



Council of the
European Union

Brussels, 5 March 2021
(OR. en, fr)

**Interinstitutional File:
2020/0349(COD)**

**5527/4/21
REV 4**

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) and the latest comments regarding block 4 received after the meeting of 22 February 2021 (Annex part 4).

Table of contents

1. GENERAL COMMENTS	4
AUSTRIA	4
BELGIUM	5
CROATIA.....	7
CZECH REPUBLIC	10
FRANCE.....	12
GERMANY	43
HUNGARY.....	45
ITALY.....	46
LITHUANIA.....	55
SPAIN	58
2. COMMENTS RECEIVED AFTER MEETING ON 25 JANUARY 2021 (BLOCKS 1 AND 3)	59
AUSTRIA	59
BELGIUM	60
BULGARIA	62
CYPRUS	66
CZECH REPUBLIC	67
ESTONIA.....	72
FINLAND	75
FRANCE.....	77
GERMANY	90
ITALY.....	93
LITHUANIA.....	94
POLAND	95
NETHERLANDS.....	98
POLAND	101
ROMANIA.....	102
SPAIN	104
3. COMMENTS RECEIVED AFTER THE MEETING ON 8 FEBRUARY 2021 (BLOCKS 1, 3, 5 AND 7)	107
AUSTRIA	107
BELGIUM	109

BULGARIA	110
CYPRUS	112
CZECH REPUBLIC	113
FINLAND	117
FRANCE.....	118
GERMANY	134
HUNGARY	138
ITALY	140
LATVIA.....	147
LITHUANIA.....	149
MALTA	151
NETHERLANDS.....	152
POLAND	157
ROMANIA.....	159
SPAIN	162
4. COMMENTS RECEIVED AFTER THE MEETING ON 22 FEBRUARY 2021	
(BLOCK 4).....	164
BELGIUM	164
BULGARIA	167
CROATIA	170
CZECH REPUBLIC	171
ESTONIA.....	172
FRANCE.....	173
GREECE	174
IRELAND	176
ITALY	177
LATVIA.....	178
LITHUANIA.....	179
NETHERLANDS.....	181
POLAND	183
SLOVENIA.....	185
SPAIN	187

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 to 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 :

<i>Commentaires des autorités françaises sur la proposition de refonte du règlement Europol de la Commission européenne</i>	
<i>I) <u>CONSIDERANTS</u></i>	
<i>Proposition de la Commission européenne</i>	<i>Commentaires des autorités françaises</i>

<p><u>Considérant 4:</u></p> <p>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</p>	<p>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.</p> <p>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.</p>
<p><u>Considérant 6 :</u></p> <p>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.</p>	<p>Le terme de « <i>high risks criminals</i> » 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.</p> <p>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 :</p> <p><i>"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:</i></p> <ul style="list-style-type: none"> <i>- 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</i> <i>- Suspected to have committed one or more of the offences defined in Article 3 of the Europol Regulation during the past year. "</i> <p>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.</p> <p>Les autorités françaises proposent donc de supprimer cette référence aux « <i>high-risks criminals</i> ».</p>

	<p>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 terme utilisé habituellement « <i>Threat assessment</i> » pour l'acronyme SOCTA.</p> <p>Soit la proposition de rédaction suivante :</p> <p><i>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.</i></p>
<p><u>Considérant 8:</u></p> <p>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</p>	<p>Les autorités françaises sont défavorables à ce considérant conformément aux positions déjà exprimées sur cette problématique.</p> <p>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.</p>

