, Europol shall provide, at the request of the EPPO, any relevant information held by Europol, concerning any offence within the competence of EPPO.

CZ is flexible as to the inclusion of "prosecutions" within this paragraph.

Recital 22

CZ believes that ownership principle should be clearly addressed. As the Commission explained, this should be covered by recital 22. However, the only relevant part is the second last sentence, which is very general. It most likely refers to Article 24, which in turn refers to Article 19. Given the general importance of this question, we propose following clarification of the second last sentence:

The rules on the **restrictions of processing and** transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO.

(end of file)

FINLAND

Finland's written comments on article 20a(3).

Article 20a(3)

In relation to Article 20a on EPPO, we pay attention especially to its Paragraph 3. It would seem that there are certain differences regarding EPPO´s access to information provided for the purposes of points (a), (b) and (c) of Article 18(2), when compared with access of Eurojust and OLAF. We would like to know if this is what is meant and, if so, for what reason. For instance: would the limitation of Subparagraph 2 of Paragraph 1 of Article 21 (".. the information that generated the hit may be shared, in accordance with the decision of the provider of the information to Europol, and only to the extent that the data generating the hit are necessary for the performance of Eurojust's or OLAF's tasks") apply to EPPO as well? The legislative technique used in Article 20a, including the reference to Article 21, thus raises some questions that we would need to clarify before we can give our final stand on the Article 20a.

******

FRANCE

NOTE DE COMMENTAIRES DES AUTORITÉS FRANÇAISES

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leurs commentaires écrits suite à la réunion de groupe LEWP du 12 avril 2021 s'agissant du bloc thématique 6 : « renforcer la coopération d'Europol avec l'EPPO ».

Commentaires généraux :

Les autorités françaises rappellent les dispositions de l'article 102 du règlement Parquet européen qui disposent que le Parquet européen *« peut également demander à Europol de fournir une aide à l'analyse dans le cadre d'une enquête particulière conduite par le Parquet européen ».* Cet article 102 du règlement ne mentionne pas la possibilité pour Europol de soutenir le Parquet européen dans ses activités de poursuite.

À ce titre, **les autorités françaises estiment que la rédaction de l'article 20a §2 proposée en l'état par la Commission charge Europol de missions qui dépassent le cadre général de sa relation avec le Parquet tel que fixé par son règlement**.

Les autorités françaises relèvent en outre que l'arrangement de travail conclu entre l'agence et le Parquet prévoit une assistance d'Europol dans les enquêtes criminelles. Elle relève d'ailleurs qu'à sa demande dans le cadre de son mandat de négociation de l'arrangement de travail entre Europol et le Parquet européen elle a fait retirer le terme « *prosecution* » du texte.

Par souci de cohérence, il conviendrait dès lors de retirer ce terme « de poursuite » du paragraphe 2 de l'article 20a tel que proposé par la Commission.

Commentaires détaillés :

Considérant 22 ***Europol and the European Public Prosecutor's Office ('EPPO') established by Council Regulation (EU) 2017/19397, should put necessary arrangements in place to optimise their operational cooperation, taking due account of their respective tasks and mandates. Europol should work closely with the EPPO and actively support the investigations and prosecutions of the EPPO upon its request, including by providing analytical support and exchanging relevant information, as well as cooperate with it,*** ***from the moment a suspected offence is reported to the EPPO until the moment it determines whether to prosecute or otherwise***	En lien avec ses commentaires ci-dessous, la France propose de supprimer le terme « *prosecution* » de ce considérant.

dispose of the case. Europol should, without undue delay, report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence. To enhance operational cooperation between Europol and the EPPO, Europol should enable the EPPO to have access, on the basis of a hit/no hit system, to data available at Europol, in accordance with the safeguards and data protection guarantees provided for in this Regulation. The rules on the transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO. Europol should also be able to support criminal investigations by the EPPO by way of analysis of large and complex datasets.	
Article 1(8) ***Article 20a*** ***Relations with the European Public Prosecutor's Office*** *1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation.* ***2. Europol shall actively support the investigations and prosecutions of the EPPO and cooperate with it, in particular through exchanges of information and by providing analytical support.*** ***3. Europol shall take all appropriate measures to enable the EPPO to have indirect access to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system. Article 21 shall apply mutatis mutandis with the exception of its paragraph 2.*** ***4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence.***	Les autorités françaises estiment que l'article proposé par la Commission charge Europol de missions qui dépassent le cadre général de sa relation avec le Parquet tel que fixé par son règlement. En effet, l'article 102 (qui disposent que le Parquet européen « *peut également demander à Europol de fournir une aide à l'analyse dans le cadre d'une enquête particulière conduite par le Parquet européen* ») du règlement ne mentionne pas la possibilité pour Europol de soutenir le Parquet européen dans ses activités de poursuite. La France relève également que l'arrangement de travail conclu entre l'agence et le parquet européen prévoit une assistance d'Europol dans les enquêtes criminelles. Dans la continuité des discussions précédentes et des positions françaises sur le sujet, la France souhaite le strict respect de l'article 102, sans aller au-delà. En conclusion, la France souhaiterait retirer le terme « *prosecution* » dans cet article, comme dans le considérant 22.

GERMANY

Germany's follow-up comments to the LEWP meeting on 12 April 2021:
Revision of the Europol Regulation – Thematic bloc 6

Please find below Germany's written comments on thematic bloc 6 (strengthening Europol's cooperation with the EPPO) following the last LEWP meeting on 12 April 2021. Further comments may be raised following ongoing scrutiny of the proposal.

Germany welcomes that the legislative proposal aims at ensuring a close and productive cooperation between Europol and the EPPO. However, in line with our and the majority of the other Member States' previous comments, the cooperation should be limited to the extent that is already foreseen by the EPPO Regulation, notably Article 102 thereof. We see no need to extend the cooperation beyond this.

Consequently, any amendment of the Europol Regulation should in principle focus on reflecting the cooperation between Europol and the EPPO as specified in Article 102 of the EPPO Regulation. To that end, we consider it important to align the wording of the proposed new Article 20a with the wording of Article 102 of the EPPO Regulation.

In addition to this general position, we would like to comment on some individual aspects of the proposal:

- Regarding the proposed wording in Article 20a para. 2 (*"... actively support..."* and *"... cooperate with it, in particular..."*), we would first like to highlight that Article 102 of the EPPO Regulation does not provide for an active role of Europol. It rather stipulates that the EPPO – at its request – should be able to obtain relevant information held by Europol. Secondly, the EPPO Regulation does not provide for further possibilities of cooperation between Europol and the EPPO beyond providing information and analytical support to a specific investigation conducted by the EPPO.

- In order to avoid national investigations being jeopardised or sensitive information being disclosed, it is important that Europol can only share information with the EPPO if the Member State, Union body, third country or international organisation that provided the information has given its prior consent. We would like to highlight that Europol's cooperation with Eurojust, OLAF and EBCG follows this principle (as stipulated in Article 21 para. 1 and 1a).

- Regarding Article 20a para. 3, we have doubts that the proposed hit/no-hit mechanism is in line with the EPPO Regulation. Unlike the provisions governing the cooperation with Eurojust and OLAF respectively (Article 100 para. 3 and Article 101 para. 5 respectively), Article 102 does not provide for such hit/no-hit mechanism in relation to Europol.

- As Article 20a para. 4 mirrors Article 24 para. 1 of the EPPO Regulation, the wording should be aligned accordingly including the references to Article 22, Article 25 para. 2 and para. 3 of the EPPO Regulation.

- Furthermore, we think that all the aspects of the proposal concerning the EPPO should be addressed in Art. 20a altogether. We will return to this topic when discussing other provisions of the proposal that also deal with EPPO.

Taking into account the above comments, we propose that Article 20a be worded as follows:

"Article 20a

Relations with the European Public Prosecutor's Office

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation.

2. At the request of the EPPO and subject to the conditions set out in Art. 102(2) of Regulation (EU) 2017/1939, Europol shall support the investigations and prosecutions of the EPPO by providing information and analytical support to a specific investigation by the EPPO.

3. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939.

4. If the information referred to in paragraphs 2 and 3 is subject to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2) of this Regulation, Europol shall consult with the provider of the information stipulating the restriction and seek its authorisation for sharing.

In such a case, the information shall not be shared without an explicit authorisation by the provider."

HUNGARY

Initial comments on Article 20a of the revised Europol Regulation.

In accordance with the text of Article 20a Europol would be able to actively support the investigations and prosecutions of the EPPO, which wording is misleading in our opinion and can be easily interpreted as an extension of the competences of Europol to indirectly initiate investigations based on its own analysis. We took note of the explanation of the Commission during the last LEWP meeting according to which the exact same wording can be found in recital (69) of the EPPO regulation, but in the same time let us stress that this provision is only a recital in the aforementioned regulation and not part of the operational part of the text. In the spirit of compromise we would be open to a solution similar to the one in the EPPO regulation, namely to have only a recital with the text of the current paragraph (2).

ITALY

Italian written contribution: LEWP 12.4.2021 follow up

Thematic block 6 on EPPO/Europol cooperation

As said during the LEWP meeting of 12.4.2021 Italy would like to stress preliminarily that in our view no provision should go beyond what art. 102 of the EPPO regulation states.

Italy believes that is of utmost importance to avoid any interference or overlap with the relations and cooperation of EPPO with the national LEAs and to prevent any risk of jeopardising ongoing investigations.

Furthermore, as expressed by other delegations during the 12.4.2021 LEWP meeting, we believe that Europol's cooperation with EPPO should be expressly limited to investigations involving two or more countries (cross border nature) and in no case involving the prosecutions as lay down by art. 20a and by recital 22 of the Proposal.

We wish to recall that the art. 4 of the "working arrangement" stipulated in January 2021 limits the areas of cooperation between Europol and EPPO as follow:

" ... the exchange of specialist knowledge, general situation reports, information on criminal investigation procedures, information on crime prevention methods, the participation in training activities as well as providing advice and support, including through analysis, in individual criminal investigations".

Furthermore, we deem it necessary to remove the term "actively" from the text of art. 20a par2 in order to avoid the possibility that the information exchange not previously and formally requested by EPPO to Europol could lead to:

- dangerous duplications and overlaps with the information flow directed to EPPO:
- the possibility to indirectly stimulate the initiation of investigations (by the European Public Prosecutor) beyond the limits established by art. 6 of the Europol Reg. (on this point the vast majority of LEWP delegates have already expressed their opposition to an amendment of art. 6 of the current Europol Regulation);
- the danger of jeopardizing ongoing investigations of EPPO or/and other national judicial authorities.

To sum up Italy believes that:

- the EPPO-Europol cooperation as defined in the Proposal should only concern investigations and not prosecutions .
- Any exchange of information between Europol and EPPO should be authorized by the Member States concerned in order not to interfere with ongoing investigations.
- The word "actively" should be removed from art. 20a to par2.

LITHUANIA

In accordance with the last LEWP meeting on 12 April 2021, please be informed that Lithuanin delegation does not have any comments/proposals for the thenatic block 6 **(the EPPO/Europol cooperation) of Europol regulation.**

NETHERLANDS

The remarks of the delegation of the Netherlands on block 6

The Netherlands would like to enter a scrutiny reservation on block 6.

- The Netherlands is still studying the comments made by other MS on the inclusion of the words "actively" and "prosecution" in para 2 of article 20a, on the hit / no hit access for the EPPO described in para 3 and on the content of the report in para 4. It reserves the right to make further comments on this later on.

- If it is decided to keep the hit / no hit access for the EPPO as described in para 3, we think that even though the EPPO is a different kind of organisation than Eurojust, OLAF and Frontex, it would be clearer for the users of the Europol Regulation if the EPPO would be included in article 21 on hit/no hit access.

- To clarify that the EPPO will only get access to data that fall within its mandate, we would like to propose that in paragraph 3 about hit / no hit access (whether this stays in article 20a or is moved to article 21) the words "within its mandate" are added. In addition, we would also like to add the final sentence of paragraph 1 and of the first section of paragraph 1a of article 21 about the ownership principle. This would align the wording of art 20a para 3 with that of paragraphs 1 and 1a of article 21 about hit / no hit access for Eurojust, OLAF and Frontex.

  > "3. Europol shall take all appropriate measures to enable the EPPO, within its mandate, to have indirect access to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system, without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2). Article 21 shall apply mutatis mutandis with the exception of its paragraph 2.

- In order to avoid the risk of the same criminal conduct being reported to the EPPO by both Europol and a Member State, we also think it would be useful if article 20a para 4 would contain a reference to article 19 para 2, to make clear that prior consent from the MS that provided the information is necessary. Maybe the following text from article 21 para 1 can be added here too:

  > "4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence, without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2)."

ROMANIA

Follow up LEWP 12 April 2021

- **Block 6: strengthening Europol' s cooperation with the EPPO**

No comments or observations on Art. 20a.

SPAIN

Follow-up comments to the last LEWP meeting (12/04/2021)

INITIAL EXAMINATION OF THEMATIC BLOC 6: STRENGTHENING EUROPOL'S COOPERATION WITH THE EPPO

Art.20.a: Spain considers it necessary to have a clear understanding of the meaning of the principle of "mutatis mutandi", in terms of its impact on Article 21.

7. COMMENTS RECEIVED AFTER THE MEETING ON 26 APRIL 2021

7.1. FOLLOW UP /ADDITIONAL WRITTEN COMMENTS ON BLOCK 6

AUSTRIA

Comments Austria Bloc 6 Cooperation with the EPPO

We thank the Presidency for the revised version of Article 20a in document WK 757/2021 REV 4. We can support the revised wording.

We are flexible concerning the inclusion or exclusion of the word „prosecutions“ in para 2 of Art. 20a.

We can support the hit/no hit system in para 3 of Art. 20a; although we believe that the system will produce many hits concerning the same case. This due to the fact that Europol will receive informations from competent authorities of Member States where they also provide information to the EPPO.

We wonder how Europol will handle the administrative burden or minimize it.

BELGIUM

Written comments of Belgium in relation to block 6

Belgium is thankful to the Presidency for taking on board its comment on including a reference to the 'request' by EPPO in Article 20a(2).

Belgium confirms its previous position with regard to Article 20a(3) and the ***unclarity of 'mutatis mutandis'***. As explained before, we are open to support the inclusion of a hit/no-hit system for EPPO. However, our preference would be to delete Article 20a(3) and to add EPPO to the relevant paragraphs of Article 21. As an alternative we propose to include the relevant text of Article 21 in Article 20a.

We believe currently there is a lot of confusion:

- We want to avoid overlap and unclarity, which we see for example emerging due to the text of Article 21(8) being 'mutatis mutandis' applied to EPPO, while there is already Article 20a(4). We also note Article 21(5) which also introduces quite similar obligations. It is unclear to us how these three obligations relate to each other.
- Furthermore, there seems unclarity as to the application of the owner principle throughout Article 20a. The Commission explained that Europol in cooperating with EPPO would take the owner principle into account and that a reference to this end was included in the recitals. In recital 22 however we only see a reference to this when it concerns specifically the hit/no-hit system.
- During the meeting of 26 April we already noted similar concerns about Article 21(8) – part of thematic block 8. Namely Bulgaria asked for the inclusion of a reference to Article 19 in the text of Article 21(8).

Thus Belgium would appreciate a ***clarification by the Commission*** on how it does sees the obligations of Europol versus EPPO (Article 20a(4)) and of Europol versus OLAF (Article 21(8)) in relation to the owner principle and Article 19(2). Also, we would appreciate clarifications on how these two new paragraphs would relate to the obligation of Article 21(5).

BULGARIA

Bulgarian contribution to thematic block 6 of the draft Regulation amending Regulation (EU) 2016/794 as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

We would like to thank the Portuguese Presidency for continuing the detailed discussions on the draft Regulation and the Commission for the explanations on Block 6.

We generally support the proposed texts on strengthening the cooperation between Europol and the EPPO.

Furthermore, we have some questions and comments:

- We would like to suggest Art. 20a which regulates the relations between Europol and EPPO to be moved from Chapter IV "Processing of information" to Chapter V "Relations with partners" after Section 1. Similar approach is used in the EPPO Regulation (EU) 2017/1939, where Art. 102 is part of Chapter X "Provisions on the relations of the EPPO with its partners".

- We would like also to suggest to incorporate para 3 of Art. 20a in para 1 of Art.21 namely:

Article 21

Access by Eurojust, OLAF, EPPO and, only for purposes of ETIAS, by the European Border and Coast Guard Agency to information stored by Europol

1. Europol shall take all appropriate measures to enable Eurojust, ~~and~~ OLAF **and EPPO**, within their respective mandates, to have indirect access on the basis of a hit/no hit system to information provided for the purposes of points (a), (b) and (c) of Article 18(2), without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2).

- We propose to mirror the wording of Art.102 para 1 of the EPPO Regulation (EU) 2017/1939 in Art. 20a para 1, because the second sentence of the proposed wording sounds like there are doubts if both these main EU bodies in JHA area will not act within their respective mandate and competences:

Article 20a

Relations with the European Public Prosecutor's Office

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). ~~In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences~~. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation.

- We propose following wording of para 2 of Art. 20a like the para 2 of Art.102 of EPPO Regulation with additional guarantees with respect to the data ownership principle.

2. **Upon request by the EPPO in accordance with Article 102 of Regulation (EU) 2017/1939,** Europol shall support the investigations [and prosecutions] of the EPPO and cooperate with it, in particular by providing any relevant information held, concerning any offence within its competence ~~through exchanges of information~~ and by providing analytical support. The transmission of information should be done without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2).

- With regards to expressed concerns from some Members States concerning the support of Europol to EPPO **prosecutions** we have a question to the European Commission linked to Art. 20 para (5)[1] namely the participation of Europol staff in judicial proceedings in the Member States.
  When EPPO requests analytical and expert support from Europol in criminal investigation will it be possible on a later stage in the framework of judicial proceedings (EPPO prosecution) following this criminal investigation, EPPO to request Europol staff to provide evidence which came to their knowledge while providing this analytical/expert support, bearing in mind the possibility of EPPO to provide an "investigative case file" for data processing and operational analysis (Art.18a (1) (a))?If yes, there should be revision of Art. 20 para (5) as well as we should keep "prosecutions" in Art. 20a.

[1] Art.20 (5). When national law allows for Europol staff to provide evidence which came to their knowledge in the performance of their duties or the exercise of their activities, only Europol staff authorised by the Executive Director to do so shall be able to give such evidence in judicial proceedings in the Member States.

CROATIA

Concerning Thematic blocks 6 and 8, we can voice our preliminary support but would like to maintain scrutiny reservation on the last presented changes.

CZECH REPUBLIC

CZ comments – amendment to Europol Regulation bloc 6

Pursuant to the request by the Presidency, CZ proposes following changes to WK 757/2020 REV 4:

Bloc 6 (EPPO)

Article 20a(3)

CZ believes that the indirect access of the EPPO should have its purpose clearly spelled out, in the same way Art. 21(1) refers to the mandate of Eurojust and OLAF. Paragraph 8 should be also excluded from the mutatis mutandis application of Article 21.

3. Europol shall take all appropriate measures to enable the EPPO**, within its mandate,** to have indirect access to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system, **without prejudice to any restrictions indicated in accordance with Article 19(2) by the Member State, Union body, third country or international organisation which provided the information in question.** Article 21 shall apply mutatis mutandis with the exception of its **paragraphs 2 and 8**.

Article 20a(4)

CZ believes that coordination of all involved authorities and EU bodies would be improved if Europol informed relevant Member State(s) at the same time:

4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence **in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939; it shall inform all national units concerned at the same time.**

Article 21(8)

CZ believes that coordination of all involved authorities and EU bodies would be improved if Europol informed relevant Member State(s) at the same time:

8. If during information-processing activities in respect of an individual investigation or specific project Europol identifies information relevant to possible illegal activity affecting the financial interest of the Union, Europol shall on its own initiative without undue delay provide OLAF with that information**; it shall inform all national units concerned at the same time**.

Recital 22

CZ notes the reiteration that restrictions referred to in Art. 21(1) actually apply. To specify the purpose of our previous comment, it is to apply restrictions pursuant to Art. 19(2) to cooperation under Art. 20a(2) rather than Art. 20a(3). With regard to Art. 20a(2), the only relevant part of the recital 22) is the second last sentence, which is very general, and refers to Article 24, which in turn refers to Article 19. Given the general importance of this question, we propose either

- *clarification of the second last sentence:*

The rules on the **restrictions of processing and** transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO.

- *or, alternatively, clarification of the second sentence:*

Europol should work closely with the EPPO and actively support the investigations and prosecutions of the EPPO upon its request, including by providing analytical support and exchanging relevant **disponible** information, as well as cooperate with it, from the moment a suspected offence is reported to the EPPO until the moment it determines whether to prosecute or otherwise dispose of the case.

Additionally, the recital should correspond to the final wording of Article 20a.

(end of file)

FRANCE

NOTE DE COMMENTAIRES DES AUTORITÉS FRANÇAISES

COMMENTS FROM THE FRENCH AUTHORITIES

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leurs commentaires écrits suite à la réunion de groupe LEWP du 26 avril 2021.

The French authorities kindly ask the Presidency to find below their written comments following the LEWP group meeting of 26 April 2021.

- **S'agissant de la révision du règlement d'Europol : bloc 6 : renforcer la coopération d'Europol avec l'EPPO :**
  - **- Concerning the revision of the Europol regulation: block 6: strengthen Europol's cooperation with EPPO :**

Les autorités françaises se félicitent et remercient la Présidence pour la prise en compte de ses commentaires relatifs à la proposition d'article 20 (a) concernant la relation entre Europol et le Parquet européen. Par ailleurs, s'agissant du terme "*prosecution*", les autorités françaises approuvent sa suppression et soulignent que pour des questions de cohérence, ce terme doit être également supprimé du considérant 22.

The French authorities welcome and thank the Presidency for taking into account its comments on the proposed Article 20(a) concerning the relationship between Europol and the European Public Prosecutor's Office. Furthermore, the French authorities approve the deletion of the term "prosecution" and stress that, for reasons of consistency, **this term should also be deleted from recital 22.**

Bloc 6. Coopération entre Europol et le parquet européen

Considérant 22 ***Europol and the European Public Prosecutor's Office ('EPPO') established by Council Regulation (EU) 2017/19397, should put necessary arrangements in place to optimise their operational cooperation, taking due account of their respective tasks and mandates. Europol should work closely with the EPPO and actively support the investigations and prosecutions of the EPPO upon its request, including by providing analytical support and exchanging relevant information, as well as cooperate with it, from the moment a suspected offence is reported to the EPPO until the moment it determines whether to prosecute or otherwise dispose of the case. Europol should, without undue delay, report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence. To enhance operational cooperation between Europol and the EPPO, Europol should enable the EPPO to have access, on the basis of a hit/no hit system, to data available at Europol, in accordance with the safeguards and data protection guarantees provided for in this Regulation. The rules on the transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO. Europol should also be able to support criminal investigations by the EPPO by way of analysis of large and complex datasets.***	En lien avec ses commentaires ci-dessus, la France propose de supprimer le terme « *prosecution* » de ce considérant. Par ailleurs, les autorités françaises s'interrogent sur la mise en œuvre du paragraphe 4* et sollicitent tout éclairage que la Commission pourra apporter sur ce point afin notamment de préciser qu'elles pourraient être les conséquences pour Europol d'une absence de signalement d'une « conduite criminelle » pour laquelle le Parquet européen s'estimerait compétent. *"*Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939*"

GERMANY

Germany's follow-up comments to the LEWP meeting on 26 April 2021: Revision of the Europol Regulation – Thematic bloc 6

Please find below Germany's written comments on thematic bloc 6 (strengthening Europol's cooperation with the EPPO) following the last LEWP meeting on 26 April 2021. Further comments may be raised following ongoing scrutiny of the proposal.

Germany welcomes the amendments proposed by the Presidency as they address some of the concerns we raised in our written comments dated 14 April 2021. Nonetheless, we would like to emphasize that the cooperation between Europol and the EPPO should be limited to the extent that is already foreseen by the EPPO Regulation, notably Article 102 thereof. We see no need to extend the cooperation beyond this. Thus, we would like to reiterate our previous comments:

- Regarding the proposed wording in Article 20a para. 2 (*"... actively support..."* and *"... cooperate with it, in particular..."*), we would first like to highlight that Article 102 of the EPPO Regulation does not provide for an active role of Europol. It rather stipulates that the EPPO – at its request – should be able to obtain relevant information held by Europol. Secondly, the EPPO Regulation does not provide for further possibilities of cooperation between Europol and the EPPO beyond providing information and analytical support to a specific investigation conducted by the EPPO.
- In order to avoid national investigations being jeopardised or sensitive information being disclosed, it is important that Europol can only share information with the EPPO if the Member State, Union body, third country or international organisation that provided the information has given its prior consent. We would like to highlight that Europol's cooperation with Eurojust, OLAF and EBCG follows this principle (as stipulated in Article 21 para. 1 and 1a).
- Regarding Article 20a para. 3, we still have doubts that the proposed hit/no-hit mechanism is in line with the EPPO Regulation. Unlike the provisions governing the cooperation with Eurojust and OLAF respectively (Article 100 para. 3 and Article 101 para. 5 respectively), Article 102 does not provide for such hit/no-hit mechanism in relation to Europol. With regard to Commission's statement in the last LEWP meeting according to which details of the hit/no-hit mechanism could be dealt with in a working arrangement, we would like to recall that working arrangements do not have legally binding effects on the Union or its Member States (Article 99(3) of the EPPO Regulation). As the EPPO-Regulation does not provide for a hit/no-hit mechanism between EPPO and Europol, there is no way to introduce such mechanism by means of a working arrangement.

In order to address our comments, we would like to suggest that Article 20a be re-worded altogether as follows (changes compared to the current text proposal of Article 20a in document WK 757/2021 REV 4):

"Article 20a

Relations with the European Public Prosecutor's Office

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation.

2. Upon request by the EPPO in accordance with Article 102 of Regulation (EU) 2017/1939, Europol shall support the investigations of the EPPO ***~~and cooperate with it, in particular through exchanges of information and~~*** *by providing* ***information and*** *analytical support.*

~~3. Europol shall take all appropriate measures to enable the EPPO to have indirect access to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system, without prejudice to any restrictions indicated in accordance with Article 19(2) by the Member State, Union body, third country or international organisation which provided the information in question. Article 21 shall apply mutatis mutandis with the exception of its paragraph 2.~~

3.~~4.~~ *Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939.*

4. If the information referred to in paragraphs 2 and 3 is subject to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2) of this Regulation, Europol shall consult with the provider of the information stipulating the restriction and seek its authorisation for sharing.

In such a case, the information shall not be shared without an explicit authorisation by the provider.*"*

HUNGARY

Article 20a

We would like to thank the Presidency for taking into account our comments regarding this article and we think that the compromise text goes into the right direction. However we would still like to stress that the text of this article cannot go beyond what is set out in Article 102 of the EPPO regulation. In this regard we would like to ask for the following modifications as it was highlighted during the last LEWP meeting:

*Upon request by the EPPO in accordance with Article 102 of Regulation (EU) 2017/1939, Europol shall support the investigations of the EPPO and cooperate with it, ~~in particular~~ ~~through exchanges of~~ **by providing** information and ~~by providing~~ analytical support.*

ITALY

Following the Italian intervention during the 26 April LEWP meeting, Italy believes that the recital 22 of the Proposal should be amended to be more in line with art. 20a.

We therefore propose a revised version of the recital :

(22) Europol and the European Public Prosecutor's Office ('EPPO') established by Council Regulation (EU) 2017/19397, should put necessary arrangements in place to optimise their operational cooperation, taking due account of their respective tasks and mandates. Europol should work closely with the EPPO and ~~actively~~ support the investigations ~~and prosecutions~~ of the EPPO upon its request, including by providing analytical support and exchanging relevant information, as well as cooperate with it, from the moment a suspected offence is reported to the EPPO until the moment it determines whether to prosecute or otherwise dispose of the case. Europol should, without undue delay, report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence, in accordance with the relevant articles of the EPPO Regulation . To enhance operational cooperation between Europol and the EPPO, Europol should enable the EPPO to have access, on the basis of a hit/no hit system, to data available at Europol, in accordance with the safeguards and data protection guarantees provided for in this Regulation, including any restrictions indicated by the entity which provided the information to Europol. The rules on the transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO. Europol should also be able to support criminal investigations by the EPPO by way of analysis of large and complex datasets.

NETHERLANDS

Comments the Netherlands on the Europol Regulation block 6

LEWP 26 April 2021

Block 6 Strengthening Europol's cooperation with the EPPO

Article 20a

- Thank you for deleting the word "actively" in para 2 and for taking on board our suggestion to include the words: "without prejudice to any restrictions indicated in accordance with Article 19(2) by the Member State, Union body, third country or international organisation which provided the information in question." in para 3 on the hit / no hit system.

- We also suggested to clarify in para 3 that the EPPO will only get access to data through the hit / no hit access that fall within its mandate. Therefore we would like to propose that in paragraph 3 the words "within its mandate" are added after "Europol shall take all appropriate measures to enable the EPPO". This would align it with the provisions on hit / no hit access for Eurojust, OLAF and Frontex in article 21 paras 1 and 1a, which also contain the words "within their respective mandates / within its mandate":

> "3. Europol shall take all appropriate measures to enable the EPPO, within its mandate, to have indirect access to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system, without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2). Article 21 shall apply mutatis mutandis with the exception of its paragraph 2.

- Finally, in order to avoid the risk of the same criminal conduct being reported to the EPPO by both Europol and a Member State, we also think it would be useful if article 20a para 4 would contain a reference to article 19 para 2, to make clear that prior consent from the MS that provided the information is necessary. Maybe the following text from article 21 para 1 can be added here too:

> "4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence, without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2)."

POLAND

PL comment on block 6 of the Europol regulation:

Bearing in mind the current wording of new art. 20a as well as new art. 24, and included references to art. 19 (2) in these provisions, Poland suggests adding the word "transmission" in the first sentence of art. 19 (2), as follows:

"Member States, Union bodies, third countries and international organization may indicate, at the moment of providing information to Europol, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its transfer, transmission, erasure or destruction. Where the need for such restrictions becomes apparent after the information has been provided, they shall inform Europol accordingly. Europol shall comply with such restrictions."

The abovementioned amendment is in line with the wording of recital 22 and will allow countries not participating in enhanced cooperation with the EPPO to fully secure the data transferred to Europol in the course of ongoing cases.

ROMANIA

9. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

9.2 Further examination of thematic block 6: strengthening Europol's cooperation with the EPPO

As we have previously stated, we have no proposals or comments on the content of Article 20a on strengthening Europol's cooperation with the EPPO.

SLOVENIA

As regards the revision of the Europol Regulation, please be informed that at the moment Slovenia don't have additional comments on: on thematic bloc 6: strengthening Europol's cooperation with the EPPO and on thematic bloc 8: strengthening the data protection framework applicable to Europol.

SPAIN

Follow-up comments to the last LEWP meeting (26/04/2021)

AS REGARDS THE REVISION OF THE EUROPOL REGULATION, SPAIN PROVIDES THE FOLLOWING MODIFICATIONS

ON THEMATIC BLOC 6: STRENGTHENING EUROPOL'S COOPERATION WITH THE EPPO

Article 20ª: With respect to point 3, it is considered necessary to clarify the application of Article 21. It would be helpful to have a practical example of the application of this paragraph.

7.2. FOLLOW UP /ADDITIONAL WRITTEN COMMENTS ON BLOCKS 1 AND 2

AUSTRIA

In regard of Bloc 1 Private Parties Recital 34 and Article 26,6b concerning the use of Europols infrastructure by Member States:

In recital 34 is stipulated that Member States may grant Europol access to such exchanges, when they use this infrastructure for exchange on crimes falling within the scope of Europol's objectives.

This should be mirrored in Article 26, 6b

Will you add this sentence or shall we send a written proposal for Art. 26,6b?

For recital 34 we propose a minor change in the wording.

The last part oft he third sentence should read „they may grant Europol access to such exchanges".

The words „or not" at the end of the sentence seem to be redundant.

FRANCE

S'agissant du bloc thématique 2 (permettre à Europol de traiter des ensembles de données complexes)

Commentaires détaillés :

article 2 (q) Definitions ***(q) 'investigative case file' means a dataset or multiple datasets that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation related to one or more Member States, in accordance with procedural requirements and safeguards under the applicable Union law or national criminal law, and submitted to Europol in support of that criminal investigation.***	Les autorités françaises remercient la présidence pour la prise en compte de leurs commentaires sur cet article.
Article 1(6) – article 18a information processing in support of a criminal investigation *1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where: (a) a Member State or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2),* ***or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2);*** *and (b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case*	En conséquence de ce qui précède les autorités françaises proposent les modifications de cet article ci-après : ***Article 1(6) – article 18a information processing in support of a criminal investigation*** 1. *Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where: (a)* ***two or more*** *Member States or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal*

file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded. *2. Europol may process personal data contained in an investigative case file in accordance with Article 18(2) for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by a Member State or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided. 3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State. That Member State, or, with its agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation, may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a related criminal investigation are on-going in that other Member State. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Such personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.* *4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement*	*investigation within the mandate of Europol pursuant to point (c) of Article 18(2), or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2); and (b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded.* *2. Europol may process personal data contained in an investigative case* file in accordance with Article 18(2*) for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by Member States or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation.* *The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided.* *3. Upon request of all the Member States or the EPPO that provided the investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in one of these Member States.* *These Member States, or, with their agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation, may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a related*

concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union.	*criminal investigation are on-going in that other Member State. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Such personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.* *4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union.* *5. The Management Board adopt guideline further specifying the procedure for the implementation of the article.*

7.3. WRITTEN COMMENTS ON BLOCK 8

AUSTRIA

Comments Austria Block 8 Data Protection Framework

After an initial analysis we have some comments on the Commission's proposal.

Article 2 definitions

Article 2 (l) recipient: As Article 27a, para 1 refers to Article 3 of Regulation EU 2018/1725, where „recipient“ is defined we would ask if item (l) should be deleted.

Article 30 para 2

We would prefer to keep the wording “prohibited, unless it is” in order to maintain the existing standards

Article 37

Para 3, 4 an 5 refer to para 2 which is deleted

Article 50

It is not clear for us why para 1 is deleted. Could Commission explain if Article 65 of EU 2018/1725 (“…damage as a result of an infringement of this regulation…”) covers the scope of para 1 of Article 50 (“…damage as a result of an unlawful data processing operation…”)

BELGIUM

Written comments of Belgium in relation to block 8

At this moment Belgium only wants to stress a more general comment on this block, which is related to the prior consultation mechanism of article 39 and accompanying recital 46.

One of the important goals of this Europol Regulation recast is that it should enable Europol to continue and further develop its operational capacities in order to support the Member States' investigations. Although it is of course necessary for Europol to apply strict data protection rules it should not result in a situation where the EDPS is in fact hampering severely the operational support by Europol. Within the Management Board of Europol of March an important discussion

was held on the matter following a letter of the EDPS to the Chair of the Management Board. Belgium thinks it is extremely important to take into account the manner in which the EDPS is conducting its supervision task. The decision by the EDPS on the use of machine learning tools is the latest development in that regard and is proof how the EDPS is interpreting the prior consultation duty of Europol very widely and is hampering Europol's supporting role in the recent important Encrochat and SKY EEC cases.

Recital 50 of the current Europol Regulation clearly states that the prior consultation mechanism should not apply to specific operational activities such as operational analysis projects. Belgium thinks it is crucial to make sure that the prior consultation mechanism is only to be interpreted by the EDPS in the spirit of current recital 50. Therefore Belgium is in favor of incorporating the relevant parts of recital 50 again in the current text proposal.

In this regard, Belgium supports the German text proposal to include in recital 46 the following two sentences: "With regard to the supervision by the EDPS, *the prior consultation mechanism is an important safeguard for new types of processing operations. This should not apply to specific individual operational activities, such as operational analysis projects, but to the use of new IT systems for the processing of personal data and any substantial changes thereto.*" [The phrase is in italic is taken literally from current recital 50 of the Europol Regulation.]

In addition to the proposed amendment of recital 46, Belgium will further look into a possible change in article 39.

BULGARIA

Bulgarian contribution to thematic block 8 of the draft Regulation amending Regulation (EU) 2016/794 as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

We would like to thank the Portuguese Presidency for continuing the detailed discussions on the draft Regulation and the Commission for the explanations on Block 8.

We generally support the proposed texts on strengthening the data protection framework of Europol and we believe they are in the right direction. We expect that by adopting these provisions the rules on processing personal data by Europol will be put in compliance with the rules already applied regarding the Union institutions, bodies, offices and agencies. The enhanced legal framework will contribute to the effective implementation of the new extended competences of the agency to support investigations conducted by the Member States.

Furthermore, we have some questions and comments:

On Art. 21, para 8 on the obligation for Europol to provide without any delay information related to possible illegal activity affecting the financial interest of the Union, we propose at the beginning of the sentence to replace "if" with "when".

We have concerns whether Europol should provide OLAF with this information taking into account the possible restrictions imposed by MS under Art.19 para 2. In addition, we are on the opinion that

Europol should notify or should report to OLAF similar to EPPO in Art. 20a (4), instead to provide OLAF with information. In this case the Member States concerned should be also notified.

8. ~~If~~ **When** during information -processing activities in respect of an individual investigation or specific project Europol identifies information relevant to possible illegal activity affecting the financial interest of the Union, Europol shall on its own initiative without undue delay ~~provide~~ **report to** OLAF ~~with that information~~ **and notify the Member States concerned.**

On Art. 24 we would like to know which institution/body/agency should be considered as **controller** in para 2? Is Europol meant as it is pointed out in the definitions in Art.3 points 8 of the Regulation (EU) 2018/1725?

On Art. 30, para 3 we would like to mention the reference made to Art. 20, para 2a where it comes on **dedicated operational analysis projects**. We kindly ask the European Commission for clarification what is meant under this definition and is it linked to the concept of High Value Targets and Operational Task Force? And which are these **dedicated** operational analysis projects?

We would like to kindly ask the Europol to provide information concerning what would be the practical implementation of this provision.

Art. 20 2a. In the framework of ~~conducting dedicated~~ operational analysis projects as referred to in Article 18(3), Member States may determine information to be made directly accessible by Europol to selected other Member States for the purpose of enhanced collaboration in specific investigations, without prejudice to any restrictions of Article 19(2)

On Art. 34, para 1 we express principle support for the obligation for Europol to inform the competent authorities of the Member States in case of a personal data breach. Nevertheless, we would like to request a clarification about the criteria on the basis of which Europol will decide whether the breach should be reported or is unlikely to result in a risk for the rights and freedoms of persons.

On Art. 39 we believe that the prior consultation procedure with the EDPS should not have impact on Europol's operational capabilities and Europol's support to MS as well as its role in innovations.

CZECH REPUBLIC

CZ comments – amendment to Europol Regulation bloc 8

Pursuant to the request by the Presidency, CZ proposes following changes to WK 757/2020 REV 4:

Bloc 8 (Data Protection)

Because the bloc 8 contains substantial and systemic changes, CZ reserves further comments.

Art. 2(l)

We understand the opinion of the Commission that the definition of "recipient" is broader in the Europol Regulation. But it is not clear at all why this definition should be different from GDPR, LED and Art. 2(13) EUDPR:

(l) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Art. 21(8)

Unless this provision is moved to Art. 24 (it concerns transfer of data by Europol, rather than access to data by OLAF), data ownership principle must be referred to. Our previous proposal to inform ENUs still applies:

8. If during information-processing activities in respect of an individual investigation or specific project Europol identifies information relevant to possible illegal activity affecting the financial interest of the Union, Europol shall**, without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2),** on its own initiative without undue delay provide OLAF with that information. **It shall inform all national units concerned at the same time.**

Art. 24(2)

This Article should be harmonized with Art. 23.

As regards para (2), we propose to explicitly establish an obligation of data recipient to cooperate in verification of its competence, due to practical reasons:

2. Where the operational personal data are transmitted following a request from another Union institution, body, office or agency, both the controller and the recipient shall bear the responsibility for the lawfulness of that transmission.

Europol shall verify the competence of the other Union institution, body, office or agency**, which shall cooperate in the process**. If doubts arise as to this necessity of the transmission of the personal data, Europol shall seek further information from the recipient.

The recipient Union institution, body, office or agency shall ensure that the necessity of the transmission of the operational personal data can be subsequently verified.

Art. 30(2)

We understand the rationale for the amendment. However, text equivalent to part of recital (29) of EUDPR should be introduced among recitals, in order to ensure that Member States may continue to access photographs as before:

„The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.“

Art. 30(3)

This prohibition is too broad in the context of police cooperation and combating crime. We believe that restricted access by the competent authorities of Member States to such personal data is fully justified, if the Europol retains access control and ability to set conditions:

3. ~~**Only Europol shall have d**~~**D**irect access to personal data as referred to in paragraphs 1 and 2 **shall be limited to Europol and, in** ~~**except for the**~~ cases outlined in Article 20 (2a) **and other justified cases identified by the Executive Director**. The Executive Director shall duly authorise a limited number of Europol **and Member State** officials to have such access if it is necessary for the performance of their tasks **and establish appropriate safeguards**.

Art. 32

We disagree with this technique, where one Regulation obliges the Member States to implement other Regulation, which was not even applicable to Member States in the first place. Consequences of such a change are completely unclear and may even include the competence of EDPS over the authorities in the Member States pursuant to Art. 43(1). The text should either be moved to recital or kept as before:

Europol and Member States shall establish mechanisms to ensure that security **needs are taken on board across information system boundaries.**

Art. 39

We believe that paragraph (1) is incompatible with risk-based approach and does not respect the importance of processing of special categories of data in police work, which is indicated by permissive wording of Art. 10 LED. We note that Art. 28 LED does not contain the obligation of such prior consultation either. Prior consultation pursuant to Art. 90 of EUDPR is fully sufficient. ***Consequently, both paragraphs (1) and (4) should be deleted.***

CZ remains flexible as regards changes to recital (50) of Europol Regulation.

Art. 39a

We believe that this provision should correspond to Art. 24 LED and include the use of profiling, where applicable (see Art. 24(1)(e) LED).

Art. 41(2)

Ability of DPO to fulfill her or his tasks under EUDPR should be included:

2. The Data Protection Officer shall be selected on the basis of his or her personal and professional qualities and, in particular, the expert knowledge of data protection and practices and the ability to fulfil his or her tasks under this Regulation **and Regulation (EU) 2018/1725**.

Art. 41(4)

The "Executive Board" should be changed to Management Board:

3.4. The Data Protection Officer shall be designated~~appointed~~ for a term of four years and~~. He or she~~ shall be eligible for reappointment ~~up to a maximum total term of eight years~~. The Data Protection Officer~~He or she~~ may be dismissed from his or her ~~function~~ post ~~as Data Protection Officer~~ by the **Management** ~~**Executive**~~ Board only with the agreement~~consent~~ of the EDPS, if he or she no longer ~~meets~~ fulfils the conditions required for the performance of his or her duties.

Art. 42(1)(2)

We do not understand why references to monitoring tasks of the national supervisory authorities should be deleted?

Art. 44 and Art. 45

It is proposed that the mechanism for cooperation in Art. 45 should be replaced by Art. 62 EUDPR. However, we believe that such a change was not properly substantiated and thought through. For example, why is it necessary to keep rules about using national DPAs expertise in Art. 44(2)? In the light of Art. 62(1)(2) EUDPR, do we need Art. 44(3)? Why the Art. 44(4) still refers to Cooperation Board and Art. 45(1)?

(end of file)

FRANCE

NOTE DE COMMENTAIRES DES AUTORITÉS FRANÇAISES

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leurs commentaires écrits concernant le bloc thématique numéro 8 relatif à la protection des bases de données en prévision de la réunion LEWP du 7 mai 2021 :

- **Commentaires généraux concernant la révision du règlement Europol :**

Les autorités françaises accueillent favorablement les propositions de la Commission qui, en adaptant le règlement Europol aux exigences du règlement du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union (règlement 1725) propose des mécanismes constructifs au service de l'agence.

Toutefois, une lecture attentive, article par article, est indispensable pour adapter ce règlement aux exigences opérationnelles de l'agence Europol. Les autorités françaises regrettent notamment la suppression de nombreuses définitions du règlement actuel.

- **Concernant le bloc thématique n°8 (protection des bases de données) :**

Bloc 8 Renforcer le cadre de protection des données applicables à Europol	
Proposition de la Commission	Commentaires des autorités françaises
Article 1(1)(a)-Article 2(h) ~~'personal data' means any information relating to a data subject;~~	Les autorités françaises relèvent que, conformément à l'article 27 (a) de sa proposition, la Commission souhaite voir appliquer les définitions prévues à l'article 3 du règlement 1725 au règlement Europol. Si les autorités françaises ne s'opposent pas à l'application de ces définitions au règlement Europol, elles relèvent que par souci de **clarté, de sécurité et afin de déterminer au mieux les besoins de l'agence,** le règlement Europol doit comporter les définitions de l'ensemble des termes qui y sont utilisés. Si les autorités françaises sont conscientes que le règlement 1725 s'appliquera à Europol dès l'adaptation de celui-ci réalisée, elles proposent de reprendre les définitions du règlement 1725 et de les inscrire dans le règlement Europol. Enfin, les autorités françaises souhaitent que la Commission précise si l'ensemble des définitions supprimées dans sa proposition sont reprises dans le règlement 1725.
Article 1(1)(a)-Article 2(i) ~~data subject' means an identified or identifiable natural person, an identifiable person being a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;~~	
Article 1(1)(a)-Article 2(j) ~~genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the~~	

~~health of that individual, resulting in particular from an analysis of a biological sample from the individual in question~~	
Article 1(1)(a)-Article 2(k) ~~'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;~~	
Article 1(1)(a)-Article 2(m) ~~'transfer of personal data' means the communication of personal data, actively made available, between a limited number of identified parties, with the knowledge or intention of the sender to give the recipient access to the personal data;~~	
Article 1(1)(a)-Article 2(n) ~~'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;~~	
Article 1(1)(a)-Article 2(o) ~~'the data subject's consent' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to him or her being processed;~~	
Article 1(1)(b)-Article 2(p)	

2

'administrative personal data' means all personal data processed by Europol apart from operational data;";	
Article 1(9)-Article 21(8) Access by Eurojust, OLAF and, only for purposes of ETIAS, by the European Border and Coast Guard Agency to information stored by Europol 8. If during information-processing activities in respect of an individual investigation or specific project Europol identifies information relevant to possible illegal activity affecting the financial interest of the Union, Europol shall on its own initiative without undue delay provide OLAF with that information.	Les autorités françaises proposent de définir les termes *"individual investigation"* et *"specific project"*. Si les autorités françaises ne s'opposent pas à cette proposition, elles rappellent néanmoins qu'Europol devra obtenir l'accord de l'Etat membre fournisseur de la donnée avant de la transmettre à l'OLAF. Elles soutiennent donc les délégations de République - Tchèque et de Bulgarie sur ce point. Les autorités françaises sont d'avis qu'il conviendrait d'ajouter les termes « *without prejudice to any restriction indicated by Member State* » à la fin du paragraphe.
Article 1(10)-Article 24 Transmission of operational personal data to Union institutions, bodies, offices and agencies 1. Subject to any further restrictions pursuant to this Regulation, in particular pursuant to Article 19(2) and (3) and without prejudice to Article 67, Europol shall only transmit operational personal data to another Union institution, body, office or agency if the data are necessary for the legitimate performance of tasks of the other Union institution, body, office or agency. 2. Where the operational personal data are transmitted following a request from another Union institution, body, office or agency, both the controller and the recipient shall bear the responsibility for the lawfulness of that transmission. Europol shall verify the competence of the other Union institution, body, office or agency . If doubts arise as to this necessity of the transmission of the personal data, Europol shall seek further information from the recipient. The recipient Union institution, body, office or agency shall ensure that the necessity of the transmission of the operational personal data can be subsequently verified.	Les autorités françaises relèvent le manque de précision de cette proposition d'article. Notamment, elles estiment qu'il conviendrait de préciser quelle instance au sein d'Europol - Directeur exécutif, Officier de protection des données (DPO), Conseil d'administration - vérifiera la compétence de l'autorité requérante de la donnée lors d'un transfert. Elles souhaiteraient également que la Commission précise l'étendue du « complément d'informations » qu'Europol pourra exiger pour apprécier la compétence des partenaires auxquels l'agence pourrait transmettre des informations. Concernant, l'expression « *legitimate performance* », les autorités françaises interrogent la Commission sur cette notion et sur l'autorité au sein d'Europol qui sera chargée d'évaluer « l'exécution légitime » des missions qui préside à la transmission de données. Enfin, les autorités françaises soutiennent la délégation hollandaise sur l'importance de préciser à l'article 24 la coopération avec les seules agences du domaine JAI.

3. The recipient Union institution, body, office or agency shall process the operational personal data only for the purposes for which they were transmitted."	
Article 1(11) (a)-Article 25 (8) Transfer of personal data to third countries and international organisations Where a transfer is based on paragraph 4a or 5, such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.	Aucun commentaire.
Article 1(14)-Article 27 (a) Processing of personal data by Europol 1. This Regulation, Article 3 and Chapter IX of Regulation (EU) 2018/1725 of the European Parliament and of the Council* shall apply to the processing of operational personal data by Europol. Regulation (EU) 2018/1725, with the exception of its Chapter IX, shall apply to the processing of administrative personal data by Europol. 2. References to 'applicable data protection rules' in this Regulation shall be understood as references to the provisions on data protection set out in this Regulation and in Regulation (EU) 2018/1725. 3. References to 'personal data' in this Regulation shall be understood as references to 'operational personal data', unless indicated otherwise. 4. Europol shall determine the time limits for the storage of administrative personal data in its rules of procedure.	Pour mémoire, les autorités françaises rappellent que l'article 98 du règlement 2018/1725 prévoit que la Commission doit réviser le règlement Europol avant le 30 avril 2022 afin de s'assurer de sa compatibilité avec la directive (UE) 2016/680 et avec le chapitre IX du règlement 1725. Les autorités françaises rappellent que, selon l'officier de protection des données d'Europol (DPO), le chapitre IX du règlement 1725 s'applique déjà aux autres agences de l'UE et que ses dispositions sont plus « génériques » que celle actuellement prévues dans le règlement Europol, autorisant ainsi une certaine flexibilité pour l'agence. Toutefois, l'application de ce chapitre à Europol - si elle peut être saluée à certains égards - nécessite des aménagements qu'il convient de détailler article par article.

Article 1(15)-Article 28 General data protection principles ~~Personal data shall be: (a) processed fairly and lawfully;~~ ~~(b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing of personal data for historical, statistical or scientific research purposes shall not be considered incompatible provided that Europol provides appropriate safeguards, in particular to ensure that data are not processed for any other purposes;~~ ~~(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;~~ ~~(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;~~ ~~e) kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed; and~~ ~~(f) processed in a manner that ensures appropriate security of personal data. 2. Europol shall make publicly available a document setting out in an intelligible form the provisions regarding the processing of personal data and the means available for the exercise of the rights of data subjects.~~	Aucun commentaire.
Article 30 Processing of special categories of personal data and of different categories of data subjects 1. Processing of personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences, or in respect of persons under the age of 18, shall be allowed if it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives	Aucun commentaire.

2. Processing of personal data, by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data and biometric data for the purpose of uniquely identifying a natural person or data concerning a person's health or sex life or sexual orientation shall be allowed only where strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol. The selection of a particular group of persons solely on the basis of such personal data shall be prohibited. 3. Only Europol shall have direct access to personal data as referred to in paragraphs 1 and 2., except for the cases outlined in Article 20 (2a). The Executive Director shall duly authorise a limited number of Europol officials to have such access if it is necessary for the performance of their tasks. 5. Personal data as referred to in paragraphs 1 and 2 shall not be transmitted to Member States, Union bodies, or transferred to third countries and international organisations unless such transmission or transfer is strictly necessary and proportionate in individual cases concerning crimes that falls within Europol's objectives and in accordance with Chapter V 6. Every year Europol shall provide to the EDPS a statistical overview of all personal data as referred to in paragraph 2 which it has processed.	
Article 1(17)-Article 32 Security of processing Europol and Member States shall establish mechanisms to ensure that security measures referred to in Article 91 of Regulation (EU) 2018/1725 are addressed across information system boundaries.	Aucun commentaire.

Article 1(18)-Article 33 Data protection by design ~~Europol shall implement appropriate technical and organisational measures and procedures in such a way that the data processing will comply with this Regulation and protect the rights of the data subjects concerned.~~	Aucun commentaire.
Article 1 (20)-Article 34 Notification of a personal data breach to the authorities concerned 1. In the event of a personal data breach, Europol shall without undue delay notify the competent authorities of the Member States concerned, of that breach, in accordance with the conditions laid down in Article 7(5),as well as the provider of the data concerned unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. 2. The notification referred to in paragraph 1 shall, as a minimum: (a) describe the nature of the personal data breach including, where possible and appropriate, the categories and number of data subjects concerned and the categories and number of data records concerned; (b) describe the likely consequences of the personal data breach; (c) describe the measures proposed or taken by Europol to address the personal data breach; and (d) where appropriate, recommend measures to mitigate the possible adverse effects of the personal data breach.	Les autorités françaises rappellent que l'actuel article 34 prévoit qu'en cas de violation de données à caractère personnel, Europol en informe le CEPD ainsi que les autorités compétentes des États membres concernés sans aucune forme de modération. Afin d'assurer la transparence totale de l'activité de l'agence, la France estime nécessaire de supprimer la phrase suivante : « *unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons* ».
Article 1 (21)-Article 35 Communication of a personal data breach to the data subject ~~1.Subject to paragraph 4 of this Article, where a personal data breach as referred to in Article 34 is likely to severely and adversely affect the rights and freedoms of the data subject, Europol shall communicate the personal data breach to the data subject without undue delay.~~ ~~2. The communication to the data subject referred~~	Aucun commentaire.

~~to in paragraph 1 shall describe, where possible, the nature of the personal data breach, recommend measures to mitigate the possible adverse effects of the personal data breach, and contain the identity and contact details of the Data Protection Officer.~~ Without prejudice to Article 93 of Regulation 2018/1725, if Europol does not have the contact details of the data subject concerned, it shall request the provider of the data to communicate the personal data breach to the data subject concerned and to inform Europol about the decision taken. Member States providing the data shall communicate the breach to the data subject concerned in accordance with the procedures of their national law. ~~4. The communication of a personal data breach to the data subject shall not be required if:~~ ~~(a) Europol has applied to the personal data concerned by that breach appropriate technological protection measures that render the data unintelligible to any person who is not authorised to access it;~~ ~~(b) Europol has taken subsequent measures which ensure that the data subject's rights and freedoms are no longer likely to be severely affected; or~~ ~~(c) such communication would involve disproportionate effort, in particular owing to the number of cases involved. In such a case, there shall instead be a public communication or similar measure informing the data subjects concerned in an equally effective manner.~~ ~~5. The communication to the data subject may be delayed, restricted or omitted where this constitutes a necessary measure with due regard for the legitimate interests of the person concerned:~~ ~~(a) to avoid obstructing official or legal inquiries, investigations or procedures;~~ ~~(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal~~	

~~penalties;~~ ~~(c) to protect public and national security;~~ ~~(d) to protect the rights and freedoms of third parties.~~	
Article 1 (22)-Article 36 Right of access for the data subject ~~**1. Any data subject shall have the right, at reasonable intervals, to obtain information on whether personal data relating to him or her are processed by Europol.**~~ ~~**2. Without prejudice to paragraph 5, Europol shall provide the following information to the data subject:**~~ ~~**(a) confirmation as to whether or not data related to him or her are being processed;**~~ ~~**(b) information on at least the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;**~~ ~~**(c) communication in an intelligible form of the data undergoing processing and of any available information as to their sources;**~~ ~~(d) an indication of the legal basis for processing the data;~~ ~~(e) the envisaged period for which the personal data will be stored;~~ ~~(f) the existence of the right to request from Europol rectification, erasure or restriction of processing of personal data concerning the data subject.~~ 3. Any data subject wishing to exercise the right of access referred to in Article 80 of Regulation (EU) 2018/1725 to personal data that relate to the data subject may make a request to that effect, without incurring excessive costs, to the authority appointed for that purpose in the Member State of his or her choice, or to Europol. Where the request is made to the Member State authority, that authority shall refer the request to Europol without delay, and in any case within one month of receipt. 4. Europol shall confirm receipt of the request	Actuellement, Europol est tenu, en vertu de l'article 36, paragraphe 5 de son règlement de consulter les autorités compétentes des États membres et le fournisseur des données sur la décision à prendre en matière d'accès aux données des personnes concernées. Si un État membre s'oppose à la fourniture d'informations, Europol doit tenir **le « plus grand compte de cette objection ».** Dans sa proposition (article 27a) la Commission propose d'appliquer au traitement de données opérationnelles par l'agence le chapitre IX du règlement 1725. Or ce chapitre prévoit - notamment l'article 83 – qu'une décision sur l'accès aux données doit être prise **en consultation et en étroite coopération avec l'autorité compétente concernée**. Ainsi, les autorités françaises souhaitent que la Commission précise comment le chapitre IX du règlement 1725 et l'article 36, tel que proposé, pourront se concilier en pratique. A ce stade des discussions, les autorités françaises relèvent que le régime prévu au chapitre IX du règlement 1725 risque de nuire à la bonne collaboration entre Europol et les services contributeurs en ce qu'il **étend considérablement la marge de manœuvre de l'agence dans l'appréciation de l'octroi du droit d'accès** sur des informations fournies par les **États membres** eux-mêmes. Également, les autorités françaises relèvent que les justifications permettant de ne pas octroyer l'accès aux données d'Europol ont été supprimées. La France s'inquiète de cette suppression en ce que ces justifications permettent de protéger les enquêtes en cours. Si le règlement 1725 prévoit effectivement de telles justifications, la France demande à ce que les restrictions au droit d'accès des données soient prévues dans l'article 36.

under paragraph 3. Europol shall answer it without undue delay, and in any case within three months of receipt by Europol of the request from the national authority. 5. Europol shall consult the competent authorities of the Member States, in accordance with the conditions laid down in Article 7(5), and the provider of the data concerned, on a decision to be taken. A decision on access to personal data shall be conditional on close cooperation between Europol and the Member States and the provider of the data directly concerned by the access of the data subject to such data. If a Member State or the provider of the data objects to Europol's proposed response, it shall notify Europol of the reasons for its objection in accordance with paragraph 6 of this Article. Europol shall take the utmost account of any such objection. Europol shall subsequently notify its decision to the competent authorities concerned, in accordance with the conditions laid down in Article 7(5), and to the provider of the data. ~~6. The provision of information in response to any request under paragraph 1 may be refused or restricted if such refusal or restriction constitutes a measure that is necessary in order to:~~ ~~(a) enable Europol to fulfil its tasks properly;~~ ~~(b) protect security and public order or prevent crime;~~ ~~(c) guarantee that any national investigation will not be jeopardised; or~~ ~~(d) protect the rights and freedoms of third parties.~~ ~~When the applicability of an exemption is assessed, the fundamental rights and interests of the data subject shall be taken into account.~~ ~~7. Europol shall inform the data subject in writing of any refusal or restriction of access, of the reasons for such a decision and of his or her right to lodge a complaint with the EDPS.~~ ~~Where the provision of such information would deprive paragraph 6 of its effect, Europol shall only notify the data subject concerned that it has carried out the checks, without giving any information which might reveal to him or her whether or not personal data concerning him or her are processed by Europol.~~	

10

Article 1 (23)-Article 37 Right to rectification, erasure and restriction 1. Any data subject wishing to exercise the right to rectification or erasure of personal data or of restriction of processing referred to in Article 82 of Regulation (EU) 2018/1725 of personal data that relate to him or her may make a request to that effect through the authority appointed for that purpose in the Member State of his or her choice, or to Europol Where the request is made to the Member State authority, that authority shall refer the request to Europol without delay and in any case within one month of receipt. 1. ~~Any data subject having accessed personal data concerning him or her processed by Europol in accordance with Article 36 shall have the right to request Europol, through the authority appointed for that purpose in the Member State of his or her choice, to erase personal data relating to him or her held by Europol if they are no longer required for the purposes for which they are collected or are further processed. That authority shall refer the request to Europol without delay and in any case within one month of receipt~~. 2.Without prejudice to Article 82(3) of Regulation 2018/1725 Europol shall restrict rather than erase personal data as referred to in paragraph 2 if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject.Restricted data shall be processed only for the purpose that prevented their erasure . 4. If personal data as referred to in paragraphs 1, 2 and 3 held by Europol have been provided to it by third countries, international organisations or Union bodies, have been directly provided by private parties or have been retrieved by Europol from publicly available ressources or result from Europol's own analyses, Europol shall rectify, erase or restrict such data and, where appropriate, inform the providers of the data. 5. If personal data as referred to in paragraphs 1, 2 and 3 held by Europol have been provided to	Pour rappel, Europol peut restreindre l'accès plutôt que supprimer la donnée « *lorsqu'il y a de bonnes raisons de croire que leur effacement pourrait porter atteinte aux intérêts légitimes de la personne concernée* ». L'article 82, paragraphe 3, du règlement 2018/1725 ne prévoit cette possibilité que dans **deux cas** de figure spécifiquement définis, à savoir si l'exactitude des données à caractère personnel est contestée par la personne concernée ou lorsque les données à caractère personnel doivent être conservées à des fins probatoires. En conséquence, les autorités françaises tirent la conclusion que la référence à l'article 82 fait perdre de la souplesse aux dispositions actuelles. Également, la France souhaite qu'une référence à la limitation du droit de rectification, de suppression et de restriction soit inscrite dans cet article en citant expressément l'article 82 (4) du règlement 1725).