<p><u>Considérant 9:</u></p> <p>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.</p>	<p>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.</p> <p>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.</p> <p>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.</p>
<p><u>Considérant 10 :</u></p> <p>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.</p>	<p>La proposition de reformulation vise à bien prendre en compte l'évolution de la menace qui vient compléter l'évolution des risques.</p> <p>Soit la proposition de rédaction suivante :</p> <p><i><u>Criminal threat</u> 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 <u>criminal threat and</u> risk assessments, Europol should provide analysis based on the information it holds on criminal phenomena and trends.</i></p>
<p><u>Considérant 11:</u></p> <p>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.</p>	<p>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.</p> <p>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 – apparaît comme plus pertinente pour éviter les redondances et mutualiser les efforts.</p> <p>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.</p>

	<p>Soit la proposition de rédaction suivante :</p> <p><i>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</i></p>
<p><u>Considérant 12:</u></p> <p>It is possible for the Union and the Member 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</p>	<p>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.</p> <p>Ensuite, le considérant introduit la notion « d'ordre public » pour laquelle l'agence Europol n'est pas compétente.</p> <p>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.</p> <p>Pour rappel le VCP est une technologie développée par une entreprise dont l'établissement légal se situe hors de l'Union européenne.</p> <p>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.</p>

<p>Considérant 13 :</p> <p>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.</p>	<p>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 ».</p> <p>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.</p>
<p><u>Considérant 14:</u></p> <p>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.</p> <p>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.</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>Elles relèvent enfin que la préservation de l'efficacité des choix des stratégies d'entrave milite en faveur de la maîtrise du dialogue entre services enquêteurs et autorités judiciaires.</p>

<p><u>Considérant 15:</u></p> <p>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.</p>	<p>Les autorités françaises proposent que ce considérant soit modifié comme suit :</p> <p><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></p>
<p><u>Considérant 18:</u></p> <p>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.</p>	<p>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 soumettre lesdites contributions.</p> <p>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.</p> <p>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.</p> <p>Proposition d’amendement en ce sens :</p> <p><i>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</i></p>

	<i>Regulation (EU) 2016/794. Europol should document that assessment</i>
<p>Considérant 19:</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>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.</p> <p>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.</p>
<p>Considérant 22:</p> <p>Europol and the European Public Prosecutor’s Office (‘EPPO’) established by Council Regulation (EU) 2017/193958, should put necessary arrangements in place</p>	<p>Les autorités françaises rappellent qu’au titre de l’article 102 du règlement Parquet européen, Europol fournit un soutien à cet organe pour <u>les enquêtes</u> et non pour les poursuites.</p>

<p>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.</p>	
<p><u>Considérant 24:</u></p> <p>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.</p>	<p>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.</p> <p>Pour mémoire, la France soutient « l'option 2 » proposée par la Commission européenne : <i>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).</i></p> <p>Les autorités françaises proposent que le régime juridique des relations d'Europol avec</p>

	<p>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.</p> <p>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.</p> <p>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.</p> <p>Proposition d'amendements :</p> <p>Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries <i>within the agreement of the management board</i> while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects.</p>
<p><u>Considérant 25:</u></p> <p>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.</p>	<p>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.</p> <p>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.</p> <p>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).</p>

<p><u>Considérant 31:</u></p> <p>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 to 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.</p>	<p>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 entraîne des interrogations sur les autorités effectivement concernées.</p> <p>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.</p> <p>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 août 2021). Les autorités françaises marquent leur attachement à ce que ces cadres existants soient respectés.</p>
<p><u>Considérant 33:</u></p> <p>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.</p>	<p>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)).</p>

<p>Considérant 35:</p> <p>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.</p>	<p>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)</p>
<p>Considérant 37 :</p> <p>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.</p> <p>The provisions on the development of new tools by Europol should not constitute a legal basis for their deployment at Union or national level.</p>	<p>Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.</p> <p>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 « <i>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</i> ». Elle précisait que ce pôle travaillerait avec Frontex, CEPOL, eu-LISA et le Centre commun de recherche (JRC).</p> <p>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.</p> <p>Proposition d'amendement :</p> <p>“To that end, Europol should <u>in close cooperation with relevant Union bodies</u> support Member States in the use of emerging</p>

	technologies in preventing and countering crimes falling within the scope of Europol's objectives."
<p>Considérant 38 :</p> <p>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.</p>	<p>Les autorités françaises réitèrent leur commentaire précédent (considérant 37). et propose l'amendement suivant :</p> <p><i>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.</i></p>
<p><u>Considérant 40:</u></p> <p>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.</p>	<p>Afin de suivre et d'enrichir les travaux de l'agence, cette information annuelle doit être communiquée aux États-membres.</p> <p>Les autorités françaises proposent de modifier le considérant comme suit :</p> <p><i>« To enable effective political monitoring of the way Europol applies additional tools and capabilities, Europol should provide the Joint Parliamentary Scrutiny <u>Group and the Member States</u> with annual information on its use of these tools and capabilities and the result thereof ».</i></p>
<p>Considérant 41:</p> <p>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</p>	<p>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.</p> <p>Elles souhaitent donc que la Commission soit interrogée sur l'existence d'un tel mécanisme dans d'autres agences de l'UE qui concerne</p>

<p>agreements within the scope of its objectives and tasks.</p>	<p>non seulement les États-Membres mais également les États tiers.</p> <p>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.</p> <p>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 <i>ab initio</i>.</p>
<h2>II) ARTICLES</h2>	
<p><u>Article – 1 (1) (c)</u></p> <p>(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</p>	<p>Les autorités françaises jugent cette disposition restrictive et précise que d'autres agences JAI pourraient également transférer des dossiers d'enquête à Europol.</p>
<p><u>Article 1 (2) (a) (i)</u></p> <p><u>Tasks</u></p> <p>(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;</p>	<p>Les autorités françaises réitèrent leur commentaire précédent sur le considérant 4. De nouvelles tâches sont assignées à Europol, sans articulation avec les compétences des États membres ou avec d'autres entités européennes : quid de l'articulation avec l'IntCen ?</p>

<p><u>Article 1 (2) (a) (iv):</u></p> <p>(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 ;</p>	<p>(q) : CF commentaires sur le concept de « high risk ».</p> <p>Soit la proposition de rédaction suivante :</p> <p>(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 <u>criminal threat</u> for security, and facilitate joint, coordinated and prioritised investigations ;</p>
<p><u>Article 1 (2) (a) (iv)</u></p> <p><u>Tasks</u></p> <p>(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);</p>	<p>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.</p>
<p><u>Article 1 (2) (a) (iv)</u></p> <p><u>Tasks</u></p> <p>(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;</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 9.</p> <p><u>Pour mémoire</u> : 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.</p> <p>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.</p> <p>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.</p>

<p><u>Article 1 (2) (a) (iv)</u></p> <p><u>Tasks</u></p> <p>(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</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 37.</p> <p><u>Pour mémoire</u> : Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.</p>
<p><u>Article 1 (2) (d)</u></p> <p><u>Tasks</u></p> <p>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.</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 37.</p> <p><u>Pour mémoire</u> : Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.</p>
<p><u>Article 1 (2) d)</u></p> <p><u>Tasks</u></p> <p>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.</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 12.</p> <p><u>Pour mémoire</u> : 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.</p> <p>Ensuite, le considérant introduit la notion « d'ordre public » pour laquelle l'agence Europol n'est pas compétente.</p> <p>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.</p>

	<p>Pour rappel le VCP est une technologie développée par une entreprise dont l'établissement légal se situe hors de l'Union européenne.</p> <p>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.</p>
<p><u>Article 4 paragraph 5</u></p> <p><u>Tasks</u></p> <p>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.</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 13.</p> <p><u>Pour mémoire :</u></p> <p>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 ».</p> <p>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.</p>
<p><u>Article 1 (3)</u></p> <p><u>Request by Europol for the initiation of a criminal investigation</u></p> <p>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.</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 14.</p> <p><u>Pour mémoire :</u></p> <p>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.</p> <p>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.</p> <p>Toutefois, les autorités françaises constatent que la nouvelle rédaction de l'article 6 tient compte de certaines réserves exposées et ne</p>