Europol by Member States, the Member States concerned shall rectify, erase or restrict such data in collaboration with Europol, within their respective competences. 6. If incorrect personal data have been transferred by another appropriate means or if the errors in the data provided by Member States are due to faulty transfer or transfer in breach of this Regulation or if they result from data being input, taken over or stored in an incorrect manner or in breach of this Regulation by Europol, Europol shall rectify or erase such data in collaboration with the provider of the data concerned. 7. In the cases referred to in paragraphs 4, 5 and 6, all addressees of the data concerned shall be notified forthwith. In accordance with the rules applicable to them, the addressees shall then rectify, erase or restrict those data in their systems. ~~8. Europol shall inform the data subject in writing without undue delay, and in any case within three months of receipt of a request in accordance with paragraph 1 or 2, that data concerning him or her have been rectified, erased or restricted.~~ ~~9. Within three months of receipt of a request in accordance with paragraph 1 or 2, Europol shall inform the data subject in writing of any refusal of rectification, erasure or restricting, of the reasons for such a refusal and of the possibility of lodging a complaint with the EDPS and of seeking a judicial remedy.~~	
Article 1 (24)-Article 37 (a) Right to restriction of processing Right to restriction of processing Where the processing of personal data has been restricted under Article 82(3) of Regulation (EU) 2018/1725, such personal data shall only be processed for the protection of the rights of the data subject or another natural or legal person or for the purposes laid down in Article 82(3) of that Regulation.”;	Aucun commentaire.
Article 1 (25)-Article 38 Responsibility in data protection matters 1. Europol shall store personal data in a way that ensures that their source, as referred to	Aucun commentaire.

in Article 17, can be established. 2. The responsibility for the quality of personal data as referred to in point (d) of Article 28(1) shall lie with: (a) the Member State or the Union body which provided the personal data to Europol; (b) Europol in respect of personal data provided by third countries or international organisations or directly provided by private parties; of personal data retrieved by Europol from publicly available sources or resulting from Europol's own analyses; and of personal data stored by Europol in accordance with Article 31(5). 3. If Europol becomes aware that personal data provided pursuant to points (a) and (b) of Article 17(1) are factually incorrect or have been unlawfully stored, it shall inform the provider of those data accordingly. 4. Responsibility for compliance with Regulation (EU) 2018/1725 in relation to administrative personal data and for compliance with this Regulation and with Article 3 and Chapter IX of Regulation (EU) 2018/1725 in relation to operational personal data shall lie with Europol. 5. The responsibility for the legality of a data transfer shall lie with: (a) the Member State which provided the personal data to Europol; (b) Europol in the case of personal data provided by it to Member States, third countries or international organisations. 6. In the case of a transfer between Europol and a Union body, the responsibility for the legality of the transfer shall lie with Europol Without prejudice to the first subparagraph, where the data are transferred by Europol following a request from the recipient, both Europol and the recipient shall be responsible for the legality of such a transfer. 7. Europol shall be responsible for all data processing operations carried out by it, with the exception of the bilateral exchange of data using Europol's infrastructure between Member States, Union bodies, third countries and	

international organisations to which Europol has no access. Such bilateral exchanges shall take place under the responsibility of the entities concerned and in accordance with their law. The security of such exchanges shall be ensured in accordance with Article 91 of Regulation (EU) 2018/172532.	
Article 1 (26)-Article 39 Prior consultation Without prejudice to Article 90 of Regulation (EU) 2018/1725, any new type of processing operations to be carried out shall be subject to prior consultation of the EDPS where : (a) special categories of data as referred to in Article 30(2) are to be processed. The EDPS shall keep a register of all processing operations that have been notified to him or her pursuant to paragraph 1. The register shall not be made public	Tout d'abord, les autorités françaises relèvent que le régime actuel est particulièrement lourd pour Europol en ce que la consultation préalable du CEPD doit être réalisée en cas de « risque spécifique » soit pour l'ensemble de l'activité d'Europol comme a pu le relever le DPO de l'agence. L'article 90 du règlement 1725 dispose que tout nouveau type d'opérations de traitement d'Europol doit faire l'objet d'une consultation préalable du CEPD « *lorsque le type de traitement, [...] présente des **risques élevés** pour les libertés et les droits des personnes concernées.* ». Les autorités françaises saluent donc la plus grande souplesse du nouveau mécanisme présenté.
Article 1 (27) – article 39a Records of categories of processing activities 1. Europol shall maintain a record of all categories of processing activities under its responsibility. That record shall contain the following information: (a) Europol's contact details and the name and the contact details of its Data Protection Officer; (b) the purposes of the processing; (c) the description of the categories of data subjects and of the categories of operational personal data; (d) the categories of recipients to whom the operational personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of operational personal data to a third country, an international organisation, or private party including the identification of that third country, international organisation or private party;	Aucun commentaire.

(f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 91 of Regulation (EU) 2018/1725. 2. The records referred to in paragraph 1 shall be in writing, including in electronic form. 3. Europol shall make the records referred to in paragraph 1 available to the EDPS on request.	
Article 1 (28)-Article 40 Logging In line with Article 88 of Regulation (EU) 2018/1725, Europol shall keep logs of its processing operations. There shall be no possibility of modifying the logs 2. LWithout prejudice to Article 88 of Regulation (EU) 2018/1725, the logs prepared pursuant to paragraph 1 if required for a specific investigation, related to compliance with data protection rules, shall be communicated to the national unit concerned. The information thus communicated shall only be used for the control of data protection and for ensuring proper data processing as well as data integrity and security.	Aucun commentaire.
Article 1 (29)-Article 41 Data Protection Officer 1. The Management Board shall appoint a Data Protection Officer, who shall be a member of the staff specifically appointed for this purpose. In the performance of his or her duties, he or she shall act independently and may not receive any instructions. 2. The Data Protection Officer shall be selected on the basis of his or her personal and professional qualities and, in particular, the expert knowledge of data protection and practices and the ability to fulfil his or her tasks under this Regulation. The selection of the Data Protection Officer shall not be liable to result in a onflict of interests between his or her duty as Data Protection Officer and ny other official duties he or	Tout d'abord, les autorités françaises font part de leur étonnement sur le fait que la Commission propose que le mandat du DPO soit renouvelable **sans limite de temps**. La délégation française à Europol rappelle fréquemment que la gestion des ressources humaines – y compris pour les postes à haute responsabilité – doit répondre à des règles strictes notamment sur l'octroi d'emplois à durée indéterminée. Du point de vue des autorités françaises, et en l'état du statut du DPO, l'accord de l'EDPS suffit à garantir la transparence et le contrôle des décisions prises et à limiter les risques de conflit d'intérêt. Si la Commission propose d'octroyer ce droit de démission au Directeur exécutif, les autorités françaises s'y opposent pour des raisons de conflit d'intérêts évidents.

she may have, in particular in relation to the application of this Regulation. The Data Protection Officer shall be designated for a term of four years and shall be eligible for reappointment; The Data Protection Officer may be dismissed from his or her by the Executive Board only with the agreement of the EDPS, if he or she no longer fulfils the conditions required for the performance of his or her duties. 5 After his or her designation the Data Protection Officer shall be registered with the European Data Protection Supervisor by the Management Board 6 Europol shall publish the contact details of the Data Protection Officer and communicate them to the EDPS	
Article 1 (30)-Article 41 (a) Position of the Data Protection Officer 1. Europol shall ensure that the Data Protection Officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. 2. Europol shall support the Data Protection Officer in performing the tasks referred to in Article 41c by providing the resources and staff necessary to carry out those tasks and by providing access to personal data and processing operations, and to maintain his or her expert knowledge. The related staff may be supplemented by an assistant DPO in the area of operational and administrative processing of personal data. 3. Europol shall ensure that the Data Protection Officer does not receive any instructions regarding the exercise of those tasks. The Data Protection Officer shall report directly to the Management Board. The Data Protection Officer shall not be dismissed or penalised by the Management Board for performing his or her tasks. 4. Data subjects may contact the Data Protection Officer with regard to all issues related to	Aucun commentaire.

processing of their personal data and to the exercise of their rights under this Regulation and under Regulation (EU) 2018/1725. No one shall suffer prejudice on account of a matter brought to the attention of the Data Protection Officer alleging that a breach of this Regulation or Regulation (EU) 2018/1725 has taken place. 5. The Management Board shall adopt further implementing rules concerning the Data Protection Officer. Those implementing rules shall in particular concern the selection procedure for the position of the Data Protection Officer, his or her dismissal, tasks, duties and powers, and safeguards for the independence of the Data Protection Officer. 6. The Data Protection Officer and his or her staff shall be bound by the obligation of confidentiality in accordance with Article 67(1).	
Article 1 (30)-Article 41 (b) Tasks of the Data Protection Officer 1. The Data Protection Officer shall, in particular, have the following tasks with regard to processing of personal data: (a) ensuring in an independent manner the compliance of Europol with the data protection provisions of this Regulation and Regulation (EU) 2018/1725 and with the relevant data protection provisions in Europol's rules of procedure; this includes monitoring compliance with this Regulation, with Regulation (EU) 2018/1725, with other Union or national data protection provisions and with the policies of Europol in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits.; b) informing and advising Europol and staff who process personal data of their obligations pursuant to this Regulation, to Regulation (EU) 2018/1725 and to other Union or national data protection provisions; c) providing advice where requested as regards the data protection impact assessment and monitoring its performance pursuant to Article 89 of Regulation (EU) 2018/1725; d) keeping a register of personal data breaches and providing advice where requested as regards the necessity of a notification or communication of a	Les autorités françaises constatent que dans le cadre de ses missions le DPO pourrait être amené à veiller au respect par Europol des règles de l'Union mais également des **règles nationales** de protection des données. Les autorités françaises estiment que cette surveillance, lorsqu'il s'agit du droit national, doit se réaliser en étroite collaboration avec les autorités nationales de supervision.

personal data breach pursuant to Articles 92 and 93 of Regulation (EU) 2018/1725; (e) ensuring that a record of the transfer and receipt of personal data is kept in accordance with this Regulation; (f) ensuring that data subjects are informed of their rights under this Regulation and Regulation (EU) 2018/1725 at their request; (g) cooperating with Europol staff responsible for procedures, training and advice on data processing; (h) cooperating with the EDPS; (i) cooperating with the national competent authorities, in particular with the appointed Data Protection Officers of the competent authorities of the Members States and national supervisory authorities regarding data protection matters in the law enforcement area; (j) acting as the contact point for the European Data Protection Supervisor on issues relating to processing, including the prior consultation under Articles 39 and 90 of Regulation (EU) 2018/1725, and consulting, where appropriate, with regard to any other matter; (k) preparing an annual report and communicating that report to the Management Board and to the EDPS; 2. The Data Protection Officer shall carry out the functions provided for by Regulation (EU) 2018/1725 with regard to administrative personal data. 3. In the performance of his or her tasks, the Data Protection Officer and the staff members of Europol assisting the Data Protection Officer in the performance of his or her duties shall have access to all the data processed by Europol and to all Europol premises. 4. If the Data Protection Officer considers that the provisions of this Regulation, of Regulation (EU) 2018/1725 related to the processing of administrative personal data or the provisions of this Regulation or of Article 3 and of Chapter IX of Regulation (EU) 2018/1725 concerning the processing of operational personal data have not been complied with, he or she shall inform the Executive Director and shall require him or her to resolve the noncompliance within a specified time.	

If the Executive Director does not resolve the non-compliance of the processing within the time specified, the Data Protection Officer shall inform the Management Board. The Management Board shall reply within a specified time limit agreed with the Data Protection Officer. If the Management Board does not resolve the non-compliance within the time specified, the Data Protection Officer shall refer the matter to the EDPS.”;	
Article 1 (31)-Article 42 Supervision by the national supervisory authority For the purpose of exercising their supervisory function the national supervisory authority shall have access, at the national unit or at the liaison officers' premises, to data submitted by its Member State to Europol in accordance with the relevant national procedures and to logs and documentation as referred to in Article 40. National supervisory authorities shall have access to the offices and documents of their respective liaison officers at Europol. 3. National supervisory authorities shall, in accordance with the relevant national procedures, supervise the activities of national units and the activities of liaison officers, insofar as such activities are relevant to the protection of personal data. They shall also keep the EDPS informed of any actions they take with respect to Europol. 4. Any person shall have the right to request the national supervisory authority to verify the legality of any transfer or communication to Europol of data concerning him or her in any form and of access to those data by the Member State concerned. That right shall be exercised in accordance with the national law of the Member State in which the request is made.	Aucun commentaire.
Article 1 (32)-Article 43 Supervision by the EDPS 1. The EDPS shall be responsible for monitoring and ensuring the application of the provisions of this	Les autorités françaises s'étonnent de constater que les autorités nationales de supervision ne soient plus consultées lorsque le CEPD produit son rapport annuel sur ses activités de supervision de

Regulation and Regulation (EU) 2018/1725 relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by Europol, and for advising Europol and data subjects on all matters concerning the processing of personal data. To that end, he or she shall fulfil the duties set out in paragraph 2 and exercise the powers laid down in paragraph 3, while closely cooperating with the national supervisory authorities in accordance with Article 44. 2. The EDPS shall have the following duties: (a) hearing and investigating complaints, and informing the data subject of the outcome within a reasonable period; (b) conducting inquiries either on his or her own initiative or on the basis of a complaint, and informing the data subject of the outcome within a reasonable period; (c) monitoring and ensuring the application of this Regulation and any other Union act relating to the protection of natural persons with regard to the processing of personal data by Europol; (d) advising Europol, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before it draws up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data; (e) keeping a register of new types of processing operations notified to him or her by virtue of Article 39(1) and registered in accordance with Article 39(4); (f) carrying out a prior consultation on processing notified to him or her. 3. The EDPS may pursuant to this Regulation: (a) give advice to data subjects on the exercise of their rights; (b) refer a matter to Europol in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects; (c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 36 and 37; (d) warn or admonish Europol;	l'agence mais simplement invitées à produire des observations.

(e) order Europol to carry out the rectification, restriction, erasure or destruction of personal data which have been processed in breach of the provisions governing the processing of personal data and to notify such actions to third parties to whom such data have been disclosed; (f) impose a temporary or definitive ban on processing operations by Europol which are in breach of the provisions governing the processing of personal data; (g) refer a matter to Europol and, if necessary, to the European Parliament, the Council and the Commission; (h) refer a matter to the Court of Justice of the European Union under the conditions provided for in the TFEU; (i) intervene in actions brought before the Court of Justice of the European Union. 4. The EDPS shall have the power to: (a) obtain from Europol access to all personal data and to all information necessary for his or her enquiries; (b) obtain access to any premises in which Europol carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there. 5. The EDPS shall draw up an annual report on his or her supervisory activities in relation to Europol That report shall be part of the annual report of the EDPS referred to in Article 60 of Regulation (EC) 2018/1725 The national supervisory authorities shall be invited to make observations on this report before it becomes part of the annual report. The EDPS shall take utmost account of the observations made by national supervisory authorities and, in any case, shall refer to them in the annual report. The report shall include statistical information regarding complaints, inquiries, and investigations as well as regarding transfers of personal data to third countries and international organisations, cases of prior consultation, and the use of the powers laid down in paragraph 3. 6. The EDPS, the officials and the other staff members of the EDPS's Secretariat shall be bound by the obligation of confidentiality laid down in Article 67(1).	

Article 1 (33)-Article 44 Cooperation between the EDPS and national supervisory authorities 1. The EDPS shall act in close cooperation with the national supervisory authorities on issues requiring national involvement, in particular if the EDPS or a national supervisory authority finds major discrepancies between the practices of Member States or potentially unlawful transfers in the use of Europol's channels for exchanges of information, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation. 1.In the cases referred to in paragraph 1, coordinated supervision shall be ensured in accordance with Article 62 of Regulation (EU) 2018/1725. The EDPS shall use theexpertise and experience of the national supervisory authorities in carrying out his or her duties as set out in Article 43(2). In carrying out joint inspections together with the EDPS, members and staff of national supervisory authorities shall, taking due account of the principles of subsidiarity and proportionality, have powers equivalent to those laid down in Article 43(4) and be bound by an obligation equivalent to that laid down in Article 43(6) 3. The EDPS shall keep national supervisory authorities fully informed of all issues directly affecting or otherwise relevant to them. Upon the request of one or more national supervisory authorities, the EDPS shall inform them of specific issues. 4. In cases relating to data originating from one or more Member States, including the cases referred to in Article 47(2), the EDPS shall consult the national supervisory authorities concerned. The EDPS shall not decide on further action to be taken before those national supervisory authorities have informed the EDPS of their position, within a deadline specified by him or her which shall not be shorter than one month and not longer than three months. The EDPS shall take the utmost account of the respective positions of the national supervisory authorities concerned. In cases where the EDPS intends not to follow the position of a national supervisory authority, he or she shall	Aucun commentaire.

inform that authority, provide a justification and submit the matter for discussion to the Cooperation Board established by Article 45(1). In cases which the EDPS considers to be extremely urgent, he or she may decide to take immediate action. In such cases, the EDPS shall immediately inform the national supervisory authorities concerned and justify the urgent nature of the situation as well as the action he or she has taken.	
Article 1 (34)-Article 45 **Cooperation Board** ~~1. A Cooperation Board with an advisory function is hereby established. It shall be composed of a representative of a national supervisory authority of each Member State and of the EDPS.~~ ~~2. The Cooperation Board shall act independently when performing its tasks pursuant to paragraph 3 and shall neither seek nor take instructions from any body.~~ ~~3. The Cooperation Board shall have the following tasks:~~ ~~(a) discussing general policy and strategy of data protection supervision of Europol and the permissibility of the transfer, the retrieval and any communication to Europol of personal data by the Member States;~~ ~~(b) examining difficulties of interpretation or application of this Regulation;~~ ~~(c) studying general problems relating to the exercise of independent supervision or the exercise of the rights of data subjects;~~ ~~(d) discussing and drawing up harmonised proposals for joint solutions on matters referred to in Article 44(1);~~ ~~(e) discussing cases submitted by the EDPS in accordance with Article 44(4);~~ ~~(f) discussing cases submitted by any national supervisory authority; and~~ ~~(g) promoting awareness of data protection rights.~~ ~~4. The Cooperation Board may issue opinions, guidelines, recommendations and best practices. The EDPS and the national supervisory authorities shall, without prejudice to their independence and each acting within the scope of their respective competences, take the utmost account of them.~~ ~~5. The Cooperation Board shall meet whenever necessary, and at least twice a year. The costs and servicing of its meetings shall be borne by the EDPS.~~	Aucun commentaire.

~~6. Rules of procedure of the Cooperation Board shall be adopted at its first meeting by a simple majority of its members. Further working methods shall be developed jointly as necessary.~~	
Article 1 (34)-Article 46 ~~Administrative personal data~~ ~~Regulation (EC) No 45/2001 shall apply to all administrative personal data held by Europol.~~	Aucun commentaire.
Article 1 (35)-Article 47 Right to lodge a complaint with the EDPS 1. Any data subject shall have the right to lodge a complaint with the EDPS if he or she considers that the processing by Europol of personal data relating to him or her does not comply with this Regulation or Regulation (EU) 2018/ 1725. 2. Where a complaint relates to a decision as referred to in Article 36, 37 or 3737a of this Regulation or Article 80, 81 or 82 of Regulation (EU) 2018/1725, the EDPS shall consult the national supervisory authorities of the Member State that provided the data or of the Member State directly concerned. In adopting his or her decision, which may extend to a refusal to communicate any information, the EDPS shall take into account the opinion of the national supervisory authority. 3. Where a complaint relates to the processing of data provided by a Member State toEuropol, the EDPS and the national supervisory authority of the Member State that provided the data shall, each acting within the scope of their respective competences, ensure that the necessary checks on the lawfulness of the processing of the data have been carried out correctly. 4. Where a complaint relates to the processing of data provided to Europol by Union bodies, third countries or international organisations, or of data retrieved by Europol from publicly available sources or resulting from Europol's own analyses, the EDPS shall ensure that Europol has correctly carried out the necessary checks on the lawfulness of the processing of the data. 5. The EDPS shall inform the data subject of the progress and outcome of the complaint, as well as the possibility of a judicial remedy pursuant to Article 48.	Aucun commentaire.

Article 1 (38)-Article 50 Right to compensation Any dispute between Europol and Member States over the ultimate responsibility for compensation awarded to a person who has suffered material or non-material damage in accordance with Article 65 of Regulation (EU) 2018/1725 and national laws transposing Article 56 of Directive (EU) 2016/680 shall be referred to the Management Board, which shall decide by a majority of two-thirds of its members, without prejudice to the right to challenge that decision in accordance with Article 263 TFEU.	Aucun commentaire.

HUNGARY

Article 21

We suggest to add in Paragraph 8 that the competent authorities of the Member States concerned shall be informed, in a timely manner if Europol provides information on its own initiative to OLAF during information-processing activities in respect of an individual investigation or a specific project.

Article 27

We would like to highlight that it would be reasonable to ensure that the retention of administrative personal data mentioned in the RoP of Europol is only possible in line with the applicable data protection provisins, so we suggest the following addition to Paragraph 4:

„Europol ***– in accordance with the applicable data protection rules, with particular attention to the storage limitation principle –*** *shall determine the time limits for the storage of administrative personal data in its rules of procedure."*

LUXEMBURG

Article 26 (11)

- *LU does accept the general principle of an annual report to the Management Board drawn up by Europol regarding the number of cases in which Europol issued follow-up requests to private parties or own-initiative requests to Member States of establishment for the transmission of personal data as requested by FR and backed by other delegations.*

- *However, we just need to assure that this new report does not include any operational data.*

- *Maybe one potential solution could be to link this new article 26 (11) with the provisions "taking into account the obligations of discretion and confidentiality" of article 51 (3) in order to avoid any confusion on this important matter.*

Recital 13 and article 4(5)

- *Like other delegations, we are kindly requesting to obtain further information about the meaning and the scope of the concept "investigative measures" as foreseen in recital 13 and article 4(5).*

NETHERLANDS

Comments the Netherlands on the Europol Regulation block 8

LEWP 26 April 2021

Bloc 8: strengthening the data protection framework applicable to Europol

- We are still studying the changes caused by the application of Regulation 2018/1725 to Europol, so we only have some preliminary remarks today.

- We would like to enter a scrutiny reservation regarding block 8.

- Article 2(m)

Article 2(m) of the Europol Regulation, which contained a definition of 'transfer of personal data' has been deleted. Is there a similar definition in the EUDPR? If not, why has it been proposed to delete article 2(m)?

- Art 24 Transmission of operational personal data to Union institutions, bodies, offices and agencies:

We would like to know the background of this article, which refers to transmitting operational personal data all institutions, bodies, offices and agencies of the Union. Why is it necessary to include them all, including non-JHA agencies? Why would Europol send operational personal data to these agencies, for example to the European Medicines Agency? In what circumstances would Europol share data with them? Does this happen a lot in practice?

- Art 27a para 4:

What is meant by Europol's "rules of procedure"? The Regulation stipulates that the MB should adopt rules of procedure (see art 11 para 1 subpara t), but as far as we can tell not that Europol should. Or is this provision intended to stipulate that it should? What would these rules of procedure be for?

- Art 39 Europol Regulation and 90 EUDPR:

- Does "filing system" as defined in art 3(7) EUDPR only refer to new IT systems or could this also refer to "specific individual operational activities"? Put another way, is art 90 EUDPR compatible with recital 50 of the Europol Regulation, which stipulates that the prior consultation mechanism "should not apply to specific individual operational activities, such as operational analysis projects, but to the use of new IT systems for the processing of personal data and any substantial changes thereto"?

- How much room does art 90 para 2 EUDPR give the EDPS to decide what falls under "a new filing system"?

- Art 90 para 3 EUDPR: Does the controller have to provide all DP impact assessments to the EDPS or only those where there is a high risk as in art 90 para 1 sub a?

- Art 39a

- Why have you included an article on records on processing activities? Chapter IX of the EUDPR does not contain one. Why is it necessary to include one here?

- Why are there no provisions for processors to keep records, as in art 31 para 2 EUDPR? Do we understand correctly that Europol does not use processors?

- Why is there no provision on a central register as in art 31 para 5 EUDPR?

- Art 41 para 2:

Art 43 para 3 EUDPR talks about "expert knowledge of data protection **law** and practices". The word "law" seems to be missing from the same phrase in art 41 para 2 of the Europol Regulation.

- Art 41 para 3:

We are not sure if we understand the phrase "shall not be liable to result in". Does this mean that the likelihood of a conflict of interest with his/her other duties should be avoided when the DPO is selected? Should a conflict of interests not be avoided completely? Maybe it would be clearer to say:

> "~~It shall be ensured in thet~~ ~~The selection of the Data Protection Officer shall not be liable to result in a~~~~that no~~ A conflict of ~~interest~~interests ~~may result from the performance of~~between ~~his or her duty as~~ the duties of the Data Protection Officer ~~in that capacity~~ and ~~from~~ any other official duties he or she may have, in particular in relation ~~those relating~~ to the application of this Regulation, shall be avoided."

Or maybe, since it is the MB that appoints / selects the DPO, the text could read like this:

> ~~It shall be ensured in thet~~ ~~The selection of~~ When selecting the Data Protection Officer, the Management Board shall ensure that there is ~~a~~~~that~~ no conflict of ~~interest~~interests ~~may result from the performance of~~between his or her duty as Data Protection Officer ~~in that capacity~~ and ~~from~~ any other official duties he or she may have, in particular in relation ~~those relating~~ to the application of this Regulation.

- Art 41 para 4:

- How often can the DPO be reappointed? Why has the maximum term of eight years been removed?

- Instead of "Executive Board" this should read "Management Board".

- Article 42(1):

We were wondering if this paragraph needs a reference to article 41 of directive 2016/680, since that is the article that stipulates that Member States shall provide for one or more supervisory authorities.

- Art 45:

Although art 62 para 3 EUDPR establishes a European Data Protection Board in which the European Data Protection Supervisor and the national supervisory authorities meet, we are wondering whether it is wise to abolish the specialised Cooperation Board for Europol. Europol is a very specific kind of organisation that does a specific kind of work, and it is therefore important that the supervisory bodies develop and maintain expertise on the work of Europol to be able to carry out their supervisory tasks. If issues regarding Europol are discussed in the general meeting where all other organisations that are subject to the supervision of the EDPS are discussed, the specificities of Europol's work might get lost.

POLAND

On page 22 of doc. 5388/4/21 REV 4, Article 2

Regulation (EU) 2016/794 is amended as follows: (1) Article 2 is amended as follows: (a) points (h) to (k) and points (m), (n) and (o) are deleted;	*Comment:* PL suggest to consider adding some explicit indication, either in the preamble or in art. 2, that the **definitions of terms: personal data, data subject, genetic data, processing, transfer, data subject's consent etc. stipulated in art. 3 of Regulation 2018/1725 apply to processing of data by Europol.** It is also worth to examine the possiblity of including the definition and difference between transfer and trasmission of personal data, which are very often used in this Regulation in different contexts.

On page 28 of doc. 5388/4/21 REV 4, Article 18

"6. Europol may temporarily process data for the purpose of determining whether such data are relevant to its tasks and, if so, for which of the purposes referred to in paragraph 2. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data, in particular with respect to access to and use of the data, as well as time limits for the storage and deletion of the data, which may not exceed six months, having due regard to the principles referred to in **Regulation (EU) 2018/1725**~~Article 28~~."	*Comment:* Proposed addendum : ... principles referred to in **Article 71** of Regulation (EU) 2018/1725.

On page 32 of doc. 5388/4/21 REV 4, Article 24

"Article 24 **Transmission of operational personal data to Union institutions, bodies, offices and agencies**	Comment: Having concerned the new art. 24 in Section 2, PL suggest to change to name of the whole section as follows : Transmission, transfer and exchange of personal data.

On page 39 of doc. 5388/4/21 REV 4, Article 27a

"Article 27a **Processing of personal data by Europol**	*Comment:* Bearing in mind the scope of the new art. 27a and its general and horizontal impact, We suggest to change the chapter in which it is included. Chaepter VI, which already include data protection safeguards, seem to be more appropriate.

On page 46 of doc. 5388/4/21 REV 4, Article 39

"1. Without prejudice to Article 90 of Regulation (EU) 2018/1725, any new type of processing operations to be carried out shall be subject to prior consultation of the EDPS where special categories of data as referred to in Article 30(2) of this Regulation are to be processed."; 	*Comment:* In line with the discussion during the last LEWP VTC, PL is of the opinion that this should not apply to specific individual operational activities, such as operational analysis projects, thus interpreted in line with the recital 50 of Regulation 2016/794

ROMANIA

ROMANIAN WRITTEN COMMENTS

-FOLLOW-UP LEWP on 26 April 2021 -

9. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

9.1 Initial examination of thematic block 8: strengthening the data protection framework applicable to Europol

A new Recital referring to Directive (EU) 2016/680 should be added due to the fact that some provisions used in the proposal for Europol Regulation are already stipulated in the above mentioned Directive (such as those from Chapter V- Transfer of personal data to third countries or international organizations). Moreover, some terms used in the proposal for Europol Regulation are already defined in Directive (EU) 2016/680 (for example "personal data", "biometric data", "personal data breach", "genetic data", etc.).

Article 1(1). We consider it necessary **to maintain the letters h) -k) and m) -o) from art. 2** of Regulation (EU) 2016/794, respectively **the definition of the terms used in the field of data protection** "personal data", "data subject", "genetic data", "processing", "transfer of personal data", "personal data breach"," the data subject's consent". **A simplified version of the definitions could be a reference to the definitions in art. 3 of Regulation (EU) 2018/1725**, for example "personal data 'means personal data as defined in point 1 of Article 4 of Regulation (EU) 2018/1725".

Article 1(1). We consider it necessary **to add this provision by inserting point (d)** concerning the definition of the term "biometric data", as follows: "(d) **the following point (r) is added:**

„(r) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" .

Article 1 (10) / Article 24 para. (3). In order to comply with the purpose limitation principle, **we propose to add this provision as follows:** 'The recipient Union institution, body, office or agency shall process the operational personnel data only for the purposes for which they were transmitted and shall not further transmit the operational personal data to other Union institution, body office or agency . "

Art 1 (16) (3) / Art. 30 para. (3) first sentence. **A confirmation from the Commission would be welcomed that the intention was to regulate the exceptional cases, as well, in which the other MSs selected by Europol will have direct access to the information.**

Article 1 (20) / Art. 34. We consider it necessary **to keep the mention regarding EDPS**, taking into account the obligation established by Art. 34 of Regulation (EU) 2018/1725.

Art. 1 (22) / Art. 36. **We do not agree with the deletion of paragraph 1) from Art. 36 of Regulation (EU) 2018/794 as that provision define the right of access of the data subject.**

Art. 1 (34) / Art. 45. We consider that it is necessary to request clarifications regarding the deletion of Art. 45 of Regulation (EU) 2016/794 which regulates the establishment of the Cooperation Board composed of a representative of the national supervisory authority of each Member State and a representative of the EDPS. Thus, **we request further clarifications on the consequences of the deletion of this article, respectively what shall be the form of cooperation between the EDPS and the supervisory authorities, as the establishment of the Cooperation Board set up by this provision will no longer be regulated**.

Furthermore, we believe that the functional tasks and responsibilities of the data protection officer should be detailed in the proposed Regulation, in order to strengthen its position, given the central role it plays in the current practice of personal data protection legislation.

In addition

Art 25. We sustain the entering of the paragraph 4a. We underline that adequate safeguards are necessary to be detailed on 4a. a).

Art. 26 paragraph 5. We agree the deletion of the final sentence from the letter a). Also, we sustain the new paragraph 11 from point d).

We sustain the entering of the Art 33a *processing of personal data for research and innovation.* We underline that technical security measures are necessary to be detailed on point b).

We sustain art 33a point 2.

SLOVENIA

As regards the revision of the Europol Regulation, please be informed that at the moment Slovenia don't have additional comments on: on thematic bloc 6: strengthening Europol's cooperation with the EPPO and on thematic bloc 8: strengthening the data protection framework applicable to Europol.

SPAIN

Follow-up comments to the last LEWP meeting (26/04/2021)

AS REGARDS THE REVISION OF THE EUROPOL REGULATION, SPAIN PROVIDES THE FOLLOWING MODIFICATIONS

ON THEMATIC BLOCK 8: : STRENGTHENING THE DATA PROTECTION FRAMEWORK APPLICABLE TO EUROPOL

Article 28: Regarding this article, it is considered that data protection principles should be included in this block to ensure the quality of data protection.

Article 30.2: With regard to Article 30 paragraph 2, it is considered appropriate to clarify what kind of criteria would be used to consider these data as strictly necessary and proportionate.

8. COMMENTS RECEIVED AFTER THE MEETING ON 7 MAY 2021 (BLOCKS 1, 2, 3, 5 AND 6)

AUSTRIA

Further to the videoconference of the LEWP on 7 May 2021, item: recast of the Europol Regulation, Austria has the pleasure to communicate to you its comments (attached) concerning the **thematic bloc 1.**

We have sent our concern on Article 26, para 6b in written on 04.05.2021.