	<p>prévoit pas de pouvoir d'enquête d'initiative pour l'agence.</p> <p>Elles relèvent enfin que la préservation de l'efficacité des choix des stratégies d'entrave milite en faveur de la maîtrise du dialogue entre services enquêteurs et autorités judiciaires.</p>
<p><u>Article 1(4)</u></p> <p><u>Article 7 :</u></p> <p>“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.</p> <hr/> <p>* 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).</p> <p>** 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).”</p>	<p>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.</p> <p>Soit la proposition de rédaction suivante :</p> <p><i>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 <u>entitled to reply to duly justified requests made by Europol</u> 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.</i></p>

<p><u>Article 1(5)</u></p> <p><u>Purposes of information processing activities</u></p> <p>(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.</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 15.</p> <p><u>Pour mémoire</u> : Les autorités françaises proposent que ce considérant soit modifié comme suit :</p> <p><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></p>
<p><u>Article 1 (6)</u></p> <p><u>Art 18a</u></p> <p><u>Information processing in support of a criminal investigation</u></p> <p>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:</p> <p>(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</p> <p>(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.</p> <p>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.</p> <p>The Management Board, acting on a proposal</p>	

<p>from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data.</p> <p>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.</p>	
<p>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.</p> <p>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.</p> <p>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.</p>	

<p>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</p>	<p>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.</p> <p>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</p> <p>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.</p> <p>Or, Europol est une agence qui soutient <u>en priorité les États membres</u> 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.</p> <p>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.</p>
<p><u>Article 1(8)</u></p> <p><u>Article 20a</u></p> <p><u>Relations with the European Public Prosecutor's Office</u></p> <p>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.</p>	<p>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 transfert de données à l'EPPO.</p> <p>Les autorités françaises rappellent les dispositions de l'article 102 du règlement Parquet européen qui disposent que le Parquet européen « <i>peut également demander à Europol de fournir une aide à l'analyse dans le</i></p>

<p>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.</p> <p>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.</p> <p>4. Europol shall without undue delay report to the EPPO any criminal conduct in respect of which the EPPO could exercise its competence.</p>	<p><i>cadre d'une enquête particulière conduite par le Parquet européen ».</i></p> <p>Elles estiment par conséquent que le terme de « poursuites » doit être retiré de cette proposition d'article.</p> <p>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.</p> <p>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.</p>
<p><u>Article 1 (11)</u></p> <p><u>Article 25</u></p> <p>Transfer of personal data to third countries and international organisations</p> <p>(a) In paragraph 5, the introductory phrase is replaced by the following:</p> <p>"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:</p> <p>(b) In paragraph 8, the following sentence is deleted :</p> <p>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.</p>	<p>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.</p> <p>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.</p>

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;

(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.

Les autorités françaises s’interrogent sur les conditions mentionnées au paragraphe 5 de l’article 26 et sur la nature cumulative de ces dernières.

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 concerned override the public interest in the transfer referred to in points (d) and (e).

Transfers shall not be systematic, massive or structural.”

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.

<p><u>Article 1 (20)</u></p> <p><u>Article 34 :</u></p> <p>(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.”;</p> <p>(b) (b) paragraph 3 is deleted;</p>	<p>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.</p> <p>Soit la proposition de rédaction suivante :</p> <p>In the event of a personal data breach, Europol shall without undue delay notify <u>the EDPS as well as</u> 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.”;</p>
<p><u>Article 1 (37)</u></p> <p><u>Article 51</u></p> <p>Joint Parliamentary scrutiny</p> <p>(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;</p>	<p>Les autorités françaises demandent la suppression de cet article, lequel ne tient pas compte du protocole validé en COSI.</p>
<p><u>Article 1 (38)</u></p> <p><u>Article 57</u></p> <p><u>Budget</u></p> <p>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.</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 41.</p> <p><u>Pour mémoire :</u></p> <p>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.</p> <p>Elles souhaitent donc que la Commission soit interrogée sur l'existence d'un tel mécanisme dans d'autres agences de l'UE qui concerne</p>