Thank you, Presidency for having given us the opportunity to reiterate our request concerning Article 26, para 6b during the meeting of 07.05.2021.

The Commission explained that Article 26/6b is the legal basis for Europol (and not for the Member States) on what Europol can do and therefore it is enough to have the sentence

> "*Where Member States use the Europol infrastructure for exchanges of personal data with private parties on crimes falling within the scope of the objectives of Europol, they may grant Europol access to such exchanges or not* "

in Recital 34.

This explanation does not convince us. Europol's access to these exchanges is dependent on the authorisation of Member States. Therefore, this should be enshrined in the legal text.

We propose the following wording of para 6b

> 6b. Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws. In cases where Member States use this infrastructure for exchanges of personal data on crimes falling within the scope of Europols objectives, they may grant Europol access, outside the scope of the objectives of Europol, Europol shall not have access to that data.

For recital 34 we propose a minor change in the wording.

The last part of the third sentence should read „they may grant Europol access to such exchanges ".

The words „or not "at the end of the sentence seem to be redundant.

BELGIUM

Written comments of Belgium related to the revision of the Europol mandate

BLOCK 1 – Europol's cooperation with private parties

We look favorable at the suggestion and reasoning of Finland on page 284 of doc. 5527/7/21 related to Europol sending personal data to private parties. Thus we would welcome the following phrase in Article 26: *"Transmissions or transfers referred to in paragraphs 5 and 6 shall not be systematic, massive or structural"*.

BLOCK 3 – Europol's role in research and innovation

Belgium notes the newly proposed paragraph 4 of Article 33a. We cannot agree to its current formulation. We cannot support a general approval of using all data provided to Europol by Belgium in the past for research and innovation purposes. We want to stress that we never intended to prevent the possibility for Member States' personal data to be used by Europol for research and innovation purposes. Belgium does however strongly believes that **there should remain a possibility for Member States to forbid Europol to use certain personal operational data for the development of innovative tools**. Certain data and certain cases might indeed be too sensitive. We also confirm the reasoning of the Netherlands that the current formulation does not abide by the ownership principle and risks to undermine the trust of police authorities in information exchange with Europol.

By preference we thus wish to delete Article 33a(4): ***~~"4. Where the requirements of paragraph 1 are fulfilled, and by way of derogation from Article 19(1), Europol may process personal data that has been processed for the purposes referred to in points (a) to (d) of Article 18(2) also for the purpose of Article 18(2)(e)."~~***

- A first consequence of the Commission's proposal without this Article 33a(4) would concern past data. Also past data would be subject to the newly introduced possibility of being given the processing purpose of research and innovation. In practice, the deletion of this paragraph will thus still entail the possibility of using past data for research and innovation purposes. Europol would however – upon entering into force of the Regulation – need to ask all the Member States whether they approve of past data having an additional processing purpose. Any Member States willing to give permission can then give either a general authorization to Europol to use past data for research and innovation purposes, or a general authorization with the exception of certain data, or even only an authorization for certain data.

- A second consequence of the Commission's proposal without this Article 33a(4) would concern future data. Any future data sent to Europol could be given the (additional or even only) purpose of research and innovation. We consider it a good way forward to create guidelines on this matter, as developed for example by the Management Board based on Article 18(7) – namely the Integrated Data Management Guidelines.

As a compromise and if the legislator insists on clarifying this way of working in the Regulation, we propose a recital clarifying that past data may also be given the additional purpose of research

and innovation. An even further step would be to include it in the operational text, where one then could consider the following amendment of the currently proposed Article 33a(4), replacing the allowed derogation from Article 19(1) with the condition that the provider of the information gives its authorization according to Article 19(1). Paragraph 4 of Article 33a would then read:
"4. Where the requirements of paragraph 1 are fulfilled, and ***if the provider of the information has given its authorisation according to*** ~~***by way of derogation from***~~ *Article 19(1), Europol may process personal data that has been processed for the purposes referred to in points (a) to (d) of Article 18(2) also for the purpose of Article 18(2)(e)."* This formulation could still mean that – without much workload – a Member State could give a general authorization applicable to all past data and even all future data.

In conclusion, we do not believe the legislator should in such a general way determine the fate of all data provided to Europol. This would not take sufficiently into account the sensitivity of certain data and certain cases. Deletion of Article 33a(4) would still enable most data – if so desired by the Member States – being used for research and innovation purposes, but without circumventing the ownership principle and while respecting the sensitivity of certain data and certain cases.

We look forward to discussing the above as well as other proposals that ensure a good balance between the ownership principle and the sensitivity of certain information and cases on the one hand, and the necessity in certain cases to make use of personal data for research and innovation purposes.

BLOCK 5 – Europol's cooperation with third countries

We want to reiterate certain elements of our previous written comments in relation to Article 25(4a).

First of all, we appreciate the addition of informing the EDPS in art. 25(8) about transfers based on the self-assessment by Europol. We believe this alignment with the Eurojust Regulation helps to prevent misunderstandings and accommodates possible concerns about oversight.

Secondly, we still consider it **useful for Europol to be able to conclude administrative arrangements with the third country after a positive self-assessment**. Administrative arrangements will help streamline this additional structural way of working with the concerned third countries. Also, we think that **the Management Board should be informed about transfers of personal data following a positive self-assessment**. This goes in the same lines of the French proposal indicating better oversight by the Management Board for Article 25(4a. In the current text there is no involvement of the Management Board at all, while Article 25(4a) does concern a structural way of working with third countries. These two elements (drawing up administrative arrangements and reporting to the Management Board) currently exist for adequacy decisions. We do not see why these two elements would not be appropriate for self-assessment under Article 25(4a).

Belgium thus proposes the following amendments to Article 25:

- The last sentence of Article 25(1) should read: "*Europol may conclude administrative arrangements to implement such agreements* ***, or*** ~~*–*~~ *adequacy decisions* ***or assessments of appropriate safeguards***."

- Article 25(2) should read: "*The Executive Director shall inform the Management Board about exchanges of personal data on the basis of adequacy decisions* ***or assessments of appropriate safeguards*** *pursuant to point (a) of paragraph 1.*"

We would appreciate further clarification on the reason(s) not to include these proposed changes.

Thirdly, we would like to express our support for the Czech comment on page 335 of doc. 5527/7/21 related to the ownership principle in Europol's cooperation with the EPPO. We would welcome the following clarifying amendment to recital 22: *"The rules on the* ***restrictions of processing and*** *transmission to Union bodies set out in this Regulation should apply to Europol's cooperation with the EPPO."*

OTHER

We support the Italian text proposal and reasoning on page 309 of doc. 5527/7/21 related to underlining the importance of focusing on structured mafia-type organizations. This would indeed be in line with reality as well as with the policy documents. Thus we consider it beneficial to include the reference to these structured mafia-type organizations in recitals 3 and 6.

CZECH REPUBLIC

CZ comments on Europol recast

(relative to wk 757/2021 rev 5)

Bloc 1

Art. 4(1)(m)

The current wording would imply, contrary to EU and national instruments, that Czech cyber-defence (or cyber security) authorities may be coordinated by Europol. It must be taken into account that there are other channels for coordination of responses to cyber incidents/attacks including large scale attacks, in particular CSIRTs' Network and CyCLONe Platform. The situation is not helped by broad definition of "competent authorities" in the Article 2(a) of the Europol Regulation. We understand that BG wishes to keep the term „competent authorities". Given the explanations of the Commission that the coordination is meant as a support, we propose to:

*a) change the „*coordination of*" to „***support of***" or „***assistance to***",*

with "support" being our most preferred option. Alternatively, we propose to:

*b) change the „*cyberattacks*" to „***cyber crime***", and/or*

*c) change the „*response*" to „***prevention, investigation and prosecution***" (that would correspond to recital 5).*

Art. 51(3(f)

We believe that the text in the second subparagraph is a copy mistake and should be deleted.

Bloc 3

Art. 33a(4)

CZ needs a mechanism for governance of this new purpose of processing to ensure data ownership principle. CZ does not wish to propose further systemic safeguards, but notes that current wording undermines the confidence of investigators in practice. While CZ prefers opt-ins to opt-outs, such governance should in any case be easily practicable and enable simple and generalized decisions by Member States or law enforcement agencies, rather than require case-by-case or data-by-data decisions.

Bloc 6

Art. 20a(4)

CZ believes that coordination of all involved authorities and EU bodies would be improved if Europol informed relevant Member State(s) at the same time:

4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence **in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939; it shall inform all national units concerned at the same time.**

At the meeting, the Commission appeared to indicate that data owner would be informed or requested to permit transfer. In such a case, we support NL suggestion to refer to Art. 19(2), so that one crime is not reported to EPPO twice (by law enforcement authorities and by Europol).

(end of file)

FRANCE

NOTE DE COMMENTAIRES DES AUTORITÉS FRANÇAISES

Les autorités françaises prient la présidence de bien vouloir trouver ci-après leurs commentaires écrits concernant les blocs thématiques numéro 1, 2, 3, 5, 6, à la suite de la réunion LEWP du 7 mai 2021 :

- **Commentaires généraux concernant la révision du règlement Europol :**

Les autorités françaises accueillent favorablement les propositions de la Commission qui, en adaptant le règlement Europol aux exigences du règlement du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union (règlement 1725) propose des mécanismes constructifs au service de l'agence.

Toutefois, une lecture attentive, article par article, est indispensable pour adapter ce règlement aux exigences opérationnelles de l'agence Europol. Les autorités françaises regrettent notamment la suppression de nombreuses définitions du règlement actuel.

Concernant le bloc thématique n°1 (Permettre à Europol de coopérer efficacement avec des parties privées)

Les autorités françaises font part des commentaires détaillés suivants :

Proposition de la Commission	Commentaires des autorités françaises
Considérant nouveau	En lien avec leur proposition ci-dessous, les autorités françaises proposent la rédaction du considérant suivant : ***In order to ensure Europol's effectiveness as a hub for information exchange, clear obligations should be laid down requiring Private parties to provide Europol with the data necessary for it to fulfil its objectives.*** ***Europol should increase the level of its support to Member States, so as to enhance mutual cooperation and the sharing of information.*** ***Given the nature of the new tasks of Europol regarding private parties, the Management Board should be given the necessary information regarding the data exchanged between Europol and Private Parties. Europol should submit an annual report to the Management Board on the***

	information provided by Private parties".
Article 26 (11) (ex 7.12 NL BE) *11. Europol shall draw up an annual report to the Management Board about the number of cases in which Europol issued follow-up requests to private parties or own initiative requests to Member States of establishment for the transmission of personal data in accordance with Article 26 and Article 26a, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks. The annual report shall be drawn up on the basis of the quantitative and qualitative evaluation criteria defined by the Management Board and shall be sent to the European Parliament, the Council, the Commission and national parliaments.*	Les autorités françaises accueillent favorablement cette proposition. Toutefois, pour la bonne information des Etats membres et la bonne conduite des échanges entre Europol et les parties privées elles proposent de compléter cette proposition d'article comme suit : *Europol shall draw up an annual report to the Management Board* ***including the number of personal data received and exchanged with private parties****, number of cases in which Europol issued follow-up requests to private parties or own initiative requests to Member States of establishment for the transmission of personal data in accordance with Article 26 and Article 26a, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks.* *The annual report shall be drawn up on the basis of the quantitative and qualitative evaluation criteria defined by the Management Board and shall be sent to the European Parliament, the Council, the Commission and national parliaments.* Toutefois, comme proposé par la Commission lors du LEWP du 12 avril 2021, et sous réserve de l'approbation de la Présidence, les autorités françaises pourraient également soutenir l'ancienne version du texte – article 7 (11).

Propositions d'articles :

Les autorités françaises renouvellent leurs propositions d'articles qu'elles souhaitent présenter plus en détail : ainsi, afin de garantir la totale transparence de l'activité d'Europol avec les parties privées et renforcer le rôle des États-membres, les autorités françaises proposent à nouveau un mécanisme pérenne permettant aux États-membres de prendre connaissance et de valider tous les protocoles d'entente (*Memorandum of understanding - MoU*) que l'agence signe avec les partenaires privées, les autorités françaises soumettent à la Présidence les propositions d'article suivante :

- **Article 11 (v) Échanges de données à caractère personnel avec les parties privées (nouveau) :**

Version FR : *« adopte des lignes directrices sur la réception et l'échange de données entre Europol et les parties privées ».*

Version EN : " *adopt guidelines on the receipt and exchange of data between Europol and private parties* ».

Argumentaire : Les autorités françaises précisent que ces lignes directrices n'interfèreraient pas avec les capacités de l'agence d'échanger des données personnelles avec les parties privées telles que prévues par les futures dispositions de ce Règlement. Il s'agirait pour les États membres d'impulser une dynamique dans un champ d'action nouveau pour l'agence en réfléchissant collectivement aux conditions et à l'application opérationnelle de ces échanges (quelles informations peuvent être envoyées par les parties privées (article 26 paragraphe 2a notamment), quelles infrastructures de communication (article 26 paragraphe 6b)…).

Cela serait plus cohérent avec les conclusions du conseil du 2 décembre 2019 qui mentionne que « *tout régime régissant la transmission directe de données à Europol par des parties privées devrait être fondé sur une procédure de consentement des États membres qui pourrait prendre la forme d'une liste proposée par Europol, constituée des parties privées de la part desquelles Europol aurait besoin de recevoir des données à caractère personnel. Cette liste ferait régulièrement l'objet de décisions prises par le conseil d'administration d'Europol, qui représente les autorités nationales* ».

- **Article 26 ter échange de données à caractère personnel avec les parties privées (nouveau) :**

Version FR : *« sans préjudice des articles 26 et 26a du présent règlement et après validation du Conseil d'administration, Europol peut conclure des protocoles d'entente avec les parties privées. Ces protocoles n'autorisent pas l'échange de données à caractère personnel et ne lient ni l'Union ni ses États membres*

Europol communique systématiquement aux États membres l'ensemble des protocoles d'ententes conclus avec les parties privées, pour information et validation par le Conseil d'administration ».

Version EN : " *Without prejudice to articles 26 and 26a and after the agreement of the Management Board, Europol may conclude memoranda of understanding with private parties. Such memoranda shall not authorise the exchange of personal data and shall not be binding on the Union or its Member States.*

Europol shall systematically communicate to the Member States all memoranda of understanding concluded with private parties for information and validation by the Management Board ".

Argumentaire : Les autorités françaises précisent que la communication aux Etats membres des protocoles d'entente ne vise pas à empêcher Europol d'échanger des données personnelles avec les parties privées mais simplement à les informer des protocoles que l'agence peut éventuellement conclure avec les parties privées, dont certains sont classifiés.

La France a déjà demandé la communication des protocoles qui restent à ce jour sans suite. Ainsi, la France souhaite seulement disposer de ces **protocoles pour information** et sans interférer avec les possibilités d'échange de données entre l'agence et les parties privées.

- **Article 11 (r) Fonctions du Conseil d'administration (amendement) :**

Version FR : *« r) Autorise la conclusion d'arrangements de travail, d'arrangements administratifs et* ***de protocoles d'entente avec les parties privées*** *conformément à l'article 23 paragraphe 4 e, à l'article 25, paragraphe 1 et l'article 26 ter ».*

Version EN: " r) *Decide upon working arrangements, administrative arrangements and memoranda of understanding with private parties in accordance with Article 23, paragraphs Article 25, paragraph 1 and article 26b".*

Concernant le bloc thématique n°2 (Permettre à Europol de traiter des ensembles de données complexes) :

Les autorités françaises font part des commentaires détaillés suivants :

Proposition de la Commission	Commentaires des autorités françaises
article 2 (q) Definitions *(q) 'investigative case file' means a dataset or multiple datasets that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation related to one or more Member States, in accordance with procedural requirements and safeguards under the applicable Union law or national criminal law, and submitted to Europol in support of that criminal investigation.*	Lors du dernier LEWP, la Suède a rappelé qu'Europol intervient en soutien des États membres lorsque deux ou plusieurs États sont impliqués (article 3 règlement Europol). À ce titre, la Suède a fait remarquer que les dossiers d'enquête (*investigative case files*) devaient eux aussi concerner deux ou plusieurs États membres. La France estime pertinente la remarque de la délégation suédoise. En conséquence, elle propose d'amender la définition des dossiers d'enquête en ce sens : *'investigative case file' means a dataset or multiple datasets that **two or more** Member State**s**, the EPPO or a third country acquired in the context of an on-going criminal investigation, in accordance with procedural requirements and safeguards under the applicable Union law or national criminal law, and submitted to Europol in support of that criminal investigation*
Article 1(6) – article 18a information processing in support of a criminal investigation *1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where: (a) a Member State or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2), **or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2)**; and (b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded.* *2. Europol may process personal data contained in an investigative case **file in accordance with Article 18(2)** for as long as it supports the on-going specific criminal investigation for which the investigative case file was*	En conséquence de ce qui précède, les autorités françaises proposent les modifications suivantes de cet article : ***Article 1(6) – article 18a information processing in support of a criminal investigation*** *1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where: (a) **two or more** Member States or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2), or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2); and (b) Europol assesses that it is not possible to carry out the operational analysis of the investigative case file without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded.* *2. Europol may process personal data contained in an*

Proposition de la Commission	Commentaires des autorités françaises
*provided by a Member State or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided. 3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State. That Member State**, or, with its agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation,** may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the **sole** purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a related criminal investigation are on-going in **that** other Member State. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Such personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.* *4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third* *country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of* *Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements*	*investigative case* file in accordance with Article 18(2*) for as long as it supports the on-going specific criminal investigation for which the investigative case file was provided by Member States or the EPPO in accordance with paragraph 1, and only for the purpose of supporting that investigation.* *The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Without prejudice to the processing of personal data under Article 18(5a), personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data and may only be accessed where necessary for the support of the specific criminal investigation for which they were provided.* *3. Upon request of all the Member States or the EPPO that provided the investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to that criminal investigation are on-going in one of these Member States.* *These Member States, or, with their agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation, may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the **sole** purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as judicial proceedings following a related criminal investigation are on-going in **that** other Member State. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data. Such personal data shall be functionally separated from other data and may only be accessed where necessary for the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process.* *4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third* *country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis*

Proposition de la Commission	Commentaires des autorités françaises
indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union.	*that supports the specific criminal investigation in a Member State or in Member States that Europol supports. Where a third country provides an investigative case file to Europol, the EDPS shall be informed. Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights. Where Europol, reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union.* *5. The Management Board adopt guideline further specifying the procedure for the implementation of the article.*

S'agissant du bloc thématique 3 (Renforcer le rôle d'Europol dans la recherche et l'innovation)

Les autorités françaises soutiennent *la proposition en vertu de laquelle Europol pourrait utiliser, pour la recherche et l'innovation, les informations passées et à venir qu'il reçoit pour quelque motif que ce soit (sauf exception expresse)*, *même lorsqu'il n'a pas été mentionné par un Etat membre qu'il autorisait l'utilisation de ces informations spécifiquement pour la recherche et l'innovation. En effet, l'Union européenne a la chance de pouvoir traiter de grands ensembles de données et ce traitement est une condition sine qua non au développement de nouveaux outils technologiques pertinents, notamment liés à l'utilisation de l'intelligence artificielle.*

Par ailleurs, les autorités françaises font part des commentaires détaillés suivants :

Considérant 40 ***Providing Europol with additional tools and capabilities requires reinforcing the democratic oversight and accountability of Europol. Joint parliamentary scrutiny constitutes an important element of political monitoring of Europol's activities. To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group with annual information on the use of these tools and capabilities and the result thereof.***	Afin de suivre et d'enrichir les travaux de l'agence, cette information annuelle doit être communiquée aux États membres. Les autorités françaises proposent de modifier le considérant comme suit : « *To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group* ***and the Member States*** *with annual information on its use of these tools and capabilities and the result thereof* ».

S'agissant du bloc thématique 5 (Renforcer la coopération d'Europol avec les pays tiers)

Les autorités françaises font part des commentaires détaillés suivants :

Considérant 24 *Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation*	Les autorités françaises estiment qu'il convient de modifier le considérant 24 en fonction de la modification de l'article 25 telle que présentée par la présidence portugaise. Les autorités françaises précisent que cette proposition de rédaction s'inspire largement des considérants du règlement Eurojust (voir considérant 51 du règlement Eurojust). Soit la proposition de rédaction suivante ***:*** ***Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation.*** ***Transfers not based on an adequacy decision or international agreement concludes by the EU should be allowed by the Management Board only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where Europol, after authorization of the Management Board, has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist.*** ***Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which***

	could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. Europol should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, Europol should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, Europol should be able to require additional safeguards.
Article 1(11)(a)- Article 25(5)- Transfer of personal data to third countries and international organisations *Subject to any possible restrictions pursuant to Article 19(2) or (3) and without prejudice to Article 67, Europol may transfer personal data to an authority of a third country or to an international organisation, insofar as such transfer is necessary for the performance of Europol's tasks, on the basis of one of the following (a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision')* ***or in the absence of such a decision, appropriate safeguards have been provided for or exist in accordance with paragraph 4a of this Article, or in the absence of both an adequacy decision and of such appropriate safeguards, a derogation applies pursuant to paragraph 5 or 6 of this Article****; (b) an international agreement concluded between the Union and that third country or international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals;* *(c) a cooperation agreement allowing for the exchange of personal data concluded, before 1 May 2017, between Europol and that third country or international organisation in*	**Les autorités françaises remercient vivement la présidence portugaise pour la prise en compte des commentaires des délégations et d'Europol sur le régime d'autres agences JAI en matière de coopération avec les États tiers.** **Toutefois, elles précisent que cette modification du cadre d'échange avec les États tiers doit absolument s'accompagner d'un renforcement du contrôle du Conseil d'administration.** **Ainsi, il conviendrait que le CAE non seulement décide des arrangements de travail et des arrangements administratifs conclu par l'agence (article 11r) mais également qu'il puisse autoriser Europol à échanger des données personnelles au terme du paragraphe 4a de l'article 25 tel que proposé par la présidence.** **Les autorités françaises proposent donc un amendement à l'article 25.4.a (voir plus haut sur le CAE).**

accordance with Article 23 of Decision 2009/371/JHA. Europol may conclude administrative arrangements to implement such agreements or adequacy decisions. 2. The Executive Director shall inform the Management Board about exchanges of personal data on the basis of adequacy decisions pursuant to point (a) of paragraph 1. *3. Europol shall publish on its website and keep up to date a list of adequacy decisions, agreements, administrative arrangements and other instruments relating to the transfer of personal data in accordance with paragraph 1.* *4. By 14 June 2021, the Commission shall assess the provisions contained in the cooperation agreements referred to in point (c) of paragraph 1, in particular those concerning data protection. The Commission shall inform the European Parliament and the Council about the outcome of that assessment, and may, if appropriate, submit to the Council a recommendation for a decision authorising the opening of negotiations for the conclusion of international agreements referred to in point (b) of paragraph (1).* ***4a. In the absence of an adequacy decision, Europol may transfer operational personal data to a third country or an international organisation where:*** ***(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or (b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data.*** *5. By way of derogation from paragraph 1, the Executive Director may authorise the transfer or a category of transfers of personal data to third countries or international organisations on a case-by-case basis if the transfer is: (a) necessary in order to protect the vital interests of the data subject or of another person;* *(b) necessary to safeguard legitimate interests of the data subject where the law of the Member*	

State transferring the personal data so provides; *(c) essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country;* *(d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions; or* *(e) necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal sanction. Personal data shall not be transferred if the Executive Director determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer referred to in points (d) and (e). Derogations may not be applicable to systematic, massive or structural transfers.* *6. By way of derogation from paragraph 1, the Management Board may, in agreement with the EDPS, authorise for a period not exceeding one year, which shall be renewable, a set of transfers in accordance with points (a) to (e) of paragraph 5, taking into account the existence of adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. Such authorisation shall be duly justified and documented.* *7. The Executive Director shall as soon as possible inform the Management Board and the EDPS of the cases in which paragraph 5 has been applied.* *8. Where a transfer is based on paragraph **4 a or** 5, such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred.*	

Propositions d'articles :

Les autorités françaises se félicitent du bon déroulement des discussions sur ce point et de l'amendement apporté par la Présidence à la proposition de la Commission.

Toutefois et afin d'assurer à l'agence une plus grande efficacité opérationnelle et stratégique, elles proposent les amendements suivants :

- **Article 7 (13) Fonctions du Conseil d'administration (nouveau) :**

Version FR :« *Europol rédige un rapport annuel portant sur la nature et le volume des données personnelles fournies à Europol et échangées avec les États tiers sur la base des critères d'évaluation quantitatifs et qualitatifs fixés par le CAE. Ce rapport annuel est transmis au parlements nationaux, au Parlement européen, au Conseil, et à la commission* ».

Version EN : " *Europol shall draw up an annual report to the Management Board on the personal data received and exchange with third countries on the basis of quantitative and qualitative evaluation criteria defined by the Management Board. The annual report shall be sent to the national parliaments, the European Parliament, the Commission, the Council and the Commission*."

- **Amendement de la proposition de la présidence (article 25.4a)**

[…]

4a. In the absence of an adequacy decision, Europol may, ***after authorization of the Management Board****, transfer operational personal data to a third country or an international organisation where:*

(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or

(b) Europol has assessed all the circumstances surrounding the transfer of operational personal data and has concluded that appropriate safeguards exist with regard to the protection of operational personal data.

S'agissant du bloc thématique 6 (Renforcer la coopération d'Europol avec le Parquet européen)

Les autorités françaises ne s'opposent pas à l'accès du Parquet européen en mode concordance / non-concordance (hit / no-hit) aux bases de données d'Europol, tel que proposé par la Commission au paragraphe n°3 de l'article 20 a) du projet de Règlement.

En effet, le mécanisme proposé n'est pas juridiquement incompatible avec le règlement Parquet européen et respecte le principe de la propriété des données insérées dans les bases d'Europol.

Par ailleurs, les autorités françaises s'interrogent sur la mise en œuvre du paragraphe 4[1] et sollicitent tout éclairage que la Commission pourra apporter sur ce point afin notamment de préciser les conséquences de l'absence de signalement par Europol d'une conduite criminelle pour laquelle le Parquet européen s'estime compétent.

[1] *Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939"*

GERMANY

Germany's follow-up comments to the LEWP meeting on 7 May 2021: Revision of the Europol Regulation – Thematic blocs 1, 2, 3, 5 and 6

Please find below Germany's written comments on the fifth revised version of the text of the Commission proposal (changes to the provisions pertaining to thematic blocs 1, 2, 3, 5 and 6). Further comments may be raised following ongoing scrutiny of the proposal.

On a general note, we would like to reiterate our previous comments in expressing that Europol should continuously be present in the meetings. In our view, delegations would benefit from being able to seek Europol's expertise and advice in the ongoing discussions. Against the background that Europol is also continuously invited at Ministerial Council level, we do not see any reasons why the participation of an agency should not be possible nor any legal obstacles. We are confident that the legal framework allows for a satisfactory solution in the best interests of the Member States while taking due account of the concerns expressed by the Council Legal Service.

Thematic bloc 1: cooperation with private parties

Article 4(1)(m):

As stated before, the exact role of Europol with respect to the new TCO Regulation remains to be determined.

Therefore, Germany suggests to refer explicitly to the coordination of removal orders for terrorist content online by Member States authorities in accordance with Art. 14 of Regulation 2021/… [the TCO-Regulation], as this provision defines the supporting role of Europol regarding the taking down of terrorist content online.

Thus, Art. 4(1)(m) would read as follows:

> *"support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States and upon their request, the coordination of competent authorities' response to cyberattacks,* ***the coordination of removal orders for terrorist content online by Member States authorities in accordance with Art. 14 of Regulation 2021/… [the TCO-Regulation]*** *and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions.*

This amendment should be mirrored in the last sentence of recital 35 as follows:

> *Nothing in this Regulation should be understood as precluding the Member States* ***and Europol*** *from using removal orders as laid down in Regulation 2021/... on addressing the dissemination of terrorist content online as an instrument to address terrorist content online* ***or making use of the coordinative and cooperative role of Europol in accordance with Art. 14 of the Regulation 2021/…, when member states issue such a removal order***."

Moreover, the meaning of "cyberattacks" needs to be explained as this term is only used in this Article of the Europol Regulation without giving a definition. Is there a suitable definition of this term in Union law that the provision could refer to?

Article 4(1)(u):

Germany does not object to the amendments to the previous version, but would still appreciate an explanation as to what the exact action by Europol to support Member States will be, inter alia vis-à-vis Article 4(1)(m). Especially, in our view it remains unclear which information could be provided to which private parties with the aim of identifying relevant online content (as the referral of terrorist internet content to the online service providers concerned is already covered by Article 4(1)(m)).

Article 26(6a) and Recital 31:

Germany welcomes the amendments to Article 26(6a) and to the corresponding Recital 31. Nevertheless, it should be specified more clearly that there is no legal obligation for the Member States and for the private parties concerned to comply with requests made by Europol. While Member States, pursuant to Article 7(6)(a), shall supply Europol with the information necessary for it to fulfil its objectives, this provision does not imply any obligation for Member States to obtain information from private parties. Above all, Article 7(6)(a) does not imply such an obligation for private parties. Therefore, the following sentence should be added to the provision (or at least the corresponding Recital):

> *"This Article does not oblige neither Member States nor private parties to comply with a request made by Europol."*

Article 26a:

As a general observation, it still remains unclear what the supporting task of Europol would be, including the relationship to the current tasks under Article 4(1)(m). The provision would also raise various issues about its exact scope. Should electronic evidence fall under it, this may have undesirable implications vis-à-vis the draft TCO Regulation and harbor contradictions to the E-Evidence dossier.

Recital 32:

The first sentence in Recital 32 as proposed by the Presidency needs to reflect the different ways of receiving data from private parties. Therefore, the text should be amended as follows:

> *"To ensure that Europol does not keep the data* ~~***received directly***~~ ***obtained*** *from private parties* ***directly or via the Member States*** *longer than necessary …"*

Thematic bloc 2: enabling Europol to process large and complex datasets

Article 2(q):

The definition of "investigative case file" establishes various criteria to be satisfied by Member States, the EPPO or third countries (e.g. *"... is authorised to process..." or "...in accordance with procedural requirements and safeguards under applicable ... law"*). As a result of the diverse legal regimes among Member States, Europol will not be in a position to verify in detail whether these criteria have been met. For the sake of legal certainty, the definition should therefore clarify that the obligation to meet these criteria lies on the aforementioned while Europol is not obliged to re-verify whether these criteria have been met.

Article 18(5):

Why was Article 18(2)(e) excluded from the scope of Article 18(5)? Article 18 establishes the regulatory model that the categories of personal data that may be processed for the purposes laid down in Article 18(2) are specified in Annex II. If differences between the purposes arise, these disparities are also addressed in Annex II, as the Annex distinguishes between different purposes of Article 18(2). Why does the proposal not follow this regulatory model, when it comes to research and innovation activities?

Article 18(5a)

The second sentence concerns the establishment of further conditions related to the processing under the first sentence. A similar provision can be found in the second sentence of paragraph 6, whereby the latter refers not only to "conditions relating to the processing of such data", but more specifically to "conditions relating to the processing of such data, in particular with respect to access and use of the data, as well as time limits for the storage and deletion of the data". Is there a reason why there is no complete alignment between these provisions

As the processing powers only serve the purpose of determining compliance with paragraph 5, why does the third sentence refer to "where necessary for the purpose of this Article"? This should rather read "…of this paragraph".

The fourth sentence sets out that in the event of deletion of the data, Europol shall inform the provider of the data accordingly. This obligation does not make sense in cases where Europol has retrieved the information from publicly accessible sources including the Internet pursuant to Article 17(2). Therefore, the obligation to inform the provider should expressly exclude Article 17(2) instead of referring to the "relevant" cases (as proposed by the Presidency in the current version).

We have noticed that while the new Article 18a stipulates that the data shall be functionally separated (cf. paragraph 2 third sentence and paragraph 3 third sentence), Article 18(5a) does not contain such requirement. From a data protection perspective, the separation of categorised and non-categorised data would presumably make sense and would certainly be welcomed by the EDPS in particular.

Article 18a(1):

Germany welcomes that the legislative proposal addresses this very important issue. As we all know, it has become urgent to address Europol's ability to process big data in accordance with relevant data protection principles since the EDPS' decision on the big data challenge. As the Ministers have expressed in their Declaration on the Future of Europol, it is of key importance to Member States that Europol will be able to continue to support Member States in this regard.

We support the fundamental approach of the proposal and generally agree with the provisions brought forward. At the same time, the processing of large and complex datasets (beyond the limitations of Art. 18(5) and Annex II) raises questions concerning data protection and fundamental rights and must strictly be limited to what is necessary and proportionate to achieve the objectives covered by Europol's mandate. Yet, the proposals of Article 18(5a) and Article 18a address part of the new operational reality. **In order to ensure that Europol can continue to fulfil its tasks to the benefit of national law enforcement authorities, it is important to clarify that the processing of data under Article 18(5a) and Article 18a – of course in full compliance with the strict data protection safeguards applicable – is as valid a possibility as the other processing purposes provided for in Article 18.**

Regarding point (b), it is not clear what the test behind *„that it is not possible"* entails. Does this mean technical impossibility? Would Europol have to arrange that the *„case file"* is processed in a way that categories of personal data that do not comply with the requirements of Article 18(5) are filtered out to the greatest extent possible? Will processing be permissible on a provisional basis then?

The new insertion in Article 18a(1)(a) proposed by the Presidency aims at opening the scope of this Article to the purposes referred to in Article 18(2)(a). This aim is in line with calls from our national law enforcement authorities for support in the area of preventing crime. However, the proposed amendment raises several questions that should be addressed:

- Apart from the new addition, the wording of the whole Article remains focused on "investigative case files" (which refer to datasets "that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation") and their "operational analysis" (which refers to Art. 18(2)(c)). Therefore, Germany proposes to revise the wording in order to better clarify which conditions would apply to the newly inserted option. *"Exceptional and duly justified cases"* alone is not an appropriate criterion.

- As EPPO is not competent for the prevention of crime, EPPO could at most request an additional analyses pursuant to Article 18(2)(a)(i). Nevertheless, Article 18a(1) concerns the general question of cooperation between Europol and EPPO. From our point of view, it does not make sense to deal with individual aspects of this topic outside the context of the underlying general issue. May we therefore suggest that all questions related to the EPPO be dealt with comprehensively in the context of thematic bloc 6.

Article 18a(4):

The part after *„with which ..."* could be aligned with the order used in Article 25(1).

The relationship of the third sentence (*"Europol shall verify .."*) and the fourth sentence (*"Where Europol ..."*) remains unclear. If the processing is already prohibited where preliminary indications of disproportionality or fundamental rights violations exist, the higher threshold in the former

sentence may be unnecessary. If this was the case, both sentences could be combined into one sentence along the requirements in what is now the latter sentence.

The last sentence should read *"... be processed by Europol where necessary **and proportionate**..."* (cf. above drafting proposal).

Thematic bloc 3: research and innovation

Article 18(2)(e):

Article 18(2) aims at realizing the principle of purpose limitation, according to which the purposes for the processing of personal data shall be specified. Could the provision indicate more specifically the purposes for which data may be processed in the context of research and innovation? For example, the text could stay closer to the Commission's proposal by amending the original wording as follows:

*"research and innovation regarding matters covered by this Regulation**, in particular** for the development, training, testing and validation of algorithms **and** for the development of **other** tools **relevant to achieve the objectives set out in Article 3**."*

Article 33a(4):

Germany welcomes that Article 33a(2) was moved to Recital 39. Besides, we would like to ask to delete the word "personal" as some of the categories mentioned are not "personal data".

Therefore, the sentence should be amended as follows:

> "*Preference should be given to using synthetic, pseudonymized and/or anonymized ~~personal~~ data.*"

Germany takes note of the clarifying amendment proposed in Article 33a(4). While we support the general idea of Article 33a, we would like to highlight that a solution must be found that preserves the interests of the provider of the information ("principle of data ownership"). The current proposal would jeopardize the confidence of national authorities in their ability to safeguard their interests as "data owners".

Thematic bloc 5: cooperation with third countries

Article 25(1), (4a) and corresponding Recitals:

Germany welcomes the revision of Article 25 in line with our previous comments. However, as we mentioned before, the amendment to Article 25 must be reflected accordingly in all other provisions that refer to the possibilities for structural exchanges of personal data with third countries foreseen by Article 25. This applies in particular to Articles 18a(4), 26(1)(c), 26(4), 26(6), 26a(2), 26a(4), 27(1)(c) and 27(2).

By way of example, Article 18a(4) should be amended as follows:

> *"Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of*

*Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision**, or in the absence of such a decision, where appropriate safeguards have been provided for or exist,** as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports."*

Furthermore, the revision of Article 25 must be reflected in the corresponding Recitals, in particular Recital 24. Inspiration could be sought from Recital 51 of the Eurojust Regulation. Germany will submit a proposal for wording.

Article 25(8):

Germany does not object to the current proposal of making available certain information to the EDPS. Nevertheless, Germany would appreciate an explanation why the former paragraph 8 was deleted.

Thematic bloc 6: strengthening Europol's cooperation with the EPPO

Germany welcomes the amendments proposed by the Presidency in Article 20a(2) as they address some of the concerns we raised in our previous written comments. Nonetheless, we would like to emphasize that the cooperation between Europol and the EPPO should be limited to the extent that is already foreseen by the EPPO Regulation, notably Article 102 thereof. We see no need to extend the cooperation beyond this. Thus, we would like to reiterate our previous comments insofar as they have not been addressed:

- Regarding the proposed wording in Article 20a(2) (*"... cooperate with it, in particular..."*), we would first like to highlight that the EPPO Regulation does not provide for further possibilities of cooperation between Europol and the EPPO beyond providing information and analytical support to a specific investigation conducted by the EPPO.

  In its non-paper on Article 20a, the Commission states:

  > *The support Europol will be called to provide in practice will not be limited to information exchange and analysis. It may for instance include forensic support, especially taking into account that the EPPO is an investigative and prosecutorial body.*
  >
  > *This would also be in line with the current Europol Regulation, where Article 4(1)(j) on the cooperation of Europol with Union bodies provides that this cooperation takes place in particular through exchanges of information and by providing analytical support, which is not exhaustive.*

  We would like to highlight that there is no legal basis for the envisioned support. Pursuant to Article 102 of the EPPO Regulation, the cooperation is clearly limited to providing information and analytical support to a specific investigation conducted by the EPPO. Further, we would like to point out Recital 100 of the EPPO Regulation, whereby the

purpose of the cooperation with Europol is for the EPPO to obtain the relevant information as well as to draw on Europol's analysis in specific investigations. The cooperation pursuant to Article 4(1)(j) can only go as far as foreseen in the legal mandate of Europol or the EPPO. Yet, EPPO Regulation demonstrated a clear intention by the co-legislator to limit the cooperation to providing information and analytical support to a specific investigation conducted by the EPPO.

- In order to avoid national investigations being jeopardised or sensitive information being disclosed, it is important that Europol can only share information with the EPPO if the Member State, Union body, third country or international organisation that provided the information has given its prior consent. We would like to highlight that Europol's cooperation with Eurojust, OLAF and EBCG follows this principle (as stipulated in Article 21(1) and (1a)).

- Regarding Article 20a(3), we maintain our doubts that the proposed hit/no-hit mechanism is in line with the EPPO Regulation. Our doubts are based in particular on the fact that Article 102 of the EPPO Regulation does not provide for such mechanism in relation to Europol (while explicitly doing so for Eurojust and OLAF in Article 100(3) and Article 101(5) respectively). This indicates the clear intention of the legislator that there should be no hit/no-hit mechanism for Europol. Furthermore, we would like to point out the legal concerns raised by the Council Legal Service. In that context, we welcome the clarification in the Commission's non-paper on Article 20a that the proposed hit/no-hit mechanism does not stem from a legal obligation arising from the EPPO Regulation, but is rather a political choice by the Commission which goes beyond the mere mirroring of the EPPO Regulation.

In order to address our comments, we would like to suggest that Article 20a be re-worded altogether as follows (changes compared to the current text proposal of Article 20a in document WK 757/2021 REV 5):

"Article 20a

Relations with the European Public Prosecutor's Office

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation.

2. Upon request by the EPPO in accordance with Article 102 of Regulation (EU) 2017/1939, Europol shall support the investigations of the EPPO ***~~and cooperate with it, in particular through exchanges of information and~~*** *by providing* ***information and*** *analytical support.*

~~3. Europol shall take all appropriate measures to enable the EPPO to have indirect access, within its mandate, to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system, without prejudice to any restrictions indicated in accordance with Article 19(2) by the Member State, Union body, third country or international organisation which provided the information in question. Article 21 shall apply mutatis mutandis with the exception of its paragraphs 2 and 8.~~

3.~~4.~~ *Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939.*

4. If the information referred to in paragraphs 2 and 3 is subject to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2) of this Regulation, Europol shall consult with the provider of the information stipulating the restriction and seek its authorisation for sharing.

In such a case, the information shall not be shared without an explicit authorisation by the provider.*"*

IRELAND

"Ireland greatly values its membership of Europol and has demonstrated its commitment by opting in early to this proposal under Article 3 of Protocol 21 to the Treaty.

Questions have been forwarded to Ireland from the SIRIUS office concerning legislation governing voluntary cooperation between law enforcement authorities from other Member States and private parties based in Ireland. Ireland is a common law State and there is no legislation covering such voluntary cooperation. It is a matter for the private party to decide if it can lawfully cooperate with any such request.

Ireland wishes to maintain its scrutiny reservation at this time on the two thematic blocks relating to private parties and large data sets. Ireland has major concerns with regard to the effect that this draft Regulation may have on the Europol National Units in some Member States, such as Ireland, particularly in relation to the volume of requests, resourcing and IT security. Also of concern is the capacity of ENUs to respond in a timely manner, taking cognisance of national legislation, should Judicial proceedings be required. It is respectfully requested that Europol set out the role that they envisage the Member States ENUs will have in processing these requests, i.e. Judicial authority requests and the requirement for Data Subject Categorisation on receipt of data from Private Parties.

Irish officials are available to virtually meet with Europol directly, and/or the Commission, to discuss how to progress matters."

NETHERLANDS

Europol Regulation

Comments the Netherlands LEWP 7 May

Block 1 Enabling Europol to cooperate effectively with private parties

Recital 32:

- There still seems to be a small mistake in recital 32:

"Transmissions should relate to Europol disclosing personal data TO ~~with~~ national units, private parties or other recipients established in the Union, while transfers should relate to Europol disclosing personal data to private parties, public authorities or bodies established in third countries or to international organisations, in accordance with the applicable rules."

Article 26 para 2:

- Thank you for including a text on determining whether a seat member state should be considered a national unit concerned in article 26 para 2. We have one textual suggestion, since we are wondering whether it is necessary to say that they will "automatically" constitute a national unit concerned. One of the options suggested here was that Member States could opt in to being informed. Such a system would mean that Member States would not "automatically" be a national unit concerned, but could choose to be one or not. We would therefore like to propose deleting the word "automatically".

> "Criteria as to whether the national unit of the Member State of establishment of the relevant private party ~~automatically~~ constitutes a national unit concerned shall be set out in the guidelines referred to in Article 18(7)."

Block 3: Strengthening Europol's role on research and innovation

Article 33a

Para 1

- Thank you for taking on board our suggestion that the MB should sometimes be consulted and not just informed about projects for research and innovation, both in article 33a para 1 subpara b and in recital 39.

Para 4

- We have some concerns about the new paragraph 4, which states that all of Europol's information can be used for research and innovation and seems to set aside the ownership principle.

- The Netherlands very much supports a strong role for Europol in the area of research and innovation. This is for example why we have taken on the role of deputy chair of the Clearing Board of the Innovation Lab.

- We understand that Europol needs to use information in order to be able to carry out innovation projects and want to make sure that it can do so.

- However, police detectives all over the Union trust Europol with their information, because they know they retain ownership over the information they provide it with and that only they can decide what happens to that information.

- They can for example provide information for cross-checking, whilst knowing that if Europol also wants to use the information for operational analysis, it has to come back to them to get permission.

- But now, this proposal is saying to them that regardless of the ownership principle, ALL the information they provide could be used for research and innovation.

- Not only that, but it will not be fellow police men and women handling this sensitive information, but IT developers.

- We think this could make police officers across the Union hesitant to share data with Europol.

- We think there is a simpler solution to this problem. Article 33a para 1 sub a states that:

> "any project shall be subject to prior authorisation by the Executive Director, based on" among other things "a description of the personal data to be processed".

- So for each innovation project, Europol already has to determine which data it wants to use.

- Maybe we could include a step where the Member States whose data will be used also have to agree to the plan for the innovation project?

- That way there is no need for all Europol data to be designated as available for research and innovation, but it can be determined project by project.

- This is why we would like to suggest adding the words "and the Member States involved" to article 33a para 1 sub a, so that it reads:

> "any project shall be subject to prior authorisation by the Executive Director and the Member States involved, based on a description of the envisaged processing activity setting out the necessity to process personal data, such as for exploring and testing innovative ~~new~~ **technological** solutions and ensuring accuracy of the project results, a description of the personal data to be processed, a description of the retention period and conditions for access to the personal data, a data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome, and the measures envisaged to address those risks;"

- In addition, we would like to suggest deleting the proposed new paragraph 4.

- This would make sure that the ownership principle remains the basis of Europol's work and that our police officers will continue to trust Europol with their data.

- One suggestion made during the LEWP of 7 May was that Member States could opt out of making all of their information available for research and innovation projects.

- We think that if such a system is introduced, a system where Member States opt IN to making all of their information available for research and innovation projects would be more in line with the ownership principle. Such a system could consist of two steps:

> - First of all, some Member States could decide to give permission for all of their information to be used for research and innovation projects;
>
> - Member States who choose not to give permission for all of their information to be used for research and innovation projects, can decide to give permission for the use of a specific part of their information for a specific research or innovation project, as described by Europol based on article 33a para 1 sub a.

General

- As a final comment on article 33a, we would again like to point to the EDPS recommendation that "the scope of the research and innovation activities should be better defined in the Europol Regulation, e.g. by clearly linking those activities to the tasks of Europol, and further clarified in a binding document, for instance adopted by the Management Board of Europol, which could be subsequently updated, if necessary". Maybe we could include some text to say that the Management Board will further define the scope of the research and innovation projects in the guidelines to be adopted under article 18 para 7? We could for example add the following sentence to the end of article 33a para 1:

> "The scope of the research and innovation activities will be further defined in the guidelines referred to in Article 18(7)."

Block 6: strengthening Europol's cooperation with the EPPO

Article 20a

Para 3

- We have a question regarding the differences between recital 22 and article 20a. Article 20a para 3 talks about: "indirect access to information […] on the basis of a hit/no hit system", but recital 22 only mentions "access, on the basis of a hit/no hit system", so without the word "indirect". Maybe we should add the word "indirect" to recital 22 too?

- Thank you for taking on board our suggestion to add the words "within its mandate" in paragraph 3.

Para 4

- As we mentioned before, in order to avoid the risk of the same criminal conduct being reported to the EPPO by both Europol and a Member State, we also think it would be useful if article 20a para 4 would contain a reference to article 19 para 2, to make clear that prior consent from the MS that provided the information is necessary. Maybe the following text from article 21 para 1 can be added here too:

> "4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence, without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2)."

Block 2: Enabling Europol to process large and complex datasets

Article 18 para 5a

- Regarding the text that has been added (or moved): "and where necessary for Europol for the purpose of determining whether personal data complies with the requirements of paragraph 5 of this Article" are the words "for Europol" really necessary here? It continues with: "Europol may temporarily process", so it is already clear that this applies to Europol. Maybe the text could read:

> "5a. Prior to the processing of data under paragraph 2 of this Article, and where necessary ~~for Europol~~ for the purpose of determining whether personal data complies with the requirements of paragraph 5 of this Article, Europol may temporarily process […]"

- We have a question about the relationship between article 18 para 5a and article 18a para 2. Article 18a para 2 stipulates that "personal data outside the categories of data subjects listed in Annex II shall be functionally separated from other data". However, an exception seems to have been made for the data outside of Annex II that is processed under article 18 para 5a, because the sentence starts with: "Without prejudice to the processing of personal data under Article 18(5a)". Do we understand correctly that under art 18 para 5a the non-annex II data does not have to be functionally separated? Why is an exception being made for this data under art 18 para 5a?

Article 18 para 5a and article 18a para 1:

- Can the Commission explain how the Police / Law Enforcement directive (directive 2016/680) allows MS to transmit big data? Which articles make it possible for Member States to provide large datasets or investigative case files to Europol? We need to add a whole new article to the Europol Regulation to make it possible for Europol to receive and process these datasets. The rules for the transmission of data are quite strict under directive 2016/680. Should the Law Enforcement Directive also be amended or does it already allow for this? We are not sure that directive 2016/680 provides this option.

- And how can Member States make sure that it is necessary and proportional for them to provide large datasets to Europol? In the Netherlands, we have guidelines that describe how law enforcement agencies should determine the purpose of the processing and whether the processing is necessary and proportionate, before they acquire and process large datasets. In order to be able to take a decision on the purpose, necessity and proportionality, they need to have a rough idea of the data subjects contained in the dataset.

- Before MS provide a large dataset to Europol, the purpose of the processing and the contents of the dataset could for example make it necessary for the Member State to minimise the dataset. This means that they cannot just provide any dataset to Europol, but they need to have a plan and adjust the dataset accordingly. So maybe Europol could also develop some guidelines for the Member States on how they should handle this, to ensure some uniformity in the provision of large datasets (of course subject to the differences in the way the directive has been implemented by MS).

- In order to achieve this, maybe when the Management Board further specifies the conditions for the processing of big data as mentioned in para 2, this should also include the conditions under which the data can be provided to Europol. So maybe the text of the second section of both art 18 para 5a and of art 18a para 2 should be changed into:

> "The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the provision and processing of such data."

Article 18a para 1

- We initially understood that the whole of article 18a was about processing non-annex II-data and that therefore processing under this whole article was limited to operational analysis. But now, para 2 stipulates that all forms of processing are allowed, even though it still mentions "personal data outside the categories of data subjects listed in Annex II". We are confused how paras 1 and 2 relate to each other. Does para 1 refer to large datasets that also include non-annex II data and does para 2 refer to the minimised version of that dataset that only includes annex II data, which means that under para 2 only annex II data can be processed? Or have we misunderstood?

- Because of the complexity of article 18 para 5a and article 18a, we would very much appreciate it if the Commission could provide us with some flow charts to see how the different steps of processing large datasets and the stipulations in these articles relate to each other.

Article 18a para 3

- The first and second section of para 3, especially the last parts, are very similar. The different uses of the word "related" may cause some confusion:

> - in the first section, the word "related" is used to indicate the connection between the judicial proceedings and the criminal investigation:
>
> > "and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State."

- in the second section, however, the word “related” refers to the connection between the original investigation and the other investigation and the word “following” is used to indicate the connection between the judicial proceedings and the criminal investigation:

> “and only for as long as judicial proceedings following a related criminal investigation are on-going in that another Member State.”

- In order to prevent confusion, we would like to suggest clarifying the text of the first section by replacing “related to” by “concerning”. This way, the word “related” will only refer to the connection between the original and the other investigation:

> “3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings ~~related to~~ concerning that criminal investigation are on-going in that Member State.”

(- We could consider replacing the word “following” in the second section by “concerning” too. “Following” could be read to mean that the judicial proceedings come after the criminal investigation in time, whereas “concerning” would more clearly indicate that the judicial proceedings are based on the criminal investigation:

> “That Member State, or, with its agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation, may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings following (or concerning?) a related criminal investigation are on-going in that other Member State.”)

Article 18a para 4

- What should Europol share with the EDPS under article 18a para 4, the complete investigative file, or just a short message that the file has been received?

- What will the EDPS do with this information?

- The EDPS already has access to all information at Europol. And if the processing will form part of a new filing system which for example involves a high risk to the rights and freedoms of data subjects, the prior consultation mechanism as defined in article 39 Europol regulation and article 90 EUDPR has to be followed. So what would be the added value of informing the EDPS in this situation?

- Is informing the EDPS about receiving an investigative case file from a third country in accordance with the role of a supervisory authority or would this mean that the EDPS would become too closely involved with Europol’s operational work?

- Regarding the third part of this paragraph about violation of fundamental rights, we are wondering about some differences between the second and third sentence. The second sentence mentions "objective elements" indicating a "manifest violation of fundamental rights". But the third sentence talks about "preliminary indications" of a "violation of fundamental rights". Why the difference?

- "Preliminary" sounds as if this will not be the last step in the process. Why is the word "preliminary" there? Does this mean that after Europol has found indications of a violation of fundamental rights and stops to process the data, it can continue to examine the possible violation of fundamental rights? Could it come to a different conclusion later and start processing the data again?

- And why is the word "manifest" missing from the third sentence? This sounds like a lower threshold for the violations. Shouldn't the third sentence also talk about "manifest violations of fundamental rights"?

POLAND

Block 2 – large and complex data sets

Art. 18a (4)

In the light of the discussion and explanation received from the Commission on the 12 April LEWP VTC, as regards processing by Europol personal data from a third country and verification if the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports and if there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights, **PL suggest deleting the second element, namely verification of respect for fundamental rights**. If we assume that third countries, which are a party to an international agreement pursuant to Article 218 TFEU or a cooperation agreement in accordance with Article 23 of Decision 2009/371/JHA, or are subject of adequacy decision, are trusted partners, which do not obtain personal data with violation of fundamental rights, there is no need to include a provision which stipulates the necessity to verify it by Europol.

Furthermore, PL still needs some more clarification as regards the term "manifestly disproportionate" and how Europol will conduct verification in practice and are there appropriate tools at its disposal? The involvement of EDPS in the process might be a challenge.

We would like to repeat once again our question what will happen if Europol reaches the conclusion that amount of personal data is disproportionate, however the data set contains crucial data for further criminal investigation in MS? **PL suggests exploring a possibility of including the provision regarding requesting a third country to narrow the scope of data.**

Block 3

Art. 33a (4)

Poland does not agree with the general derogation from Article 19(1) as regards processing of personal data for the purpose of research and innovation, with reference to data transmitted after entering the amended regulation into force. We are convinced that, in general, the achievement of appropriate results in the field of research and innovation is largely based on the use of as many and the most reliable data. The development of efficient and reliable algorithms in the research carried out by Europol must rely on the use of the data it processes for this purpose. **Poland supports the strengthening of the role of Europol in the field of research and innovation**, and our intention is not to block its access to data, which is of decisive importance primarily in the field of artificial intelligence tools. However, their processing will have to be subject to a number of safeguards, already enshrined in Article 33a (1). Notwithstanding the above, **the preferable and safest solution for us seems to be the data owner deciding on the purpose of processing, as it has been the case so far, e.g. with operational and strategic analysis.** At the same time we remain open for a discussion on how to implement it, for example by introducing new handling code for reasearch and innovation purposes with default agreement feature.

On the other hand, as regards the past data, verifying the purposes of processing and reaching the primary data owners seem to be rather impossible and we are strongly committed to strengthen the Europol capabilities in research and innovation, therefore we incline towards supporting the derogation form Article 19 (1) in this context. We would find the CLS opinion in that matter helpful.

Block 6 – EPPO

Bearing in mind the current wording of new art. 20a as well as new art. 24, and included references to art. 19 (2) in these provisions, Poland suggests adding the word "transmission" in the first sentence of art. 19 (2), as follows:

"Member States, Union bodies, third countries and international organization may indicate, at the moment of providing information to Europol, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its transfer, **transmission,** erasure or destruction. Where the need for such restrictions becomes apparent after the information has been provided, they shall inform Europol accordingly. Europol shall comply with such restrictions."

The abovementioned amendment is in line with the wording of recital 22 and will allow countries not participating in enhanced cooperation with the EPPO to fully secure the data transferred to Europol in the course of ongoing cases.

ROMANIA

ROMANIAN WRITTEN COMMENTS

-FOLLOW-UP LEWP on 07 May 2021 -

5. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

Art. 20a - We can support the current text.

Art. 25(8) and Art. 2 (s). We can agree with the amendments to Article 25 (8) and the introduction of a definition of transfer categories in Article 2 (s).

Art. 26 (6a) and Art. 26a (5). Clarifications are needed on the situations in which Europol may request personal data from private parties through national units the type of data requested and their content.

The private parties are, as a rule, subject to national legislation on the protection of personal data, so the responses to Europol's requests should be voluntary both for private parties and MS authorities.

Thus, Europol's request should not be mandatory, but follow the means of communication regulated at national level, in the sense that it is made through the national competent authorities.

Consequently, for an unequivocal understanding, we consider necessary that the safeguards with regard to the principles in the matter of the jurisdiction of the states, judicial cooperation and protection of human rights and protection of personal data should be highlighted.

Art. 26 (11) - We can agree with the text, including the new additions at the end of the paragraph ***("By principle, these examples shall be anonymized insofar as personal data is concerned").***

Art. 33a (4) – We request the examination reservation. This is necessary in order to examine in detail whether it is appropriate to allow the use of data collected in the past by EUROPOL, before the entry into force of the new regulations.

In principle, the regulations in the field of data protection do not allow the data collected for one purpose to be used for other purposes, except in the limited situations provided by GDPR and LED. In the situation under analysis, the intention is that the data collected before the entry into force of the new regulations to be used for innovation purposes, which is different from the initial one for which they were collected.

Thus, **we do NOT agree with the specification relating to the derogation from Art. 19, paragraph 1.**

At the same time, we would like some clarifications on the wording regarding the political decision (way forward which is considered by PRES PT).

*The Presidency decided to clarify in the text that **data provided to Europol before the amendment of the Regulation may be used for research and innovation**, on the assumption that this is what the majority of Member States understood and supported until this moment.*

*However, **allowing or not to use past data originally transmitted for other purposes than innovation is a matter of political choice** and the Member States are invited to discuss this issue in order to make an informed decision regarding the new paragraph 4 in Article 33a.*

Art. 18(5a). We request **the deletion of** the wording **"where relevant"** at the end of the paragraph, because it can create confusions in practical approach.

*"Europol may only process personal data pursuant to this paragraph for a maximum period of one year, or in justified cases for a longer period with the prior authorisation of the EDPS, where necessary for the purpose of this Article. Where the result of the processing indicates that personal data do not comply with the requirements of paragraph 5 of this Article, Europol shall delete that data and inform the provider of the data accordingly **where relevant**."*

SPAIN

Spain.- Follow-up comments to the last LEWP meeting (7/05/2021)

AS REGARDS THE REVISION OF THE EUROPOL REGULATION, SPAIN PROVIDES THE FOLLOWING MODIFICATIONS

ON THEMATIC BLOCK 1:

Article.26.6b) : Regarding this article, it would be necessary to clarify in this article that in case this exchange falls outside the scope of the objectives of Europol, this exchange, should be initiated by initiative of the Member Estate interested".

ON THEMATIC BLOCK 8: : STRENGTHENING THE DATA PROTECTION FRAMEWORK APPLICABLE TO EUROPOL

Article 28: Regarding this article, it is considered that data protection principles should be included in this block to ensure the quality of data protection.

Article 30.2: With regard to Article 30 paragraph 2, it is considered appropriate to clarify what kind of criteria would be used to consider these data as strictly necessary and proportionate.

9. COMMENTS RECEIVED AFTER THE MEETING ON 18 MAY 2021 (BLOCKS 1, 2, 3, 5, 6 AND 7)

BELGIUM

Written comments of Belgium related to the revision of the Europol mandate following the LEWP on 18/05

BLOCK 1 – Europol's cooperation with private parties

Recital 35a

We note the newly added recital 35a and paragraph 4a of Article 26a. While we do see a benefit in ensuring that no duplication arises, we believe the using of the word "before" in recital 35a will prove too restrictive in practice. This would indeed introduce a timeline of these actions that could be cumbersome or even problematic in practice, when trying to prevent information to go viral. We follow the reasoning of the Commission that – based on Article 4(1)(u) – the whole of the actions by Europol in this regard, is already subject to the request of the Member States. Therefore, we consider it appropriate to change the word "before" to "when", which still indicates a sufficient time indication according to Belgium.

Additionally, we believe that the last sentence of this recital 35a is not fitting for the actual and practical way of working in the context of referrals. It might not always be realistic to abide by this sentence, which is more suited for dealing with removal orders than for dealing with referrals. We thus believe also this formulation will prove to be too restrictive in practice and will not provide the necessary flexibility. Belgium believes the first sentence covers the essence and is sufficiently clear. For the reasons just mentioned, we thus propose to delete this phrase.

Our text proposal for recital 35a thus reads: *"In order to avoid duplication of effort and possible interferences with investigations and to minimise the burden to the hosting service providers affected, Europol should exchange information, coordinate and cooperate with the competent authorities* ***when*** ~~***before***~~ *transmitting or transferring personal data to private parties to prevent the dissemination of online content related to terrorism or violent extremism.* ~~***Where Europol is informed by a competent authority of a Member State of an existing transmission or transfer, it should not transmit or transfer personal data concerning the same subject matter.***~~*"*

BLOCK 2 – Processing of large data sets

Following the interesting debate in the LEWP meeting on 18/05, Belgium is still not convinced that the provision of a definition of an investigative file and the texts of article 18.5a and 18a are sufficient both from the perspective of legal clarity (and hence leaving as little as possible room for interpretation) and operational efficiency and clarity when thinking about implementing the new provisions.

Article 2 (q) - Definition of an investigative case file

- Belgium is not at all convinced that we need the concept of an "investigative case file" and a definition of the concept. As we understand it, the underlying rationale of Article 18a is that Europol should be allowed to process data outside Annex II if this is in support of a criminal investigation of a Member State or third "trusted" country (or EPPO). Defining and using the concept of an "investigative case file" only creates interpretation problems (for instance the Commission said it would not apply to intelligence gathering – for us that is exactly one of the most important reasons for asking Europol to support us in analysing data) and creates the need to further define a whole procedure (who decides on the creation?, when does it apply: only when it is very likely that it contains data outside of Annex II?, how does it relate to other procedures with regard to sending data for operational analyses?...).

- With regard to the definition in Article 2(q): do we really need the terminology of "datasets"? There is no definition of a "dataset" in the Regulation and this might pose a risk of difference of interpretation between the EDPS and Europol when applied in practice. Would a reference to "data" not be sufficient?

- All in all Belgium still prefers the deletion of this definition and to go for an integration of the definition in the text of article 18a as follows (for a more reasoned explanation see our previous written comments on this article):

    - *"1.* ~~***Where necessary for the support of a specific criminal investigation,***~~ *Europol may process personal data outside the categories of data subjects listed in Annex II where:*

    - *(a) a Member State or the EPPO* ***in accordance with procedural requirements and safeguards under applicable national or Union law*** *provides* ***for the purpose of operational analysis or in exceptional and duly justified cases for cross-checking*** ~~***an investigative case file***~~ ***data*** *to Europol* ***for Europol's support of a***~~***[In ongoing]***~~ ***criminal investigation*** ~~*[within the mandate of Europol]*~~ ***related to one or more Member States*** ~~***pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2), or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2)***~~*; and*

    - *(b) Europol assesses that it is not possible to carry out the operational analysis of* ~~*the investigative case file*~~ ***the data*** *without processing personal data that does not comply with the requirements of Article 18(5). This assessment shall be recorded."*

The relation between article 18.5a and 18a

As a result of the discussion during the LEWP on 18/05, Belgium believes that there is now a consensus that article 18.5a would not be used always as a first step and that it would depend on the situation in which the data is sent to Europol. Belgium believes that there is now a consensus on the fact that in practice article 18a would be able to be used when Europol receives the data in the context of an investigation and where the data owner has the legal possibility to send that data to Europol.