	<p>non seulement les États-Membres mais également les États tiers.</p> <p>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.</p> <p>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 <i>ab initio</i>.</p> <p>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.</p>
--	--

<p>Article 1 (40)</p> <p>Article 67</p> <p>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). 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.</p> <p>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.</p>	<p>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.</p> <p>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).</p> <p>Les autorités françaises s'interrogent sur les raisons de ce changement envisagé par la proposition de la Commission.</p>
---	---

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-Bas 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 membre 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
<p><u>With reference to recital 3:</u></p> <p><i><u>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.</u></i></p>	<p>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.</p> <div><p>We therefore propose a revised version of recital 3:</p><p><i>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.</i></p></div>
<p><u>With reference to recital 6:</u></p> <p><i>"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".</i></p>	<p>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.</p>

<p><u>With reference to recital 8 and the connected amendment of art.4 r)</u></p>	<p>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.</p>
<p><u>With reference to recital 12 and connected new paragraph 4b of art.4</u></p> <p><i>“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.”</i></p>	<p>Italy believes that UNEs and AROs should be explicitly involved in the screening of foreign direct investments.</p> <div data-bbox="738 853 1358 891" style="border: 1px solid black; padding: 2px;"> <p><i>Therefore we propose to rephrase the recital as follows:</i></p> </div> <p><i>“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.”</i></p>
<p><u>With reference to recital 15 and the connected new article 18 f)</u></p> <p><u>Recital 15:</u></p> <p><i>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.</i></p>	<p>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.</p> <p>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).</p>

<p>Art 18 f</p> <p><i>“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.”</i></p>	<p>Therefore we suggest to modify the text of recital 15 and Art 18f as follows:</p> <p><u>Recital 15</u></p> <p><i>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.</i></p> <p><u>Art 18 f</u></p> <p><i>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</i></p>
<p><u>With reference to recital 33:</u></p> <p><i>(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.</i></p>	<p>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.</p> <p>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.</p> <p>If agreed the new wording of Art 7 par 8 would be replaced by the following:</p> <p><i>“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</i></p>

	<p><i>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.</i></p>
<p><u>With reference to the amendment of art.4 h) and connected recital 4</u></p> <p><i>“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;”</i></p>	<p>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.</p>
<p><u>With reference to the amendment of art.4 m)</u></p> <p><i>“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 <u>coordination of law enforcement authorities’</u> response to cyberattacks, <u>the taking down of</u> 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;”</i></p>	<p>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 <u>to coordinate</u> (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 <u>supporting</u> member States and not coordinating them.</p> <p>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.</p>
<p><u>With reference to the amendment of art.4 r) and connected recital 8</u></p>	

<p>(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);</p>	<p>Italy recalls the observations made with reference to recital 8. We can not support the text,</p>
<p><u>With reference to the amendment of art.4 new paragraph 4b and connected recital 12:</u></p> <p>“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”</p>	<p>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.</p> <div data-bbox="727 1106 1366 1142" style="border: 1px solid black; padding: 2px;"> <p>Therefore we propose to rephrase recital 12 as follows:</p> </div> <p>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</p>
<p><u>With reference to the new proposed version of Article 6 and connected recital 14:</u></p> <p>“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</p>	<p>We would like to have explanations on the need to replace the actual Art 6 (under current Europol Regulation) with the proposed version.</p>

<p><i>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.”</i></p>	<p>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.</p> <p>We believe that no modification should involve art. 6 of the Europol actual Regulation.</p>
<p><u>With reference to the new proposed version of Article 7:</u></p> <p><i>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</i></p>	<p>As already observed under our comment in relation to recital 33, Italy asks for the recital to be merged with Art 7.</p>
<p><u>With reference to the new article 18 3a:</u></p> <p><i>“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.”</i></p>	<p>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.</p> <div data-bbox="727 1485 1364 1520" style="border: 1px solid black; padding: 2px;"> <p>Therefore, we propose the following rephrasing:</p> </div> <p><i>“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”.</i></p>

<p><u>With reference with the new Article 25 paragraph 5, replaced by the following:</u></p> <p><i>"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:"</i></p>	<p>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?</p>
<p><u>With reference paragraph 8, the following sentence is deleted:</u></p> <p><i>"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."</i></p>	<p>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.</p>
<p><u>With reference to the Article 26 paragraph 2 that would be replaced by the following:</u></p> <p><i>"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</i></p>	<p>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).</p> <p>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,</p>

<p><i>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.”</i></p>	<p>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.”</p> <p>Moreover, in our opinion both conditions should apply simultaneously in order to allow Europol to receive data from Private parties:</p> <ul style="list-style-type: none"> — having identified and forwarded the relevant personal data — it is not possible to identify further national units concerned. <p>Therefore we suggest to replace the word « or » with « and ».</p> <p>In general, Italy believes that any information exchange should comply with the current regulatory framework and fully involve the Europol National Units.</p> <p>Furthermore Italy believes that the first part of the article should be reworded according to the following version:</p> <p>“Europol may only receive personal data directly from private parties, based on third countries, in compliance with national legal framework ...”</p>
<p><u>Regarding the new paragraphs 6a and 6b of art. 26:</u></p> <p><i>“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</i></p>	<p>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?</p> <p>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 done in accordance with their national law (which automatically implies lawfully). So why foreseeing this obligation explicitly?</p>

<p><i>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”.</i></p>	
--	--

<p><u>With regard to the new art. 26a</u></p>	<p>We want to raise the same objection of the new version of article 26</p>
<p><u>With reference to the new version of Article 57, paragraph 4 proposed:</u></p> <p><i>“..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.”</i></p>	<p>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.</p> <p>This situation would be harmful both for Member States but also for the credibility of the Agency, of the European institutions and the confidence that Member States place in it.</p> <p>Therefore, we cannot support the text proposed.</p>

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 particularly 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 whether 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 and 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 “Europol's 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.
 - o 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.
 - o 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.
 - o 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)).
 - o 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.
 - o 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 block 3 on research and innovation 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 (erase¹) 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:

- (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

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

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 protocol¹ 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, its 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).

Article 26(5)(c)

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

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.

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.

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 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:

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

- 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;

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 :

<p><u>Considérant 25:</u> 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.</p>	<p>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.</p> <p>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.</p> <p>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).</p>
<p><u>Considérant 31:</u> 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</p>	<p>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 entraîne des interrogations sur les autorités effectivement concernées.</p> <p>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.</p> <p>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 août 2021). Les autorités françaises marquent leur attachement à ce que ces cadres existants soient respectés.</p>

<p>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.</p>	
<p><u>Considérant 33:</u></p> <p>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.</p>	<p>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.</p> <p>Néanmoins, en l'état, sont identifiés les risques suivants :</p> <ul style="list-style-type: none"> - 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). <p>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</p>

	doivent pas être déjà transmises aux CRF selon la Directive LBC/FT.
<p><u>Considérant 35:</u></p> <p>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.</p>	<p>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).</p>

<p><u>Article 1(4)</u></p> <p><u>Article 7 :</u></p> <p>“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.</p> <p>* 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</p>	<p>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.</p> <p>Soit la proposition de rédaction suivante :</p> <p><i>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 <u>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**</u>, in particular via their national unit regarding financial information and analyses, within the limits of their mandate and competence.</i></p>
---	--