However, Belgium remains very concerned that this way of interpreting of both articles will still be open to interpretation, especially by the EDPS. While there is no language nor in the recitals nor in the articles 185a and 18a about having to be applied exceptionally, the EDPS in its opinion clearly

indicates that both article 18.5a and certainly article 18a would have to applied exceptionally. According to Belgium, there is no doubt whatsoever that the EDPS will interpret both articles as exceptions and will demand (as the EDPS is to be consulted) that its suggestions be included in the Management Board Decision further specifying the provisions of the processing. The EDPS shall certainly always demand that Europol applies both articles as strict as possible. In other words, according to our assessment, while both provisions intend to give Europol the legal basis that was lacking according to the EDPS admonishment, it remains very likely that in practice, Europol's possibilities to process non DSC data in order to support Member States will continue to suffer due to a strict interpretation of both provisions. The fact that the Commission (as pointed out by the EDPS in its Opinion) has presented these possibilities as (strict) exceptions in its impact assessment remains an important vulnerability towards the EDPS and most likely towards the European Parliament.

Taking into account all of the above, Belgium still wonders whether it a shorter, clearer and simpler proposal would not be a better solution. We even should consider stepping out of the logic that Europol in principle (article 18.5 is regarded as such, certainly by the EDPS) always has to be able to apply a DSC. Indeed, this requirement for Europol is stricter than the requirements other JHA agencies have (eg EPPO) and what we as Member States have. Other EU agencies and MS indeed only have to apply a DSC "as far as possible". However, we do have to admit that we have not been able yet to come up with such a proposal (yet), but perhaps – if other MS could support this – we should take the time to come up with such a proposal as this concerns indeed the very heart of Europol's operational support to the MS.

Paragraph 4 of Article 18a

We sustain our previous comment concerning the role of the EDPS in paragraph 4 of Article 18a and ask for deletion of the obligation to inform the EDPS. We have similar concerns as the Netherlands and Poland during the LEWP meeting of 19 May (namely the added value of this process for these 'trusted third countries' and the risk of the EDPS being too closely involved in operational cases).

We sustain our previous comment questioning the added value of the reference to the violation of human rights in paragraph 4 Article 18a, in the same line of the Polish comments during the LEWP meeting of 19 May. We wonder what the difference is with current Article 23(9), which applies already to all information provided to Europol. This unclarity about the added value compared to Article 23(9) was also confirmed by Europol and did not yet receive a response by the Commission. We wonder thus still whether this obligation here is not redundant and thus suggest to delete it.

The text of paragraph 4 of Article 18a would then read: *"4. Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports.* ~~***Where a third country provides an investigative case file to Europol, the EDPS shall be informed.***~~ *Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports*~~***, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights***~~*. Where Europol*~~***, or the EDPS,***~~ *reaches the conclusion that there are preliminary indications that*

such data is disproportionate ~~*or collected in violation of fundamental rights*~~*, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union."*

BLOCK 3 – Europol's role in research and innovation

As a red line Belgium finds it unacceptable that a derogation from Article 19(1) is created in the Europol Regulation. It is not possible to anticipate all sensitive cases for the future. This would not abide by the division of powers, because such a text would then entail that all operational information should always be put at the disposal of research and innovation purposes. This is also not compatible with the nature of operational law enforcement data. As expressed by Germany, the decision to exclude certain data often resorts to a decision by operational entities, such as prosecutors or investigating judges who confer with police authorities. It is not advisable to legislatively consider áll past and future operational data to be 'sharable' by default. We cannot support circumventing the ownership principle seeing as how this does not respect the competency of the national authorities and the sensitivity of certain data and certain cases.

Preferred option related to recital 39, Article 33a(1)(b) and Article 33a(4) to ensure data to be able to be used for research and innovation purposes

Taking into account the above, Belgium still has an explicit preference for not including the proposed amendments to recital 39, Article 33a(1)(b) and Article 33a(4). In this way, all Member States can individually decide whether to grant Europol access to all past and even future data, to exclude certain data, to only authorize access for certain data or to not authorize access. Guidelines for this could be drafted by the Management Board on this to ensure an effective and efficient procedure. These guidelines could be an appropriate amendment of the Integrated Data Management Guidelines developed by the Management Board based on Article 18(7).

We repeat that not changing the original Commission's proposal thus still perfectly allows for Member States giving a general go-ahead to use all there data for research and innovation purposes. It is clear that also without an amendment of the original Commission's proposal information provided to Europol in the past can be marked by the Member States as able to be processed for research and innovation purposes, if so desired.

We thus propose to keep the original Commission's proposal on this topic and to delete the proposed changes to recital 39, Article 33a(1)(b) and Article 33a(4).

Compromise proposal related to recital 39, Article 33a(1)(b) and Article 33a(4) to ensure data to be able to be used for research and innovation purposes

In the spirit of compromise and if the legislator insists on clarifying this way of working in the Regulation, we can continue to work on the proposed amendments to recital 39, Article 33a(1)(b) and Article 33a(4). Our red line detailed above remains however and a legislative derogation from Article 19(1) is not acceptable to Belgium. A derogation is furthermore also not compatible with the agreed upon owner principle, reflected in recital 39 in the sentence stating that *"Europol should not*

process personal data for research and innovation without the agreement of the Member State that submitted the data to Europol." We propose an amendment to make sure that the text clarifies that a Member State or third partner (we suppose that also the data of thirds partners can be used?) can give a general or a specific go-ahead to use data provided to Europol in the past and/or the future. In this way, efficiency is guaranteed and the owner principle is respected.

The text of Article 33a(4) would then read (the order of the two sentences has been reversed): *"In the context of the consultation of the Europol Management Board for a research and innovation project as referred to in point (b) of paragraph 1~~,a Member State~~ the provider of the information may indicate that* ***all or part of the*** *personal data it submitted* ***or will submit*** *to Europol in accordance with Article 19(1)* ***may*** ***~~shall not~~*** *be used for that project. Where the requirements of paragraph 1 are fulfilled, and* ***~~by way of derogation from Article 19(1)~~*** ***if the provider of the information] has indicated this in the context of a specific project****, Europol may process personal data that has been processed for the purposes referred to in points (a) to (d) of Article 18(2) also for the purpose of Article 18(2)(e)."*

Streamlining our compromise proposal with recital 39 would require the following changes: *"Europol should inform the European Data Protection Supervisor prior to the launch of its research and innovation projects that involve the processing of personal data.* ***It should ~~also inform or~~ consult its Management Board, ~~depending on specific criteria that should be set out in relevant guidelines~~ including on the personal data to be processed. Europol should not process personal data for research and innovation without the agreement of the ~~Member State~~ provider of the information that submitted the data to Europol. To that end, in the context of a consultation of the Europol Management Board for a research and innovation project, a ~~Member State~~ the provider of the information may indicate that all or part of the personal data it submitted or will submit to Europol may ~~should not~~ be used for that project.*** *(...)"*

BLOCK 5 – Europol's cooperation with third countries

Article 25(4a) references in Article 25(1) and Article 25(2)

We still consider it useful for Europol to be able to conclude administrative arrangements with the third country after a positive self-assessment. Administrative arrangements will help streamline this additional structural way of working with the concerned third countries. This possibility currently exist for adequacy decisions. We note the explanation of the Commission but don't see any pertinent difference with how an administrative arrangement functions with regard to an adequacy decision.

Belgium thus proposes the following amendment to the last sentence of Article 25(1): "*Europol may conclude administrative arrangements to implement such agreements****, ~~or~~*** *~~adequacy decisions~~* ***or assessments of appropriate safeguards****."*

Also, we think that the Management Board should be informed about transfers of personal data following a positive self-assessment. This possibility currently exist for adequacy decisions. Article 25(2) should therefore read: "*The Executive Director shall inform the Management Board about exchanges of personal data on the basis of adequacy decisions* ***or assessments of appropriate safeguards*** *pursuant to point (a) of paragraph 1."*

Article 25(4a) references throughout the Regulation

We support the German comment stating that the newly added possibilities of Article 25(4a) should be added throughout the Regulation, where appropriate. There are several instances where reference is given to cooperation to third countries through enumerating the structural ways of working with third countries (namely the Article 218 agreement or the adequacy decision). Seeing as the new paragraph 4a is also foreseen as a structural form of cooperation, it should be added in these instances.

CZECH REPUBLIC

Please find enclosed last CZ comments on the recast of the Europol Regulation,

CZ also reiterates its previously submitted comments on Bloc 8.

CZ comments on Europol recast

(relative to wk 757/2021 rev 6)

Bloc 1

Art. 26a(4a)

CZ understands that this provision is limited to online crises defined in Art. 2(r) and that Europol will support the Member States only on their request pursuant to Art. 4(1)(u). Within such conditions, speedy action of Europol would be necessary. In order to protect the efforts and investigations of different Member States, a general reference to cooperation procedures (such as Crisis Protocol) seems appropriate:

4a. **Europol and the Member States shall develop procedures of cooperation in order to avoid duplication of effort and interference with investigations.**

The Member States should be able to indicate relevant contact points for such procedures. Recital 35a) should be modified accordingly.

Bloc 2

Art. 18a(2)

In order to avoid impossible levels of verification by Europol, CZ proposes to clearly attribute the responsibility for initiation of processing of investigative case files to Member States, with greater role of Europol in cross-checking:

2. (second subparagraph): The Management Board, acting on proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data**. These conditions shall respect the sole responsibility of the Member States or EPPO for**

determination of investigative case files to be processed, but shall enable Europol to review justification of processing requested pursuant to point (a) of Article 18(2).

Bloc 3

Art. 33a

CZ broadly supports the Presidency proposal, while being open to possible iteration. While CZ prefers opt-ins to opt-outs, the mechanism should in any case be easily practicable and enable simple and generalized decisions by Member States or law enforcement agencies, rather than require case-by-case or data-by-data decisions. In order to support the confidence of investigators in practice, we propose to clarify that Member State may block also usage of personal data yet to be submitted (even though correctly applied Art. 19(1) would enable case-by-case decisions):

4. Where the requirements of paragraph 1 are fulfilled, and by way of derogation from Article 19(1), Europol may process personal data that has been processed for the purposes referred to in points (a) to (d) of Article 18(2) also for the purpose of Article 18(2)(e). In the context of the consultation of the Europol Management Board for a research and innovation project as referred to in point (b) of paragraph 1, a Member State may indicate that personal data it submitted or will submit to Europol in accordance with Article 19(1) shall not be used for that project.

Bloc 5

Art. 25(4a)

CZ supports this provision and necessary changes to related provisions, such as Articles 18a(4), 26(1)(c), 26(4), 26(6), 26a(2), 26a(4), 27(1)(c) and 27(2).

Art. 25(5)

CZ believes that the wording of (b) should be adapted, as the transfer of personal data is done by the Europol rather than by the Member State. The same applies to recital 24). Possible solution is in the wording of Art. 26(6)(b).

Bloc 6

Art. 20a(1)

Given that data ownership principle has been explicitly reiterated in both paragraphs 3 and 4, and given FR request to refer to "data related to offences within EPPO mandate", CZ proposes to streamline and re-order the text and provide for these assurances in paragraph 1:

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). To that end, they shall conclude a working arrangement setting out the modalities of their cooperation. In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. **Information related to offences within the mandate of**

EPPO shall be provided by the Europol without prejudice to any restrictions indicated in accordance with Article 19(2) by the Member State, Union body, third country or international organisation which provided the information in question.

2. **Upon request by the EPPO in accordance with Article 102 of Regulation (EU) 2017/1939,** Europol shall ~~actively~~ support the investigations ~~and prosecutions~~ of the EPPO and cooperate with it, in particular ~~through exchanges of~~ by providing information and ~~by providing~~ analytical support.

3. Europol shall take all appropriate measures to enable the EPPO to have indirect access~~, within its mandate,~~ to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system~~, without prejudice to any restrictions indicated in accordance with Article 19(2) by the Member State, Union body, third country or international organisation which provided the information in question~~**.** Article 21 shall apply mutatis mutandis with the exception of its **paragraphs** 2 **and 8**.

4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence **in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939**~~, and without prejudice to any restrictions indicated in accordance with Article 19(2) of this Regulation by the Member State, Union body, third country or international organisation providing the information in question.~~ **Europol shall notify the Member States concerned without delay.**

Bloc 7

CZ wishes to reiterate that it supports deletion of amendment to Art. 6(1) ("Member State or"). CZ also believes that Europol is fully able to inform the Member State of any crime within its competence even without such an amendment.

(end of file)

FRANCE

Objet : Note de commentaires des autorités françaises – Commentaires de la France suite de la réunion du groupe LEWP du 18 mai 2021.

WK 757/2021 REV 6, Recital 24

(24) ~~Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise a categoryies of transfers of personal data to third countries in specific situations and on a case by case basis, where such a group of transfers relateds to a the same specific situation. consist of the same categories of personal data and the same categories of data subjects; and are necessary and meet all the requirements of this Regulation. This should cover situations where the transfer of personal data is necessary in order to protect the vital interests of the data subject or of another person; necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country; necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions; or necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal sanction.~~

Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects. To reinforce cooperation with third countries in preventing and countering crimes falling within the scope of Europol's objectives, the Executive Director of Europol should be allowed to authorise categories of transfers of personal data to third countries in specific situations and on a case-by-case basis, where such a group of transfers related to a specific situation are necessary and meet all the requirements of this Regulation.

Transfers not based on an adequacy decision or international agreement concludes by the EU should be allowed by the Management Board only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where Europol, after authorization of the Management Board, has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist.

Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. Europol should be able to also take into account the fact that the transfer of personal data will

7

Commented [A1]: Les autorités françaises estiment qu'il convient de modifier le considérant 24 en fonction de la modification de l'article 25 telle que présentée par la présidence portugaise.
Les autorités françaises précisent que cette proposition de rédaction s'inspire largement des considérants du règlement Eurojust (voir considérant 51 du règlement Eurojust). Soit la proposition de rédaction suivante :

be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, Europol should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, Europol should be able to require additional safeguards.

(25) To support Member States in cooperating with private parties ~~providing cross-border services~~ where those private parties hold information relevant for preventing and combatting crime, Europol should be able to receive, and in specific circumstances, exchange personal data with private parties.

In order to ensure Europol's effectiveness as a hub for information exchange, clear obligations should be laid down requiring private parties to provide Europol with the data necessary for it to fulfil its objectives.

Europol should increase the level of its support to Member States, so as to enhance mutual cooperation and the sharing of information.

Given the nature of the new tasks of Europol regarding privates parties, the Management Board should be given the necessary information regarding the data exchanged between Europol and Private Parties. Europol should submit an annual report to the Management Board on the information exchanged by private parties.

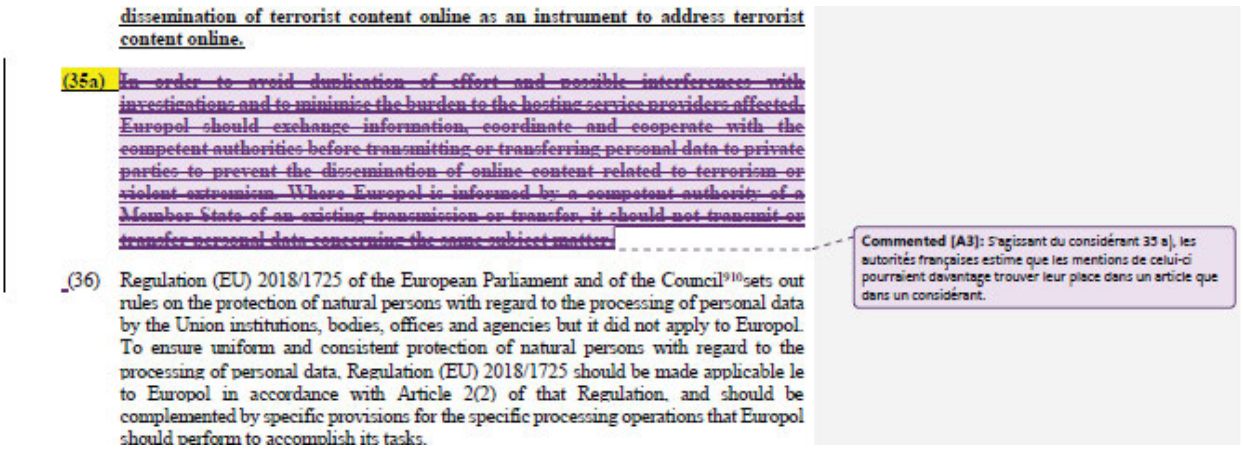
Commented [A2]: Les autorités françaises suggèrent la création d'un considérant en lien avec l'article 26(11)

(26) Criminals increasingly use cross-border services of private parties to communicate and carry out illegal activities. Sex offenders abuse children and share pictures and videos world-wide using online platforms on the internet. Terrorists abuse cross-border services by online service providers to recruit volunteers, plan and coordinate attacks, and disseminate propaganda. Cyber criminals profit from the digitalisation of our societies using phishing and social engineering to commit other types of cybercrime such as online scams, ransomware attacks or payment fraud. As a result from the increased use of online services by criminals, private parties hold increasing amounts of personal data that may be relevant for criminal investigations.

(27) Given the borderless nature of the internet, these services can often be provided from anywhere in the world. As a result, victims, perpetrators, and the digital infrastructure in which the personal data is stored and the service provider providing the service may all be subject to different national jurisdictions, within the Union and beyond. Private parties may therefore hold data sets relevant for law enforcement which contain personal data with links to multiple jurisdictions as well as personal data which cannot easily be attributed to any specific jurisdiction. National authorities find it difficult to effectively analyse such multi-jurisdictional or non-attributable data sets through national solutions. When private parties decide to lawfully and voluntarily share the data with law enforcement authorities, they do currently not have a single point of contact with which they can share such data sets at Union-level. Moreover, private parties face difficulties when receiving multiple requests from law enforcement authorities of different countries.

8

WK 757/2021 REV 6, Recital (35a)



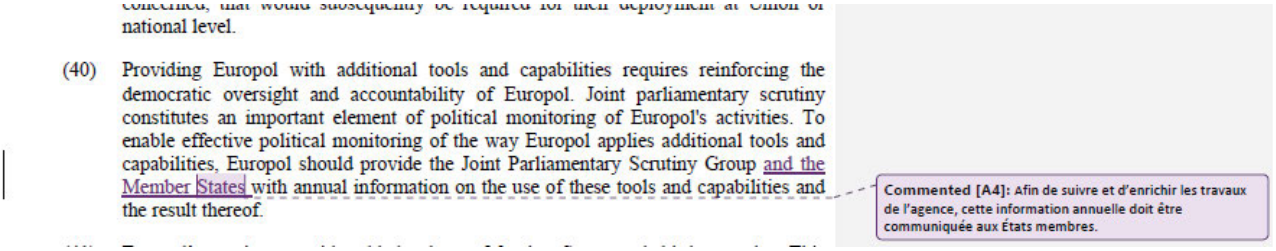
dissemination of terrorist content online as an instrument to address terrorist content online.

(35a) ~~In order to avoid duplication of effort and possible interferences with investigations and to minimise the burden to the hosting service providers affected, Europol should exchange information, coordinate and cooperate with the competent authorities before transmitting or transferring personal data to private parties to prevent the dissemination of online content related to terrorism or violent extremism. Where Europol is informed by a competent authority of a Member State of an existing transmission or transfer, it should not transmit or transfer personal data concerning the same subject matter.~~

Commented [A3]: S'agissant du considérant 35 a), les autorités françaises estime que les mentions de celui-ci pourraient davantage trouver leur place dans un article que dans un considérant.

(36) Regulation (EU) 2018/1725 of the European Parliament and of the Council[910] sets out rules on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies but it did not apply to Europol. To ensure uniform and consistent protection of natural persons with regard to the processing of personal data, Regulation (EU) 2018/1725 should be made applicable le to Europol in accordance with Article 2(2) of that Regulation, and should be complemented by specific provisions for the specific processing operations that Europol should perform to accomplish its tasks.

WK 757/2021 REV 6, Recital (40)



national level.

(40) Providing Europol with additional tools and capabilities requires reinforcing the democratic oversight and accountability of Europol. Joint parliamentary scrutiny constitutes an important element of political monitoring of Europol's activities. To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny Group and the Member States with annual information on the use of these tools and capabilities and the result thereof.

Commented [A4]: Afin de suivre et d'enrichir les travaux de l'agence, cette information annuelle doit être communiquée aux États membres.

~~(h) 'personal data' means any information relating to a data subject;~~

~~(i) 'data subject' means an identified or identifiable natural person, an identifiable person being a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;~~

~~(j) 'genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;~~

~~(k) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;~~

(l) 'recipient' means a natural or legal person, public authority, agency or any other body to which data are disclosed, whether a third party or not;

~~(m) 'transfer of personal data' means the communication of personal data, actively made available, between a limited number of identified parties, with the knowledge or intention of the sender to give the recipient access to the personal data;~~

~~(n) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;~~

~~(o) 'the data subject's consent' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to him or her being processed;~~

(p) 'administrative personal data' means all personal data processed by Europol apart from operational **personal** data~~those that are processed to meet the objectives laid down in Article 3~~;

(q) 'investigative case file' means a dataset or multiple datasets that a Member State, when two or more are affected, the EPPO or a third country ~~acquired~~ **is authorised to process** in the context of an on-going criminal investigation **related to one or more Member States**, in accordance with procedural requirements and safeguards under ~~the~~ applicable **Union law or** national criminal law, and **that it** submitted to Europol in support of that criminal investigation.

(r) 'online crisis situation' means the dissemination of online content that is linked to or suspected as being carried out in the context of terrorism or violent extremism stemming from an ongoing or recent real-world event, which depicts harm to life or physical integrity or calls for imminent harm to life or physical integrity, and where the online content aims at or has the effect of seriously

Commented [A5]: Les autorités françaises relèvent que, conformément à l'article 27 (a) de sa proposition, la Commission souhaite voir appliquer les définitions prévues à l'article 3 du règlement 1725 au règlement Europol.

Si les autorités françaises ne s'opposent pas à l'application de ces définitions au règlement Europol, elles relèvent que par souci de clarté, de sécurité et afin de déterminer au mieux les besoins de l'agence, le règlement Europol doit comporter les définitions de l'ensemble des termes qui y sont utilisés.
Si les autorités françaises sont conscientes que le règlement 1725 s'appliquera à Europol dès l'adaptation de celui-ci réalisée, elles proposent de reprendre les définitions du règlement 1725 et de les inscrire dans le règlement Europol.

Enfin, les autorités françaises souhaitent que la Commission précise si l'ensemble des définitions supprimées dans sa proposition sont reprises dans le règlement 1725.

Commented [A6]: Conformément aux remarques de la Commission et d'Europol au LEWP du 18/05/2021, les autorités françaises proposent d'amender l'article comme suit.

Néanmoins, les autorités françaises sont disposées à accepter une formulation de compromis qui se limiterait à faire référence à l'article 3(1).

WK 757/2021 REV 6, Article 4

(r) ~~enter data into the Schengen Information System, in accordance with Regulation (EU) 2018/1862 of the European Parliament and of the Council, following consultation with the Member States in accordance with Article 7 of this Regulation, and under authorisation by the Europol Executive Director, on the suspected involvement of a third country national in an offence in respect of which Europol is competent and of which it is aware on the basis of information received from third countries or international organisations within the meaning of Article 17(1)(b);~~

(r) Support Member States in processing data transmitted by third countries to Europol on lists of foreign terrorist fighters and data on persons involved in serious and organized crimes and propose the possible entry by the Member States, subject to their verification and analysis, of alerts into the Schengen information System, in accordance with Regulation (EU) 2018/1862 of the European Parliament and the Council. A periodic state of play mechanism shall be put in place in order to ensure that Member States and relevant stakeholders are informed on the data inserted in the SIS within a period of 18 months from the communication by Europol of its information to the Member States"

(s) support the implementation of the evaluation and monitoring mechanism under Regulation (EU) No 1053/2013 within the scope of Europol's objectives as set out in Article 3;

(t) proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States, ~~and~~ implement its research and innovation activities regarding matters covered by this Regulation, including in the development, training, testing and validation of algorithms for the development of tools, **and disseminate the results of these activities to the Member States in accordance with Article 67, and contribute to the coordination of activities of Union agencies established on the basis of Title V of the TFEU in the field of research and innovation within their mandates in close cooperation with Member States;**

Commented [A7]: Soit la proposition de considérant correspondante :

In the framework of its mandate and its task of supporting the Member States in preventing and combating serious crime and terrorism, Europol should support the Member States in processing third-country data by proposing the possible entry by Member States of alerts into the SIS, in order to make it available to the end-users of the SIS. To that end, a periodic state of play mechanism should be put in place in order to ensure that Member States and relevant stakeholders involved in the processing and analysis are informed on the data inserted in the SIS. The modalities for Member States' cooperation for the processing of data and the insertion of alerts into the SIS, notably as concerns the fight against terrorism, should be subject to [continuous] coordination amongst the Member States.

WK 757/2021 REV 6, Article 11

(u) adopt, where appropriate, other internal rules.

(v) " adopt guidelines on the receipt and exchange of data between Europol and private parties in accordance with article 26, after consulting the EDPS ».

(w) adopt guidelines on the memoranda of understanding to be signed between Europol and private parties

2. If the Management Board considers it necessary for the performance of Europol's tasks, it may suggest to the Council that it draw the attention of the Commission to the need for an adequacy decision as referred to in point (a) of Article 25(1) or for a recommendation for a decision authorising the opening of negotiations with a view to the conclusion of an international agreement as referred to in point (b) of Article 25(1).

3. The Management Board shall, in accordance with Article 110 of the Staff Regulations, adopt a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment of Other Servants delegating the relevant appointing authority powers to the Executive Director and establishing the conditions under which such delegation of powers may be suspended. The Executive Director shall be authorised to subdelegate those powers.

Where exceptional circumstances so require, the Management Board may, by way of a decision, temporarily suspend the delegation of the appointing authority powers to the Executive Director and any subdelegation of such powers and exercise them itself or delegate those powers to one of its members or to a staff member other than the Executive Director.

Commented [A8]: Argumentaire : Les autorités françaises précisent que ces lignes directrices n'interfèreraient pas avec les capacités de l'agence d'échanger des données personnelles avec les parties privées telles que prévues par les futures dispositions de ce Règlement. Il s'agirait pour les États membres d'impulser une dynamique dans un champ d'action nouveau pour l'agence en réfléchissant collectivement aux conditions et à l'application opérationnelle de ces échanges (quelles informations peuvent être envoyées par les parties privées (article 26 paragraphe 2a notamment), quelles infrastructures de communication (article 26 paragraphe 6b)...).
Cela serait plus cohérent avec les conclusions du conseil du 2 décembre 2019 qui mentionne que « *tout régime régissant la transmission directe de données à Europol par des parties privées devrait être fondé sur une procédure de consentement des États membres qui pourrait prendre la forme d'une liste proposée par Europol, constituée des parties privées de la part desquelles Europol aurait besoin de recevoir des données à caractère personnel. Cette liste ferait régulièrement l'objet de décisions prises par le conseil d'administration d'Europol, qui représente les autorités nationales* ».

Commented [A9]: Les autorités françaises soumettent une proposition de rédaction alternative à l'article 26b pour faciliter la prise en compte du contrôle par le CAE des MoU.

WK 757/2021 REV 6, Article 18a

Article 18a

Information processing in support of a criminal investigation

1. Where necessary for the support of a specific criminal investigation, Europol may process personal data outside the categories of data subjects listed in Annex II where:

(a) a Member State, when two ore more Member states are affected, or the EPPO provides an investigative case file to Europol pursuant to point (a) of Article 17(1) for the purpose of operational analysis in support of that specific criminal investigation within the mandate of Europol pursuant to point (c) of Article 18(2), **or in exceptional and duly justified cases, upon request by a Member State or the EPPO, pursuant to point (a) of Article 18(2)**; and

Commented [A10]: Sur ce point les autorités françaises renvoient aux remarques formulées à l'article 2(q).

WK 757/2021 REV 6, Article 20a

Article 20a

Relations with the European Public Prosecutor's Office

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation.

2. **Upon request by the EPPO in accordance with Article 102 of Regulation (EU) 2017/1939**, Europol shall ~~actively~~ support the investigations ~~and prosecutions~~ of the EPPO and cooperate with it, in particular ~~through exchanges of~~ by providing information and ~~by providing~~ analytical support.

3. Europol shall take all appropriate measures to enable the EPPO to have indirect access to data related to offences~~,~~ **within its mandate**, ~~to information~~ provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system, **without prejudice to any restrictions indicated in accordance with Article 19(2) by the Member State, Union body, third country or international organisation which provided the information in question.** Article 21 shall apply mutatis mutandis with the exception of its **paragraphs** 2 **and 8**.

4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence **in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939, and without prejudice to any restrictions indicated in accordance with Article 19(2) of this Regulation by the Member State, Union body, third country or international organisation providing the information in question. Europol shall notify the Member States concerned without delay.**

Commented [A11]: L*to theectile 26 (12)i les processus de traitement de l'er la procédure d's misison et '2424242424242424242424242424242424242424242424242424242424242424242424242424242424242424*es autorités françaises souhaiteraient savoir si le sens du terme comportement délictueux ici est bien le même que celui figurant dans le règlement d'EPPO à savoir : Le comportement délictueux (« *criminal conduct* ») doit s'entendre comme un comportement délictueux au sens des articles 22, 25(2) et (3) du règlement Parquet européen, c'est-à-dire un comportement répréhensible susceptible de relever de la compétence du Parquet européen.

Dans le cas où ce comportement délictueux prendrait la forme d'une donnée personnelle transmise par un EM, les autorités françaises notent qu'il conviendra dès lors de lui appliquer le régime de restrictions fixé à l'article 19 (2) du règlement Europol.

Enfin, les autorités françaises souhaitent, en retour, le service contributeur est informé de ce que l'agence a transmis à l'EPPO.

[3] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

WK 757/2021 REV 6, Article 21

8. If during information-processing activities in respect of an individual investigation or specific project Europol identifies information relevant to possible illegal activity affecting the financial interest of the Union, Europol shall on its own initiative without undue delay provide OLAF with that information without prejudice to any restriction indicated by Member States.

Article 22

Duty to notify Member States

Commented [A12]: Si les autorités françaises ne s'opposent pas à cette proposition, elles rappellent néanmoins qu'Europol devra obtenir l'accord de l'Etat membre fournisseur de la donnée avant de la transmettre à l'OLAF. Elles soutiennent donc les délégations de République - Tchèque et de Bulgarie sur ce point.

WK 757/2021 REV 6, Article 24

Article 24

Transmission of operational personal data to Union institutions, bodies, offices and agencies

1. Subject to any further restrictions pursuant to this Regulation, in particular pursuant to Article 19(2) and (3) and without prejudice to Article 67, Europol shall only transmit operational personal data to another Union institution, body, office or agency if the data are necessary for the legitimate performance of tasks of the other Union institution, body, office or agency.

2. Where the operational personal data are transmitted following a request from another Union institution, body, office or agency, both the controller and the recipient shall bear the responsibility for the lawfulness of that transmission.