<p>of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).</p> <p>** 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)."</p>	
<p><u>Article 1(2)(a)(iii)</u></p> <p>« 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 ».</p>	<p>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.</p>
<p><u>Article 1(2)(a)(iv)</u></p> <p>« 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 ».</p>	<p>Les autorités françaises estiment pertinent que cette définition de la situation de crise soit inscrite dans l'article dévolu aux définitions.</p>

<p><u>Article 1(12)</u></p>	<p>Comme indiqué pour le considérant 33, une modification de l'article 26 apparaît opportune pour intégrer les dispositions prévues au considérant 33 : « <i>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</i> ».</p>
<p><u>Article 1(12)(a)</u></p> <p>“ 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.”</p>	<p>Les autorités françaises saluent cette proposition équilibrée de la Commission. Toutefois, elles rappellent que <u>la coopération entre Europol et les parties privées doit être transparente envers les États membres</u> et proposent à cet effet deux nouvelles dispositions (<i>cf. fin de document</i>).</p>
<p><u>Article 1 (13) :</u></p> <p><u>Article 26a</u></p> <p>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).</p>	<p>Comme indiqué pour le considérant 33, une modification de l'article 26 apparaît opportune pour intégrer les dispositions prévues au considérant 33 : « <i>les informations transmises par les parties privées ne concerneront que des informations qui ne doivent pas être déjà</i></p>

<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>6. Europol shall ensure that detailed records of all transfers of personal data and the grounds for such</p>	<p><i>transmises aux cellules de renseignement financier selon la Directive (UE) 2015/849 ».</i></p> <p>Par ailleurs, les autorités françaises réitèrent leur commentaire précédent -Article 1(2) (a) (iv)- sur la définition de la situation de crise.</p>
---	---

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 :

- 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-Bas 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 membre 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.

<p><u>Considérant 11:</u></p> <p>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.</p>	<p>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.</p> <p>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 – apparaît comme plus pertinente pour éviter les redondances et mutualiser les efforts.</p> <p>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.</p> <p>Soit la proposition de rédaction suivante :</p> <p><u>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></p>
<p><u>Considérant 12:</u></p> <p>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</p>	<p>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.</p> <p>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.</p> <p>Les autorités françaises proposent donc la suppression de ce considérant.</p>

<p><u>Considérant 37 :</u></p> <p>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.</p> <p>The provisions on the development of new tools by Europol should not constitute a legal basis for their deployment at Union or national level.</p>	<p>Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.</p> <p>Elles rappellent que la Commission, dans sa stratégie de sécurité intérieure pour l'Union 2020-2025 évoquait dans la lignée de la révision du règlement Europol « <i>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</i> ». Elle précisait que ce pôle travaillerait avec Frontex, CEPOL, eu-LISA et le Centre commun de recherche (JRC).</p> <p>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.</p> <p>Proposition d'amendement :</p> <p><u>"To that end, Europol should <i>in close cooperation with relevant Union bodies</i> support Member States in the use of emerging technologies in preventing and countering crimes falling within the scope of Europol's objectives."</u></p>
<p><u>Considérant 38 :</u></p> <p>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.</p>	<p>Les autorités françaises réitèrent leur commentaire précédent (considérant 37) et propose l'amendement suivant :</p> <p><u>Europol <i>should in close cooperation with relevant Union bodies</i> 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.</u></p>

<p><u>Considérant 40:</u></p> <p>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.</p>	<p>Afin de suivre et d'enrichir les travaux de l'agence, cette information annuelle doit être communiquée aux États membres.</p> <p>Les autorités françaises proposent de modifier le considérant comme suit :</p> <p><i>« 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 ».</i></p>
<p><u>Considérant 41:</u></p> <p>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.</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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 <i>ab initio</i>.</p>