Europol shall verify the competence of the other Union institution, body, office or agency . If doubts arise as to this necessity of the transmission of the personal data, Europol shall seek further information from the recipient.

The recipient Union institution, body, office or agency shall ensure that the necessity of the transmission of the operational personal data can be subsequently verified.

Commented [A13]: Les autorités françaises relèvent le manque de précision de cette proposition d'article. Notamment, elles estiment qu'il conviendrait de préciser quelle instance au sein d'Europol - Directeur exécutif, Officier de protection des données (DPO), Conseil d'administration - vérifiera la compétence de l'autorité requérante de la donnée lors d'un transfert.
Elles souhaiteraient également que la Commission précise l'étendue du « complément d'informations » qu'Europol pourra exiger pour apprécier la compétence des partenaires auxquels l'agence pourrait transmettre des informations. Concernant, l'expression « *legitimate performance* », les autorités françaises interrogent la Commission sur cette notion et sur l'autorité au sein d'Europol qui sera chargée d'évaluer « l'exécution légitime » des missions qui préside à la transmission de données. Enfin, les autorités françaises soutiennent la délégation hollandaise sur l'importance de préciser à l'article 24 la coopération avec les seules agences du domaine JAI.

WK 757/2021 REV 6, Article 25

4a. In the absence of an adequacy decision, Europol may, after authorization of the Management Board, transfer operational personal data to a third country or an international organisation where:

(a) appropriate safeguards with regard to the protection of operational personal data are provided for in a legally binding instrument; or

5. By way of derogation from paragraph 1, the Executive Director may authorise the transfer or a categories of transfers of personal data to third countries or international organisations on a case-by-case basis if the transfer is:

(a) necessary in order to protect the vital interests of the data subject or of another person;

(b) necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides;

(c) essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country;

(d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions; or

Commented [A14]: Les autorités françaises remercient vivement la présidence portugaise pour la prise en compte des commentaires des délégations et d'Europol sur le régime d'autres agences JAI en matière de coopération avec les États tiers.
Toutefois, elles précisent que cette modification du cadre d'échange avec les États tiers doit absolument s'accompagner d'un renforcement du contrôle du Conseil d'administration.
Ainsi, il conviendrait que le CAE non seulement décide des arrangements de travail et des arrangements administratifs conclu par l'agence (article 11r) mais également qu'il puisse autoriser Europol à échanger des données personnelles au terme du paragraphe 4a de l'article 25 tel que proposé par la présidence.
Les autorités françaises proposent donc un amendement à l'article 25.4.a (voir plus haut sur le CAE).

WK 757/2021 REV 6, Article 26

6b. Europol's infrastructure may be used for exchanges between the competent authorities of Member States and private parties in accordance with the respective Member States' national laws, **and those exchanges may also cover crimes falling outside the scope of the objectives of Europol. In cases where Member States use this infrastructure for exchanges of personal data on crimes falling within the scope of Europols objectives, they may grant Europol access to such data in order for Europol to process it according to the provisions of the articles 18(2) and 19(1). Europol may request further information from the Member States for that purpose.** In cases where Member States use this infrastructure for exchanges of personal data on crimes falling outside the scope of the objectives of Europol, Europol shall not have access to that data.

7. Europol shall ensure that detailed records of all transfers of personal data and the grounds for such transfers are recorded in accordance with this Regulation and communicated upon request to the EDPS pursuant to Article 40.

Commented [A15]: Les autorités françaises interrogent la Commission afin de savoir si Europol pourra traiter les données personnelles auxquelles l'agence aura accès dans ce cadre.
Dans l'affirmative, ce traitement devra être assorti de garanties appropriées.

11. Europol shall draw up an annual report to the Management Board including the number of personal data received ~~on the personal data~~ and exchanged with private parties pursuant Articles 26 and 26a on the basis of quantitative and qualitative evaluation criteria defined by the Management Board, including specific examples of cases demonstrating why these requests were necessary for Europol to fulfil its objectives and tasks. The annual report shall be sent to the European Parliament, the Council, the Commission and national parliaments. By principle, these examples shall be anonymized insofar as personal data is concerned.

Commented [A16]: Les autorités françaises accueillent favorablement cette proposition. Toutefois, pour la bonne information des États membres et la bonne conduite des échanges entre Europol et les parties privées elles proposent de compléter cette proposition

Par ailleurs, comme proposé par la Commission lors du LEWP du 12 avril 2021, et sous réserve de l'approbation de la Présidence, les autorités françaises pourraient également soutenir l'ancienne version du texte – article 7 (11)

WK 757/2021 REV 6, Article 27a

Article 27a

Processing of personal data by Europol

1. This Regulation, Article 3 and Chapter IX of Regulation (EU) 2018/1725 of the European Parliament and of the Council* shall apply to the processing of operational personal data by Europol.

Regulation (EU) 2018/1725, with the exception of its Chapter IX, shall apply to the processing of administrative personal data by Europol.

Commented [A17]: Pour mémoire, les autorités françaises rappellent que l'article 98 du règlement 2018/1725 prévoit que la Commission doit réviser le règlement Europol avant le 30 avril 2022 afin de s'assurer de sa compatibilité avec la directive (UE) 2016/680 et avec le chapitre IX du règlement 1725.

Les autorités françaises rappellent que, selon l'officier de protection des données d'Europol (DPO), le chapitre IX du règlement 1725 s'applique déjà aux autres agences de l'UE et que ses dispositions sont plus « génériques » que celle actuellement prévues dans le règlement Europol, autorisant ainsi une certaine flexibilité pour l'agence.

Toutefois, l'application de ce chapitre à Europol - si elle peut être saluée à certains égards - nécessite des aménagements qu'il convient de détailler article par article.

WK 757/2021 REV 6, Article 33a

Article 33a

Processing of personal data for research and innovation

1. For the processing of personal data performed by means of Europol's research and innovation projects as referred to in point (e) of Article 18(2), the following additional safeguards shall apply:

(a) any project shall be subject to prior authorisation by the Executive Director, based on a description of the envisaged processing activity setting out the necessity to process personal data, such as for exploring and testing innovative ~~new~~ **technological** solutions and ensuring accuracy of the project results, a description of the personal data to be processed, a description of the retention period and conditions for access to the personal data, a data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome, and the measures envisaged to address those risks;

Commented [A18]: Les autorités françaises affirment leur soutien à la Commission dès lors qu'il s'agit de permettre à Europol d'utiliser par principe –et sauf exception expresse- toutes les données dont il dispose pour la recherche et l'innovation. Elles estiment en effet indispensable au développement efficace de nouveaux outils technologiques, notamment liés à l'intelligence artificielle).

Cette utilisation devra se faire dans le plein respect du cadre juridique applicable en la matière. Une attention particulière doit être donnée aux données relatives à la lutte contre le terrorisme et au cadre légal de conservation des données.

WK 757/2021 REV 6, Article 34

Article 34

Notification of a personal data breach to the authorities concerned

1. In the event of a personal data breach, Europol shall without undue delay notify ~~the EDPS, as well as~~ the competent authorities of the Member States concerned, of that breach, in accordance with the conditions laid down in Article 7(5),as well as the provider of the data concerned ~~unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons~~.

2. The notification referred to in paragraph 1 shall, as a minimum:

(a) describe the nature of the personal data breach including, where possible and appropriate, the categories and number of data subjects concerned and the categories and number of data records concerned;

(b) describe the likely consequences of the personal data breach;

Commented [A19]: Les autorités françaises rappellent que l'actuel article 34 prévoit qu'en cas de violation de données à caractère personnel, Europol en informe le CEPD ainsi que les autorités compétentes des États membres concernés sans aucune forme de modération.
Afin d'assurer la transparence totale de l'activité de l'agence, la France estime nécessaire de supprimer la phrase suivante : « *unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons* ».

WK 757/2021 REV 6, Article 36

~~(c) such communication would involve disproportionate effort, in particular owing to the number of cases involved. In such a case, there shall instead be a public communication or similar measure informing the data subjects concerned in an equally effective manner.~~

~~5. The communication to the data subject may be delayed, restricted or omitted where this constitutes a necessary measure with due regard for the legitimate interests of the person concerned:~~

~~(a) to avoid obstructing official or legal inquiries, investigations or procedures;~~

~~(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;~~

~~(c) to protect public and national security;~~

~~(d) to protect the rights and freedoms of third parties.~~

Article 36

Right of access for the data subject

~~1. Any data subject shall have the right, at reasonable intervals, to obtain information on whether personal data relating to him or her are processed by Europol.~~

~~2. Without prejudice to paragraph 5, Europol shall provide the following information to the data subject:~~

Commented [A20]: Actuellement, Europol est tenu, en vertu de l'article 36, paragraphe 5 de son règlement de consulter les autorités compétentes des États membres et le fournisseur des données sur la décision à prendre en matière d'accès aux données des personnes concernées. Si un État membre s'oppose à la fourniture d'informations, Europol doit tenir **le « plus grand compte de cette objection »**.
Dans sa proposition (article 27a) la Commission propose d'appliquer au traitement de données opérationnelles par l'agence le chapitre IX du règlement 1725. Or ce chapitre prévoit - notamment l'article 83 – qu'une décision sur l'accès aux données doit être prise **en consultation et en étroite coopération avec l'autorité compétente concernée**.

Ainsi, les autorités françaises souhaitent que la Commission précise comment le chapitre IX du règlement 1725 et l'article 36, tel que proposé, pourront se concilier en pratique.
A ce stade des discussions, les autorités françaises relèvent que le régime prévu au chapitre IX du règlement 1725 risque de nuire à la bonne collaboration entre Europol et les services contributeurs en ce qu'il **étend considérablement la marge de manœuvre de l'agence dans l'appréciation de l'octroi du droit d'accès** sur des informations fournies par les **États membres** eux-mêmes.

Également, les autorités françaises relèvent que les justifications permettant de ne pas octroyer l'accès aux données d'Europol ont été supprimées. La France s'inquiète de cette suppression en ce que ces justifications permettent de protéger les enquêtes en cours. Si le règlement 1725 prévoit effectivement de telles justifications, la France demande à ce que les restrictions au droit d'accès des données soient prévues dans l'article 36.

WK 757/2021 REV 6, Article 37

Article 37

Right to rectification, erasure and restriction

1. Any data subject ~~having accessed~~wishing to exercise the right to rectification or erasure of personal data or restriction of processing referred to in Article 82 of Regulation (EU) 2018/1725 of personal data that relate to him or her may make a request to that effect~~concerning him or her processed by Europol in accordance with Article 36 shall have the right to request Europol~~, through the authority appointed for that purpose in the Member State of his or her choice, or to Europol~~, to rectify personal data concerning him or her held by Europol if they are incorrect or to complete or update them~~. ~~That~~Where the request is made to the Member State authority, that~~That~~ authority shall refer the request to Europol without delay and in any case within one month of receipt.

~~2. Any data subject having accessed personal data concerning him or her processed by~~

Commented [A21]: Pour rappel, Europol peut restreindre l'accès plutôt que supprimer la donnée « *lorsqu'il y a de bonnes raisons de croire que leur effacement pourrait porter atteinte aux intérêts légitimes de la personne concernée* ».
L'article 82, paragraphe 3, du règlement 2018/1725 ne prévoit cette possibilité que dans **deux cas** de figure spécifiquement définis, à savoir si l'exactitude des données à caractère personnel est contestée par la personne concernée ou lorsque les données à caractère personnel doivent être conservées à des fins probatoires.
En conséquence, les autorités françaises tirent la conclusion que la référence à l'article 82 fait perdre de la souplesse aux dispositions actuelles.
Également, la France souhaite qu'une référence à la limitation du droit de rectification, de suppression et de restriction soit inscrite dans cet article en citant expressément l'article 82 (4) du règlement 1725) :

WK 757/2021 REV 6, Article 39

Article 39

Prior consultation

1. ~~AnyA~~Without prejudice to Article 90 of Regulation (EU) 2018/1725, any new type of processing operations to be carried out shall be subject to prior consultation of the EDPS where ~~:~~

~~(a) special categories of data as referred to in Article 30(2) are to be processed;~~

~~(b) the type of processing, in particular using new technologies, mechanisms or procedures, presents specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.~~

~~2. The prior consultation shall be carried out by the EDPS following receipt of a notification from the Data Protection Officer that shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards and security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of the data subjects and other persons concerned.~~

~~3. The EDPS shall deliver his or her opinion to the Management Board within two months following receipt of the notification. That period may be suspended until the EDPS has obtained any further information that he or she may have requested.~~

~~If the opinion has not been delivered after four months it shall be deemed to be favourable.~~

Commented [A22]: Tout d'abord, les autorités françaises relèvent que le régime actuel est particulièrement lourd pour Europol en ce qui concerne la consultation préalable du CEPD qui doit être réalisée en cas de « risque spécifique » soit pour l'ensemble de l'activité d'Europol comme a pu le relever le DPD de l'agence.
L'article 90 du règlement 1725 dispose que tout nouveau type d'opérations de traitement d'Europol doit faire l'objet d'une consultation préalable du CEPD « *lorsque le type de traitement, [...] présente des* ***risques élevés*** *pour les libertés et les droits des personnes concernées.* ».
Les autorités françaises saluent donc la plus grande souplesse du nouveau mécanisme présenté.

Toutefois, les autorités françaises estiment nécessaires d'étudier des pistes de réflexion pour davantage fluidifier la procédure et sous réserve d'un avis juridique de prévoir une régime d'urgence permettant au CEPD de valider ex-ante dans un certain délai les processus de traitement de l'information.

Les délais de mise en œuvre de la consultation préalable selon l'article 39 sont en moyenne de 4 mois. Ces délais ne sont pas compatibles avec les nécessités opérationnelles. Un exemple très concret a notamment été présenté récemment par Europol concernant un système de Machine learning nécessaire à l'analyse de l'ensemble des données saisies dans le cadre de l'opération EMMA (ENCROCHAT).

WK 757/2021 REV 6, Article 41

Article 41

Designation of the **Data Protection Officer**

1. The Management Board shall appoint a Data Protection Officer, who shall be a member of the staff~~.~~ specifically appointed for this purpose. In the performance of his or her duties, he or she shall act independently and may not receive any instructions.

2. The Data Protection Officer shall be selected on the basis of his or her personal and professional qualities and, in particular, the expert knowledge of data protection and practices and the ability to fulfil his or her tasks under this Regulation.

3. ~~It shall be ensured in that~~The selection of the Data Protection Officer shall not be liable to result in a~~that no~~ conflict of ~~interest~~interests ~~may result from the performance of~~between his or her duty as Data Protection Officer ~~in that capacity~~ and ~~from~~ any other official duties he or she may have, in particular in relation ~~those relating~~ to the application of this Regulation.

Commented [A23]: Tout d'abord, les autorités françaises font part de leur étonnement sur le fait que la Commission propose que le mandat du DPO soit renouvelable **sans limite de temps**. La délégation française à Europol rappelle fréquemment que la gestion des ressources humaines – y compris pour les postes à haute responsabilité – doit répondre à des règles strictes notamment sur l'octroi d'emplois à durée indéterminée.
Du point de vue des autorités françaises, et en l'état du statut du DPO, l'accord de l'EDPS suffit à garantir la transparence et le contrôle des décisions prises et à limiter les risques de conflit d'intérêt.
Si la Commission propose d'octroyer ce droit de démission au Directeur exécutif, les autorités françaises s'y opposent pour des raisons de conflit d'intérêts évidents.

WK 757/2021 REV 6, Article 41b

Article 41b

Tasks of the Data Protection Officer

1. The Data Protection Officer shall, in particular, have the following tasks with regard to processing of personal data:

(a) ensuring in an independent manner the compliance of Europol with the data

Commented [A24]: Les autorités françaises constatent que dans le cadre de ses missions le DPO pourrait être amené à veiller au respect par Europol des règles de l'Union mais également des **règles nationales** de protection des données. Les autorités françaises estiment que cette surveillance, lorsqu'il s'agit du droit national, doit se réaliser en étroite collaboration avec les autorités nationales de supervision.

WK 757/2021 REV 6, Article 43

Article 43

Supervision by the EDPS

1. The EDPS shall be responsible for monitoring and ensuring the application of the provisions of this Regulation and Regulation (EU) 2018/1725 relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by Europol, and for advising Europol and data subjects on all matters concerning the processing of personal data. To that end, he or she shall fulfil the duties set out in paragraph 2 and exercise the powers laid down in paragraph 3, while closely cooperating with the national supervisory authorities in accordance with Article 44.

Commented [A25]: Les autorités françaises s'étonnent de constater que les autorités nationales de supervision ne soient plus consultées lorsque le CEPD produit son rapport annuel sur ses activités de supervision de l'agence mais simplement invitées à produire des observations.

GERMANY

Germany's follow-up comments to the LEWP meeting on 7 May 2021: Revision of the Europol Regulation – Thematic blocs 1, 2, 3, 5, 6 and 7

Please find below Germany's written comments on the fifth revised version of the text of the Commission proposal (changes to the provisions pertaining to thematic blocs 1, 2, 3, 5, 6 and 7). Further comments may be raised following ongoing scrutiny of the proposal.

On a general note, we would like to reiterate our previous comments in expressing that Europol should continuously be present in the meetings. In our view, delegations would benefit from being able to seek Europol's expertise and advice in the ongoing discussions. Against the background that Europol is also continuously invited at Ministerial Council level, we do not see any reasons why the participation of an agency should not be possible nor any legal obstacles. We are confident that the legal framework allows for a satisfactory solution in the best interests of the Member States while taking due account of the concerns expressed by the Council Legal Service.

Thematic bloc 1: cooperation with private parties

Article 4(1)(m):

As stated before, the exact role of Europol with respect to the new TCO Regulation remains to be determined.

Therefore, Germany suggests to refer explicitly to the coordination of removal orders for terrorist content online by Member States authorities in accordance with Art. 14 of Regulation 2021/… [the TCO-Regulation], as this provision defines the supporting role of Europol regarding the taking down of terrorist content online.

Thus, Art. 4(1)(m) would read as follows:

> *"support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States and upon their request, the coordination of competent authorities' response to cyberattacks,* ***the coordination of removal orders for terrorist content online by Member States authorities in accordance with Art. 14 of Regulation 2021/… [the TCO-Regulation]*** *and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions.*

This amendment should be mirrored in the last sentence of recital 35 as follows:

> *Nothing in this Regulation should be understood as precluding the Member States* ***~~and Europol~~*** *from using removal orders as laid down in Regulation 2021/... on addressing the dissemination of terrorist content online as an instrument to address terrorist content online*

or making use of the coordinative and cooperative role of Europol in accordance with Art. 14 of the Regulation 2021/…, when member states issue such a removal order."

Moreover, the meaning of "cyberattacks" needs to be explained as this term is only used in this Article of the Europol Regulation without giving a definition. Is there a suitable definition of this term in Union law that the provision could refer to?

Article 26(6a) and Recital 31:

Germany welcomes the amendments to Article 26(6a) and to the corresponding Recital 31. Nevertheless, it should be specified more clearly that there is no legal obligation for the Member States and for the private parties concerned to comply with requests made by Europol. While Member States, pursuant to Article 7(6)(a), shall supply Europol with the information necessary for it to fulfil its objectives, this provision does not imply any obligation for Member States to obtain information from private parties. Above all, Article 7(6)(a) does not imply such an obligation for private parties. Therefore, the following sentence should be added to the provision (or at least the corresponding Recital):

"This Article does not oblige neither Member States nor private parties to comply with a request made by Europol."

This applies mutatis mutandis also to Article 26a(5).

Article 26a:

In principle, Germany supports the addition of Article 26a(4a) as the new paragraph mirrors the provisions of Article 14(1) of the TCO Regulation in order to clarify the relation between the instruments covered by the TCO Regulation and the corresponding instruments of the Europol Regulation.

In our view, this amendment could be further enhanced by clarifying that it refers to all the actions covered by Article 26a because duplication of efforts should be avoided in relation to all these instruments. For the same reason, the new provision should be inserted in paragraph 5a instead of 4a.

Moreover, the new paragraph should refer to competent authorities within the meaning of Article 12 of the TCO Regulation in order to mirror more clearly the provision of Article 14(1) of the TCO Regulation that also deals with the coordination between the competent authorities (within the meaning of the TCO Regulation) and Europol.

Therefore, the new provision should read as follows:

> ***"5**a. Europol shall exchange information, coordinate and cooperate with competent authorities **within the meaning of Art. 12 Regulation XXX [TCO Regulation]** with regard to **the actions covered by** ~~this Article transmission or transfer of personal data to private parties under paragraphs 3 or 4 of~~ this Article, in particular to avoid duplication of effort, enhance coordination and avoid interference with investigations in different Member States.*

A reference to the instruments of the TCO Regulation and to the competent authorities within the meaning of Article 12 of the TCO Regulation, which have to cooperate with Europol in accordance with Article 14 TCO Regulation, should be included in the corresponding Recital 35a.

Recital 32:

The first sentence in Recital 32 as proposed by the Presidency needs to reflect the different ways of receiving data from private parties. Therefore, the text should be amended as follows:

> *"To ensure that Europol does not keep the data **~~received directly~~ obtained** from private parties **directly or via the Member States** longer than necessary …"*

Thematic bloc 2: enabling Europol to process large and complex datasets

Article 2(q):

The definition of "investigative case file" establishes various criteria to be satisfied by Member States, the EPPO or third countries (e.g. *"… is authorised to process…" or "…in accordance with procedural requirements and safeguards under applicable … law"*). As a result of the diverse legal regimes among Member States, Europol will not be in a position to verify in detail whether these criteria have been met. For the sake of legal certainty, the definition should therefore clarify that the obligation to meet these criteria lies on the aforementioned while Europol is not obliged to re-verify whether these criteria have been met.

Article 18(5):

Why was Article 18(2)(e) excluded from the scope of Article 18(5)? Article 18 establishes the regulatory model that the categories of personal data that may be processed for the purposes laid down in Article 18(2) are specified in Annex II. If differences between the purposes arise, these disparities are also addressed in Annex II, as the Annex distinguishes between different purposes of

Article 18(2). Why does the proposal not follow this regulatory model, when it comes to research and innovation activities?

Article 18(5a)

The second sentence concerns the establishment of further conditions related to the processing under the first sentence. A similar provision can be found in the second sentence of paragraph 6, whereby the latter refers not only to "conditions relating to the processing of such data", but more specifically to "conditions relating to the processing of such data, in particular with respect to access and use of the data, as well as time limits for the storage and deletion of the data". Is there a reason why there is no complete alignment between these provisions

As the processing powers only serve the purpose of determining compliance with paragraph 5, why does the first sentence of the third subparagraph ~~sentence~~ refer to "where necessary for the purpose of this Article"? This should read as follows:

> *"Europol may only process personal data pursuant to this paragraph for a maximum period of one year, or in justified cases for a longer period with the prior authorisation of the EDPS, where necessary for the purpose of this* ***~~Article~~ paragraph****".*

The second sentence of the third subparagraph sets out that in the event of deletion of the data, Europol shall inform the provider of the data accordingly. This obligation does not make sense in cases where Europol has retrieved the information from publicly accessible sources including the Internet pursuant to Article 17(2). Therefore, the obligation to inform the provider should expressly exclude Article 17(2) instead of referring to the "relevant" cases (as proposed by the Presidency in the current version).

Article 18a(1):

Germany welcomes that the legislative proposal addresses this very important issue. As we all know, it has become urgent to address Europol's ability to process big data in accordance with relevant data protection principles since the EDPS' decision on the big data challenge. As the Ministers have expressed in their Declaration on the Future of Europol, it is of key importance to Member States that Europol will be able to continue to support Member States in this regard.

We support the fundamental approach of the proposal and generally agree with the provisions brought forward. At the same time, the processing of large and complex datasets (beyond the limitations of Art. 18(5) and Annex II) raises questions concerning data protection and fundamental rights and must strictly be limited to what is necessary and proportionate to achieve the objectives covered by Europol's mandate. Yet, the proposals of Article 18(5a) and Article 18a address part of the new operational reality. In order to ensure that Europol can continue to fulfil its tasks to the benefit of national law enforcement authorities, it is important to clarify that the processing of data under Article 18(5a) and Article 18a – of course in full compliance with the strict data protection

safeguards applicable – is as valid a possibility as the other processing purposes provided for in Article 18.

Regarding point (b), it is not clear what the test behind *„that it is not possible“* entails. Does this mean technical impossibility? Would Europol have to arrange that the *„case file“* is processed in a way that categories of personal data that do not comply with the requirements of Article 18(5) are filtered out to the greatest extent possible? Will processing be permissible on a provisional basis then?

The new insertion in Article 18a(1)(a) proposed by the Presidency aims at opening the scope of this Article to the purposes referred to in Article 18(2)(a). This aim is in line with calls from our national law enforcement authorities for support in the area of preventing crime. However, the proposed amendment raises several questions that should be addressed:

- Apart from the new addition, the wording of the whole Article remains focused on "investigative case files" (which refer to datasets "that a Member State, the EPPO or a third country acquired in the context of an on-going criminal investigation") and their "operational analysis" (which refers to Art. 18(2)(c)). Therefore, Germany proposes to revise the wording in order to better clarify which conditions would apply to the newly inserted option. *"Exceptional and duly justified cases"* alone is not an appropriate criterion.
- As EPPO is not competent for the prevention of crime, EPPO could at most request an additional analyses pursuant to Article 18(2)(a)(i). Nevertheless, Article 18a(1) concerns the general question of cooperation between Europol and EPPO. From our point of view, it does not make sense to deal with individual aspects of this topic outside the context of the underlying general issue. May we therefore suggest that all questions related to the EPPO be dealt with comprehensively in the context of thematic bloc 6.

Article 18a(4):

The part after *„with which ...“* could be aligned with the order used in Article 25(1).

The relationship of the third sentence (*"Europol shall verify .."*) and the fourth sentence (*"Where Europol ..."*) remains unclear. If the processing is already prohibited where preliminary indications of disproportionality or fundamental rights violations exist, the higher threshold in the former sentence may be unnecessary. If this was the case, both sentences could be combined into one sentence along the requirements in what is now the latter sentence.

The last sentence should read *"... be processed by Europol where necessary **and proportionate**..."*.

Thematic bloc 3: research and innovation

Article 18(2)(e):

Article 18(2) aims at realizing the principle of purpose limitation, according to which the purposes for the processing of personal data shall be specified. Could the provision indicate more specifically the purposes for which data may be processed in the context of research and innovation? For example, the text could stay closer to the Commission's proposal by amending the original wording as follows:

*"research and innovation regarding matters covered by this Regulation**, in particular** for the development, training, testing and validation of algorithms **and** for the development of **other** tools **relevant to achieve the objectives set out in Article 3.**"*

Article 33a(4):

Germany supports the general idea of Article 33a. Nevertheless, as we highlighted before, we think it is important that national authorities can safeguard their interests as "data owners". We therefore welcome the Presidency's intention to amend Article 33 with a view to preserving the interests of the provider of the information ("principle of data ownership").

However, the Presidency's latest proposal is still under discussion within the Federal Government. In this context, we also would like to hear from Europol whether from a practical point of view, the mandatory consultation of the Management Board would be a feasible approach to involve the Member States concerned."

Recital 39:

Germany welcomes that Article 33a(2) was moved to Recital 39. Besides, we would like to ask to delete the word "personal" as some of the categories mentioned are not "personal data".

Therefore, the sentence should be amended as follows:

"*Preference should be given to using synthetic, pseudonymized and/or anonymized **~~personal~~** data.*"

Thematic bloc 5: cooperation with third countries

Article 25(1), (4a) and corresponding Recitals:

Germany welcomes the revision of Article 25 in line with our previous comments. However, as we mentioned before, the amendment to Article 25 must be reflected accordingly in all other provisions that refer to the possibilities for structural exchanges of personal data with third countries foreseen by Article 25. This applies in particular to Articles 18a(4), 26(1)(c), 26(4), 26(6), 26a(2), 26a(4), 27(1)(c) and 27(2).

By way of example, Article 18a(4) should be amended as follows:

*"Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision**, or in the absence of such a***

decision, where appropriate safeguards have been provided for or exist, *as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports."*

Furthermore, the revision of Article 25 must be reflected in the corresponding Recitals, in particular Recital 24. Inspiration could be sought from Recital 51 of the Eurojust Regulation. Germany will shortly submit a proposal for wording.

Article 25(8):

Germany does not object to the current proposal of making available certain information to the EDPS. Nevertheless, Germany would appreciate an explanation why the former paragraph 8 was deleted.

Thematic bloc 6: strengthening Europol's cooperation with the EPPO

Germany thanks the Presidency once again for addressing some of our concerns in Article 20a(2). Nonetheless, we still hold the view that the cooperation between Europol and the EPPO should be limited to the extent that is already foreseen by the EPPO Regulation, notably Article 102 thereof. We see no need and no possibility to extend the cooperation beyond this. According to the wording of Article 20a as proposed in Rev6 this means in detail:

- Article 20a (2): We are still in favour of the deletion of the words "and cooperate with it, in particular". However, in a spirit of compromise we would also except the Presidency's proposal under the condition that the words "in particular" will be deleted. It has to be clear that the cooperation pursuant to Article 4(1)(j) can only go as far as foreseen in the legal mandate of Europol or the EPPO. Yet, EPPO Regulation demonstrated a clear intention by the co-legislator to limit the cooperation to providing information and analytical support to a specific investigation conducted by the EPPO.
- Regarding Article 20a(3), we maintain our doubts that the proposed hit/no-hit mechanism is in line with the EPPO Regulation also in regards of the new version as set out in Rev6 Article 102 of the EPPO Regulation does not provide for such mechanism in relation to Europol at all. The restriction by the words "in its mandate" is therefore not sufficient. This restriction would only make sense if the EPPO-Regulation provided in principal a regulation that would allow a hit/no-hit mechanism for Europol as this is the case for Eurojust and OLAF in Article 100(3) and Article 101(5) but is not the case for Europol. This indicates the clear intention of the legislator that there should be no hit/no-hit mechanism for Europol. Furthermore, we would like to point out the legal concerns raised by the Council Legal Service. In that context, we welcome the clarification in the Commission's non-paper on Article 20a that the proposed hit/no-hit mechanism does not stem from a legal obligation arising from the EPPO Regulation, but is rather a political choice by the Commission which goes beyond the mere mirroring of the EPPO Regulation.
- Regarding Article 20a(4) it is important that Europol can only share information with the EPPO if the Member State, Union body, third country or international organisation that provided the information has given its prior consent, in order to avoid national investigations being jeopardised or sensitive information being disclosed. We would like to highlight that

Europol's cooperation with Eurojust, OLAF and EBCG follows this principle (as stipulated in Article 21(1) and (1a)). Against this background it is not enough to notify the Member State concerned without delay. It should rather be clarified that the information shall not be shared without an explicit authorisation by the provider as suggested earlier by Germany.

In order to address our comments, we would like to suggest that Article 20a be re-worded altogether as follows (changes compared to the current text proposal of Article 20a in document WK 757/2021 REV 5):

"Article 20a

Relations with the European Public Prosecutor's Office

1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation.

2. Upon request by the EPPO in accordance with Article 102 of Regulation (EU) 2017/1939, Europol shall support the investigations of the EPPO and cooperate with it ~~***, in particular through exchanges of information and***~~ *by providing* ***information and*** *analytical support.*

~~***3. Europol shall take all appropriate measures to enable the EPPO to have indirect access, within its mandate, to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system, without prejudice to any restrictions indicated in accordance with Article 19(2) by the Member State, Union body, third country or international organisation which provided the information in question. Article 21 shall apply mutatis mutandis with the exception of its paragraphs 2 and 8.***~~

3. ~~***4.***~~ *Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence in accordance with Article 22, Article 25(2) and (3) of Regulation (EU) 2017/1939.*

4. If the information referred to in paragraphs 2 and 3 is subject to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2) of this Regulation, Europol shall consult with the provider of the information stipulating the restriction and seek its authorisation for sharing.

In such a case, the information shall not be shared without an explicit authorisation by the provider.*"*

Thematic bloc 7: ability to request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

Germany welcomes the deletion of the proposed Recital 14. In order to avoid any doubt that Article 6 only applies to cross-border cases, Recital 11 of the current Europol Regulation should be retained.

Recital 11 of the current Europol Regulation reads as follows:

> *"(11) Europol should be able to request Member States to initiate, conduct or coordinate criminal investigations in specific cases where cross-border cooperation would add value. Europol should inform Eurojust of such requests."*

We therefore agree to provisionally close thematic block 7 on the condition that Recital 11 of the current Europol Regulation is retained.

NETHERLANDS

Europol Regulation

Comments the Netherlands LEWP 18 May 2021

We would again like to enter a scrutiny reservation on the proposed changes, since we have not been able to study and discuss them properly.

Block 1: Enabling Europol to cooperate effectively with private parties

Article 4 para 1 subpara m:

We would like to support the suggestion by our Luxembourg colleagues that the word "cyberattacks" is changed to "cybercrime":

> "support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States **and upon their request**, the ~~coordination of~~ **assistance to** ~~la~~w enforcement **competent** authorities' response to cybercrime ~~cyberattacks~~, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;" -

Article 26 para 2:

Thank you for deleting the word "automatically".

Article 26a

- Thank you for taking on board our suggestions for including a new recital 35a and a new paragraph 4a in article 26a to avoid duplication of efforts by Europol and MS.

- After listening to the discussion during the meeting on 18 May, we can support the following changes to the text (in blue):

Recital 35a:

In order to avoid duplication of effort and possible interferences with investigations and to minimise the burden to the hosting service providers affected, Europol should assist, exchange information~~,~~ ~~coordinate~~ and cooperate with the competent authorities with regard to ~~before~~ transmitting or transferring personal data to private parties to prevent the dissemination of online content related to terrorism or violent extremism. Where Europol is informed by a competent authority of a Member State of an existing transmission or transfer, it should not transmit or transfer personal data concerning the same subject matter.

Article 26a para 4a: Europol shall assist, exchange information~~, coordinate~~ and cooperate with the competent authorities with regard to the transmission or transfer of personal data to private parties under paragraphs 3 or 4 of this Article, in particular to avoid duplication of effort, enhance coordination and avoid interference with investigations in different Member States.

Art 51 para 3 sub f:

In order to avoid the risk that the EP might think that art 51 para 3 sub f refers to a different report than art 26 para 11, maybe a reference to art 26 para 11 could be included here?

Block 2: Enabling Europol to process large and complex datasets

Article 2 sub q / article 18a para 1 sub a:

We think that a single Member State should be able to provide Europol with an investigative case file. If the file relates to serious crime, the crime should of course affect two or more Member States, but that does not mean that the file also needs to be submitted by two or more MS.

Article 18 para 5a

- Would it be possible to receive the presentation that Europol gave in the LEWP of 7 May?

- The last time we discussed this block, the Commission tried to explain the different possible steps in some possible scenarios. Because of the complexity of article 18 para 5a and article 18a, it would really help us it if the Commission could visualise for us how the different steps of processing large datasets and the stipulations in these articles relate to each other by providing us with some more detailed flow charts.

- Since the data being processed under article 18 para 5a could contain data that falls outside the categories of data subjects listed in Annex II, we think it might be a good idea to ensure that this data is also functionally separated. We would like to know what Europol thinks of this idea. If it does not create major practical problems, we would like to suggest adding the following sentence to this paragraph:

> "This personal data shall be functionally separated from other data."

- Regarding the text that has been added (or moved): "and where necessary for Europol for the purpose of determining whether personal data complies with the requirements of paragraph 5 of this Article" are the words "for Europol" really necessary here? It continues with: "Europol may temporarily process", so it is already clear that this applies to Europol. Maybe the words "for Europol" could be deleted.

> *"5a. Prior to the processing of data under paragraph 2 of this Article, and where necessary ~~for Europol~~ for the purpose of determining whether personal data complies with the requirements of paragraph 5 of this Article, Europol may temporarily process […]"*

Article 18 para 5a and article 18a para 1:

- We think it would be a good idea for Europol to develop some guidelines for the Member States on how to provide large datasets to Europol, to ensure some uniformity in the way this is done. The

guidelines could describe how law enforcement agencies should determine the purpose of the processing and whether the processing is necessary and proportionate. This is of course subject to the differences in the way the Law Enforcement Directive has been implemented by MS.

- In order to achieve this, maybe when the Management Board further specifies the conditions for the processing of non-annex II data under art 18 para 5a and art 18a, this should also include the conditions under which the data can be provided to Europol. So maybe the text of the second section of both art 18 para 5a and of art 18a para 2 could be changed into:

> "The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the provision and processing of such data."

Article 18a para 1

- If we heard this correctly, the Commission said that you can legally do more with annex II-data than with non-annex II data. However, in article 18a para 2 it says that Europol may process personal data contained in an investigative case file in accordance with article 18 para 2, i.e. it can apply all forms of processing to these data. So does the Commission in fact mean that you can legally do the same with both annex II and non-annex II data, but that the circumstances in which you can process the non-annex II data are more limited than the circumstances in which you can process annex II data?

- If we also heard this correctly, the Commission also said that article 18 para 5a could be used for ad hoc requests for support, but is that not the next step, since 18(5a) is only intended for determining whether the data comply with annex II? Will the actual processing of the information in response to such an ad hoc request for support not take place under article 18 para 2, once the data has been minimised so that it only includes annex II data?

Article 18a para 3

- The first and second section of para 3, especially the last parts, are very similar. The different uses of the word "related" may cause some confusion:

> - in the first section, the word "related" is used to indicate the connection between judicial proceedings and a criminal investigation:
>
> > "and only for as long as the judicial proceedings related to that criminal investigation are on-going in that Member State."
>
> - in the second section, however, the word "following" is used to indicate the connection between judicial proceedings and a criminal investigation and the word "related" instead refers to the connection between the original investigation and the other investigation:
>
> > "and only for as long as judicial proceedings following a related criminal investigation are on-going in that another Member State."

- In order to prevent confusion, we would like to suggest clarifying the text of the first section by replacing "related to" by "concerning". This way, the word "related" will only refer to the connection between the original and the other investigation:

"3. Upon request of the Member State or the EPPO that provided an investigative case file to Europol pursuant to paragraph 1, Europol may store that investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings ~~related to~~ concerning that criminal investigation are on-going in that Member State."

- And if we want to be completely consistent, we could consider replacing the word "following" in the second section by "concerning" too. "Following" could be read to mean that the judicial proceedings come after the criminal investigation in time, whereas "concerning" would more clearly indicate that the judicial proceedings are based on the criminal investigation:

"That Member State, or, with its agreement, another Member State in which judicial proceedings are ongoing with respect to a related criminal investigation, may also request Europol to store the investigative case file and the outcome of its operational analysis beyond the storage period set out in paragraph 2 for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings following (or concerning?) a related criminal investigation are on-going in that other Member State."

Article 18a para 4

- We would like to propose removing the obligation from para 4 to inform the EDPS. The EDPS already has access to all information at Europol. And if the processing will form part of a new filing system which for example involves a high risk to the rights and freedoms of data subjects, the prior consultation mechanism as defined in article 39 Europol Regulation and article 90 EUDPR has to be followed. Moreover, these investigative case files will be from third countries with which there is a cooperation agreement or that are the subject of an adequacy decision. Informing the EDPS about receiving an investigative case file from a third country would mean involving the EDPS too much in Europol's operational work. This is not in keeping with its supervisory role. We believe there are sufficient safeguards in place to process these investigative case files and it is not necessary to add more. We would therefore like to propose the following change (in blue):

Paragraphs 1 to 3 shall also apply where Europol receives personal data from a third country with which there is an agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA in accordance with point (c) of Article 25(1) of this Regulation or on the basis of Article 218 TFEU in accordance with point (b) of Article 25(1) of this Regulation, or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, and such third country provides an investigative case file to Europol for operational analysis that supports the specific criminal investigation in a Member State or in Member States that Europol supports. ~~Where a third country provides an investigative case file to Europol, the EDPS shall be informed.~~ Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental

rights. Where Europol~~, or the EDPS,~~ reaches the conclusion that there are preliminary indications that such data is disproportionate or collected in violation of fundamental rights, Europol shall not process it. Data processed pursuant to this paragraph may only be accessed by Europol where necessary for the support of the specific criminal investigation in a Member State or in Member States. It shall be shared only within the Union.

- Regarding the third part of this paragraph about violation of fundamental rights, we are wondering about some differences between the second and third sentence. The second sentence mentions "objective elements" indicating a "manifest violation of fundamental rights". But the third sentence talks about "preliminary indications" of a "violation of fundamental rights". Why the difference?

- "Preliminary" sounds as if this will not be the last step in the process. Why is the word "preliminary" there? Does this mean that after Europol has found indications of a violation of fundamental rights and stops to process the data, it can continue to examine the possible violation of fundamental rights? Could it come to a different conclusion later and start processing the data again?

- And why is the word "manifest" missing from the third sentence? This sounds like a lower threshold for the violations. Shouldn't the third sentence also talk about "manifest violations of fundamental rights"?

Block 3: Strengthening Europol's role on research and innovation

Article 33a

- Thank you for taking on board our concerns regarding the new paragraph 4, which would have allowed Europol to use all data provided by MS for research and information.

- The Netherlands very much supports a strong role for Europol in the area of research and innovation. This is for example why we have taken on the role of deputy chair of the Clearing Board of the Europol Innovation Lab.

- We understand that Europol needs to use information in order to be able to carry out innovation projects and want to make sure that it can do so.

- However, as we explained before, we believe that the ownership principle provides the trust that Europol is built on and it should also be respected when data is used for research and innovation.

- We believe the new text is an improvement on the previous version.

- We have some doubts, however, about the level at which the decisions on the use of data for research and innovation will be taken. In our proposal, we suggested to say that the Member States involved would have to authorise the projects plans. We chose to say Member States and not Management Board and to include this in para 1 subpara a and not subpara b on purpose, since we are not sure whether it is necessary for the Management Board to approve the use of data for research and innovation. This is quite an operational task and we think this is something that for example the National Units could do.

- To ensure that Member States can authorise the use of their data at a more operational level, we would like to reiterate our proposal to add “and the Member States involved” to article 33a para 1 sub a:

> “any project shall be subject to prior authorisation by the Executive Director and the Member States involved, based on a description of the envisaged processing activity setting out the necessity to process personal data, such as for exploring and testing innovative ~~new~~ **technological** solutions and ensuring accuracy of the project results, a description of the personal data to be processed, a description of the retention period and conditions for access to the personal data, a data protection impact assessment of the risks to all rights and freedoms of data subjects, including of any bias in the outcome, and the measures envisaged to address those risks;”

- Since this would mean that the MB would not need to be involved in every innovation project to approve the use of data, we would like to propose changing the text of article 33a para 1 sub b back to the previous version, so that the MB is again consulted on some but not all of the innovation projects:

> “~~the Management Board and~~ the EDPS shall be informed prior to the launch of the project; the Management Board shall be either consulted or informed prior to the launch of the project, in accordance with criteria laid down in the guidelines referred to in article 18(7);”

- Our second comment is that the current proposal is based on an opt out system, but we think that a system where Member States opt in to making their information available for research and innovation projects would be more in line with the ownership principle. We could realise this by changing the current text to provide for an opt in system where MS have to give permission for each innovation project. This would require making the following changes to article 33a para 4:

> “Where the requirements of paragraph 1 are fulfilled, and ~~by way of derogation from Article 19(1)~~ if authorised so to do so by the provider of the information, Europol may process personal data that has been processed for the purposes referred to in points (a) to (d) of Article 18(2) also for the purpose of Article 18(2)(e). In the context of the ~~consultation of the Europol Management Board for~~ prior authorisation of a research and innovation project as referred to in point (~~b~~ a) of paragraph 1, a Member State may indicate that personal data it submitted to Europol in accordance with Article 19(1) ~~shall not~~ may be used for that project.”

This would also require a small change to recital 39. The last part of recital 39 would read:

"Europol should not process personal data for research and innovation without the agreement of the Member State that submitted the data to Europol. To that end, in the context of the prior authorisation of ~~a consultation of the Europol Management Board for~~ a research and innovation project, a Member State may indicate that all or part of the personal data it submitted to Europol ~~should not~~ may be used for that project."

- We would very much like to know what Europol thinks of this proposal.

- Our general comment that we should take into account the EDPS recommendation that "the scope of the research and innovation activities should be better defined" still stands. We could for example add the following sentence to the end of article 33a para 1:

"The scope of the research and innovation activities will be further defined in the guidelines referred to in Article 18(7)."

Block 5: Strengthening Europol's cooperation with third countries

Article 25 para 4a

We agree with the inclusion of the new para 4a in article 25. We agree with Germany that this could be interpreted more widely than has been suggested. For example, "legally binding instrument" could also refer to national legislation in a third country. We therefore support keeping the provisions on appropriate safeguards in the text.

Block 6: Strengthening Europol's cooperation with the EPPO

Overweging 22:

Thank you for including the word "indirect" in recital 22.

Article 20a para 4:

Thank you for taking on board our suggestion to add the text "without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2)." in para 4.

Block 7: Clarifying that Europol may request the initiation of an investigation of a crime affecting a common interest covered by a Union policy

We can agree with closing block 7.

POLAND

With reference to the last VTC LEWP (18/05/2021), please find attached PL comments on block 2 and 6 of Europol regulation

Block 2 – large and complex data sets

Art. 18a (4)

In the light of the discussion and explanation received from the Commission and Europol on the 18 May LEWP VTC, **PL suggest deleting the whole third sentence of the article: "*Europol shall verify that the amount of personal data is not manifestly disproportionate in relation to the specific investigation in a Member State that Europol supports, and that there are no objective elements indicating that the case file has been obtained by the third country in manifest violation of fundamental rights"* and replace it with the sentence: *"Each time the data should be transferred in accordance with provisions contained in art. 23, par. 5, 8 and 9.*** The proposed amendment will allow to avoid duplication of the safeguards included in the text.

Block 6 – EPPO

Bearing in mind the current wording of new art. 20a as well as new art. 24, and included references to art. 19 (2) in these provisions, Poland suggests adding the word "transmission" in the first sentence of art. 19 (2), as follows:

"Member States, Union bodies, third countries and international organization may indicate, at the moment of providing information to Europol, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its transfer, **transmission,** erasure or destruction. Where the need for such restrictions becomes apparent after the information has been provided, they shall inform Europol accordingly. Europol shall comply with such restrictions."

The abovementioned amendment is in line with the wording of recital 22 and will allow countries not participating in enhanced cooperation with the EPPO to fully secure the data transferred to Europol in the course of ongoing cases.

ROMANIA

ROMANIAN WRITTEN COMMENTS

-FOLLOW-UP LEWP on 18 May 2021 -

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

- Examination of the proposal regarding thematic blocks 1, 2, 3, 5, 6 and 7

- **RO reiterates previous written comments on Art. 26 (6a) şi 26a (5)**, respectively:

Clarifications are needed on the situations in which Europol may request personal data from private parties through national units the type of data requested and their content.

The private parties are, as a rule, subject to national legislation on the protection of personal data, so the responses to Europol's requests should be voluntary both for private parties and MS authorities.

Thus, Europol's request should not be mandatory, but follow the means of communication regulated at national level, in the sense that it is made through the national competent authorities.

Consequently, for an unequivocal understanding, we consider necessary that the safeguards with regard to the principles in the matter of the jurisdiction of the states, judicial cooperation and protection of human rights and protection of personal data should be highlighted.

Furthermore, similar positions (doc. 5527/7/21 REV 7) have been sent by DE (pg 95), CZ (pg 119), NL (pg 163), ES (pg 169).

- **Art. 26 (6a).** For clarity of the text, it is necessary to be review ***„ (for the purpose)….with the view to identifying the national units concerned".***

Europol may request Member States, via their national units, *to obtain personal data from private parties, which are established or have a legal representative in their territory, in accordance with their national laws,* ***for the purpose*** *of sharing it with Europol, on the condition that the requested personal data is strictly limited to what is necessary for Europol with a view* ***to identifying the national units concerned****.*

Recital 35 (a) and art. 26a (4a). For reasons of legal clarity, we consider it opportune to delete the term *coordinated* as the cooperation with Europol must be carried out in accordance with the national legislative regulations as well as with those in the field of judicial cooperation in criminal matters.

- **Art. 33a (b).** We appreciate the changes.

- **Art. 33a (1) (g).** Additional clarification is needed on the extension of the log retention period from 1 year to 2 years.

- **Art. 33a (4). As a compromise between our views on this subject, we can support the wording at the end of paragraph 4, as it is possible for the MS to refuse the use by Europol of personal data previously transmitted in a research / innovation project.**

SPAIN

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
BLOCK 1			
• **RECITAL 35a**		It should be clarify how avoid this duplication and the problem of interference or duplication and the procedure to detect already existing transmissions or transfers. In any case, this recital should be consistent with the articles of the block.	
• **Article 4(1)(m) [amended]**			***(m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States and upon their request, the coordination of law enforcement competent authorities' response to cyberattacks, the taking down of terrorist content online, and the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions;;***

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
• Article 4(1)(u) [new]			
• Article 18(2)(d) [amended]	Se debería considerar la posiblidad de que los estados miembros se dirijan a las partes implicadas cuando estas se encuentren en sus estados	Consideration should be given to the possibility for member states to address the parties involved when they are in their states.	***facilitating the exchange of information between Member States, Europol, other Union bodies, third countries, and international organisations and private parties;***
26,6a	Se debería incluir la posición de la delegación sobre la posibilidad de rehusar por los estados miembros	The delegation's position on the possibility of refusal by member states should be included.	***With regard to points (a), and (b) and (d) of paragraph 5 of this Article, if the private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, the transfer shall only be authorised by the Executive Director if the transfer is: (a) necessary in order to protect the vital interests of the data subject or another person; or***
26, 6b		Already clarify. In case this exchange falls outside the scope of the objetives of Europol, this exchange, should be inititated by initiative of the Member Estate interested.	
BLOCK 2			
2q	Parece razonable que los estados miembros, el EPPO y terceros estados puedan	It seems reasonable that EPPO, member states and third states can enter data	***(q) 'investigative case file' means a dataset or multiple datasets that a Member State, the***

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
	introducir datos que se consideren de interés. Convendría aclaración sobre la implementación de este último punto.	that are considered to be of interest. Clarification on the implementation of this last point would be welcome.	***EPPO or a third country acquired in the context of an on-going criminal investigation, in accordance with procedural requirements and safeguards under the applicable national criminal law, and submitted to Europol in support of that criminal investigation.***
18. 5	El texto: "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II." debería decir "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II."	The text: "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II." should be modified as follows: "Without prejudice to Article 8(4) and Article 18a, categories of personal data and categories of subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II."	***CWithout prejudice to Article 8(4) and Article 18a, categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in points (a) to (d) and (f) of paragraph 2 are listed in Annex II.***
18. 5a	No hay comentarios. Se considera adecuado	No comments. It is considered appropriate	***5a. Prior to the processing of data under paragraph 2 of this Article, Europol may temporarily process personal data received pursuant to Article 17(1) and (2) for the purpose of determining whether such data comply with the requirements of paragraph 5 of this Article, including by checking the data against all data that Europol already processes in accordance with paragraph 5.***
18a	Se entiende que los datos obtenibles públicamente se	It is understood that publicly available data may be	***Páginas 20-21 del doc. Wk00757***

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
	podrán tratar, aún no siendo de los del Anexo II. Se propone aclarar este punto.	processed, even if they are not Annex II data. It is proposed to clarify this point.	
BLOQUE 3			
18.2 e	Se debería elevar consulta al EDPS sobre el uso de datos personales y valorar la normativa de protección de datos de los Estados miembros.	EDPS should be consulted on the use of personal data and Member States' data protection authorities should make a revision of this article as well.	
4.1t	**se considera adecuado PERO DEBERÍA PRIORIZARSE EL USO DE DATOS SINTÉTICOS**	is considered appropriate BUT PRIORITY SHOULD BE GIVEN TO THE USE OF SYNTHETIC DATA	***(t) proactively monitor and contribute to research and innovation activities relevant to achieve the objectives set out in Article 3, support related activities of Member States,implement its research and innovation activities regarding matters covered by this Regulation, including in the development, training, testing and validation of algorithms for the development of tools, and contribute to the coordination of activities of Union agencies established on the basis of Title V of the TFEU in the field of research and innovation within their mandates in close cooperation with Member States;***
4.4a	**Se considera apropiado**	It is considered appropriate	***4a. Europol shall assist the Commission in identifying key research themes, drawing up and implementing the Union framework programmes for research and innovation activities that are relevant to achieve the objectives set out in Article 3. When Europol assists the Commission in identifying key research themes, drawing up and implementing a Union framework programme, the***

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
			Agency shall not receive funding from that programme.
DELETED 4.4b	**Se debería definir con más detalle la labor de apoyo de Europol**	Europol's supporting role should be further defined.	***4b. Europol shall support the screening of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council2 that concern undertakings providing technologies used or being developed by Europol or by Member States for the prevention and investigation of crimes covered by Article 3 on the expected implications for security.***
33a	Se debería elevar consulta al EDPS sobre el uso de datos personales y valorar la normativa de protección de datos de los Estados miembros. En cualquier caso, debería priorizarse el uso de datos sintéticos , siempre que sea posible.	EDPS should be consulted on the use of personal data and the data protection regulations of the Member States should be assessed. In any case, the use of synthetic data should be prioritised whenever possible.	***Processing of personal data for research and innovation***
BLOCK 4			
article	**COMENTARIO DELEGACIÓN ESPAÑOLA**	**SPANISH DELEGATION COMMENTS**	***texto***
4,1 r	Nuestra posición pasa por solicitar la eliminación del artículo tratado, justificando esto en base a los comentarios hechos durante las reuniones anteriores y escritos presentados por esta delegación. Se considera que Europol no debe insertar alertas en SIS. Entendemos que la grabación	SPAIN-LEWP Our position is to request the article's deletion in question, justifying this on comments made during previous meetings and written submissions by this delegation. This delegation don´t support the insertion of alerts in SIS by Europol.	***enter data into the Schengen Information System, in accordance with Regulation (EU) 2018/1862 of the European Parliament and of the Council, following consultation with the Member States in accordance with Article 7 of this Regulation, and under authorisation by the Europol Executive Director, on the suspected involvement of a third country national in an offence in respect of which***

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
	de alertas en SIS por parte de Europol no es una solución adecuada o que suponga una mejora para los frontline officers que no pueda ser obtenida por otros medios que consideramos más adecuados. Aunque España está comprometida en la lucha contra el terrorismo y la delincuencia grave creemos que la grabación en SIS, aún cuando no suponga medidas coercitivas, no aporta otro beneficio que el de llevar un control de paso por un punto; si el individuo marcado es de interés para los estados miembros, serán ellos mismos los que se encarguen de realizar la grabación correspondiente y además podrán proporcionar a los frontline officers una base legal más sólida más llevar a cabo vigilancias discretas o la medida que corresponda. En caso de que no exista nada más sobre el individuo a controlar que el dato proporcionado por un país tercero, la utilidad del seguimiento sólo puede ser para ese país; hasta que se produzca un evento o circunstancia que haga de interés al individuo para el estado miembro. Dado que se está tratando de valorar si la propuesta supone una mejora se observa que:	We understand that the recording of alerts in SIS by Europol is not an adequate solution or an improvement for frontline officers that could not be obtained by other means that we consider more appropriate. Although Spain is committed to the fight against terrorism and serious crime, we believe that EUROPOL should not record in SIS. Even if it does not imply coercive measures, it only provides identification in a concrete location. If the individual is of interest to the Member States, they would record the alert and give frontline officers a more solid legal basis to take any necessary measure. In case there is nothing more about the individual to be monitored than the data provided by a third country, the usefulness of the monitoring it's just for that country; until there is another circumstance that makes the individual of interest to the member state. Given that an attempt is being made to assess whether the proposal is an improvement, it is noted that: ● The alternatives presented by the delegations do not seem to be good enough as the SIS recording option, but from a practical point of view, it only brings the	***Europol is competent and of which it is aware on the basis of information received from third countries or international organisations within the meaning of Article 17(1)(b);***

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
	● Las alternativas presentadas por las delegaciones no parecen ser lo suficientemente buenas pero la opción de grabación en el SIS, desde el punto de vista práctico, sólo aporta la posibilidad de realizar un chequeo discreto y tomar otras medidas en caso de que se den circunstancias más allá de la alerta. ● Aunque se razona en algunos de los escritos presentados que esta grabación va más allá de la alternativa de grabación en EIS que dicen tener sólo fines de investigación, la grabación en SIS en estos términos no aporta operatividad ni una posibilidad evidente de actuar más allá de estos fines investigativos. ● En caso de un HIT, puede que los agentes se vean inducidos a tomar alguna medida inapropiada cuando no existe una base legal sólida para ello. ● Sin aportar nada distinto a otras herramientas, se puede crear ruido o distorsión de la información para los frontline officers. ● El beneficiario más evidente es el país que facilitó la información para grabar la alerta no los estados miembros. Aunque estos pudiesen beneficiarse también, lo harían a raíz de circunstancias al margen de que la grabación se haga por parte de Europol.	possibility to perform a discreet check and take further action in case of circumstances beyond the alert. ● Although it is reasoned in some of the submissions that this recording goes beyond the alternative of recording in EIS that claim to be for investigative purposes only, recording in SIS in these terms does not provide operationally or an obvious possibility to act beyond these investigative purposes. ● In the case of a HIT, officers could be induced to take some inappropriate action when there is no sound legal basis for doing so. ● Without providing anything different from other tools, it could create noise or distortion of information for frontline officers. ● The most obvious beneficiary is the country that provides the information to record the alert, not the member states. Even if they could also benefit, they would do so due to circumstances other than the fact that Europol does the recording on SIS. As a reply to some technical aspects provided in the document: WK 3974/2021 REV 1 Regarding access to actionable information and interoperability: In Spain's	

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
	Desde un punto de vista más técnico y replicando a las respuestas aportadas en el documento: WK 3974/2021 REV 1 ● Respecto al acceso a la actionable information e interoperabilidad: En el caso de España, sería claro para los frontline officers y no daría lugar a interpretaciones erróneas. ● Respecto a la no inclusión del multiple identity detector (MID): Sería contradictorio grabar datos en el SIS y que no haya proceso de búsqueda en el MID. En este caso, se consideraría más conveniente la grabación en EIS. CONCLUSIÓN Y RESPUESTA A LA COMPROMISE SUGGESTION DE LA PRESIDENCIA En respuesta a "In the spirit of compromise, could you support the wording proposed by the Presidency, and if so, could you indicate which of the square brackets should be used/left out?" Aunque la respuesta de esta delegación es que NO es posible apoyar la redacción propuesta; Relativo a los brackets 1. Entendemos que las grabaciones en SIS deben hacerse por o para los estados miembros y por tanto con autorización de al menos	case, this would be clear for frontline officers and would not give rise to misinterpretation. Regarding the non-inclusion of the multiple identity detector (MID): It would be contradictory to record data in the SIS and make no search process in the MID. In this case, recording in EIS would be considered more appropriate. CONCLUSION AND RESPONSE TO THE PRESIDENCY'S COMPROMISE SUGGESTION In response to "In the spirit of compromise, could you support the wording proposed by the Presidency, and if so, could you indicate which of the square brackets should be used/left out?" Although the answer from this delegation is that it is NOT possible to support the wording proposed; Concerning the brackets: 1. We understand that SIS recordings must be made by or for member states and therefore with the authorisation of at least one of them. 2. brackets a/b: from a practical point of view, in addition to terrorism, serious crime should be included. Considering that these alerts would be recorded for terrorism reasons, in that case, the details of this article	

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
	uno de ellos. Se debería incluir. 2. brackets a/b: La finalidad práctica implica que se incluyese, además de terrorismo, serious crime. No obstante, parece que la utilidad de esta grabación de Europol apunta limitarse a terrorismo; en ese caso, los pormenores de este artículo deberían ser debatidos en el grupo correspondiente tal y como se propuso en la pasada reunión del día 15 de abril. 3. La información que se grabe en SIS debe tener un origen confiable y que pueda ser validado por los estados miembros interesados. Se debería incluir.	should be discussed in the relevant group as proposed at the last meeting on 15 April. 3. The information to be recorded in SIS must have a reliable origin and should be validated by the member states concerned.	
BLOCK 5			
Article 25(5) [amended]		It is necessary to clarify the scope of the term "category of transfers". It was proposed to eliminate it from this article, indicating only the transmission of personal data "case by case", as the regulation itself states. It should be noted that this clarification is motivated by the fact that the inclusion of the term CATEGORY means adding the possibility of a massive authorization of transfers that can be included in the same group, so it is not considered incorrect. The included definition clarifies this point.	***By way of derogation from paragraph 1, the Executive Director may authorise the transfer or a category of transfers of personal data to third countries or international organisations on a case-by-case basis if the transfer is:***

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
BLOCK 6			
20 a		With respect to point 3, it was considered necessary to clarify the application of Article 21	***Article 20a Relations with the European Public Prosecutor's Office 1. Europol shall establish and maintain a close relationship with the European Public Prosecutor's Office (EPPO). In the framework of that relationship, Europol and the EPPO shall act within their respective mandate and competences. To that end, they shall conclude a working arrangement setting out the modalities of their cooperation. 2. Europol shall actively support the investigations and prosecutions of the EPPO and cooperate with it, in particular through exchanges of information and by providing analytical support. 3. Europol shall take all appropriate measures to enable the EPPO to have indirect access to information provided for the purposes of points (a), (b) and (c) of Article 18(2) on the basis of a hit/no hit system. Article 21 shall apply mutatis mutandis with the exception of its paragraph 2. 4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence***
BLOCK 7			
6.1	Se considera adecuado	It is considered appropriate	
BLOCK 8			
Article 28 [deleted]	En cuanto al artículo 28, se considera que los principios	Regarding Article 28, it is considered that data	***General data protection principles***

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
	de protección de datos deben incluirse en este bloque para garantizar la calidad de la protección de datos.	protection principles should be included in this block to ensure the quality of data protection.	***1. Personal data shall be:*** ***(a) processed fairly and lawfully;*** ***(b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing of personal data for historical, statistical or scientific research purposes shall not be considered incompatible provided that Europol provides appropriate safeguards, in particular to ensure that data are not processed for any other purposes;*** ***(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;*** ***(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;*** ***(e) kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed; and*** ***(f) processed in a manner that ensures appropriate security of personal data.*** ***2. Europol shall make publicly available a document setting out in an intelligible form the provisions regarding the processing of personal data and the means available for the exercise of the rights of data subjects.***
Article 30(2)	Con respecto al artículo 30, apartado 2, se considera	With regard to Article 30	***Processing of personal data, by automated or other means,***

article	COMENTARIO DELEGACIÓN ESPAÑOLA	SPANISH DELEGATION COMMENTS	*texto*
[amended]	apropiado aclarar qué criterios se utilizarían para considerar estos datos como estrictamente necesarios y proporcionados.	paragraph 2, it is considered appropriate to clarify what criteria would be used to consider these data as strictly necessary and proportionate.	***revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data and biometric data for the purpose of uniquely identifying a natural person or data concerning a person's health or sex life or sexual orientation shall be prohibited, unless it isallowed only where strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol. The selection of a particular group of persons solely on the basis of such personal data shall be prohibited.***