<p><u>Article 1 (2) (a) (iv)</u></p> <p><u>Tasks</u></p> <p>(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</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 37.</p> <p><u>Pour mémoire :</u> Les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.</p>
<p><u>Article 1 (2) (d)</u></p> <p><u>Tasks</u></p> <p>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.</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 37.</p> <p><u>Pour mémoire :</u> les autorités françaises s'étonnent de l'absence de référence aux autres agences JAI dans ce considérant consacré à l'innovation.</p>
<p><u>Article 1 (2) d)</u></p> <p><u>Tasks</u></p> <p>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.</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 12.</p> <p><u>Pour mémoire :</u> 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.</p> <p>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.</p>
<p><u>Article 1 (38)</u></p> <p><u>Article 57</u></p> <p><u>Budget</u></p> <p>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</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 41.</p> <p><u>Pour mémoire :</u></p> <p>Les autorités françaises s'étonnent d'une telle proposition et rappellent que l'agence Europol ne</p>

<p>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.</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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 <i>ab initio</i>.</p> <p>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.</p>
---	---

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** preventing the 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 stemmings 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" and "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 accordingly 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 Treaty on the European Union as well as recognizes that national security remains the sole responsibility of each Member State. Since the objective of this Regulation is to strengthen 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 necessary 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:

<i>(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.</i>	<u>Comment:</u> Due to the cross-sectoral nature of the EU Innovation Hub, we believe that effective inter-agency cooperation is necessary
--	--

On page 29 of 13908/20, Article 4:

<p><i>“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.</i></p>	<p><u>Comment:</u> We consider it important to provide adequate human and financial support to Europol, given the significant expansion of its competences and tasks.</p>
<p><i>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.</i></p>	<p><u>Comment:</u> 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.</p> <p>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.</p> <p>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 securty, is excluded from the scopeof EU law. Therefore, in the opinion of our experts</p>

	Europol should not play an active role in the process of screening foreign direct investment.
--	---

On page 29 of 13908/20, Article 6

<p>(3) in Article 6, paragraph 1 is replaced by the following:</p> <p><i>“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.”</i></p>	<p>In the opinion of our experts (initial remarks) :</p> <p>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 proceedings.</p>
---	---

On page 31 of 13908/20, Article 18a

<p>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:</p> <p><i>(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</i></p> <p><i>(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.</i></p>	<p><u>Comment:</u></p> <p>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 clarified if a Member State is supposed to provide whole case file to Europol ?</p>
--	--

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

<p><i>“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.</i></p> <p><i>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.</i></p>	<p><u>Comment:</u></p> <p>This issue is analyzed by the Polish ENU, e.g. in the context of the possible generation of additional tasks for ENUs.</p> <p>The request made by Europol shall not pose any obligation to Member States. Obtaining any information from private parties should be conducted on a voluntary basis.</p>
---	--

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, .

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 Protocol¹, 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 :

<p><u>Considérant 25:</u> 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.</p>	<p>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.</p> <p>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.</p> <p>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).</p>
<p><u>Considérant 31:</u> 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. <u>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.</u> In many cases, these Member States may not be able to establish a link to</p>	<p>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.</p>

<p>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.</p>	
<p><u>Considérant 35:</u></p> <p>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.</p>	<p>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).</p>

<p><u>Article 2</u></p> <p>(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.</p>	<p>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 ».</p> <p>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 entraîner des interprétations divergentes, en fonction de la réponse apportée, il pourra être</p>
---	---

	demandé de supprimer : « or suspected as being carried out in ».
<p><u>Article 4</u></p> <p>(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.</p>	<p>Les autorités françaises soutiennent cette suppression, la définition d'une situation de crise en ligne étant prévue à l'article 2.</p>
<p><u>Article 1(4)</u></p> <p><u>Article 7 :</u></p> <p>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 <u>entitled to reply to duly justified requests made by allowed to cooperate with</u> 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 <u>and subject to national procedural safeguards.</u></p> <p>* 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).</p> <p>** 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</p>	<p>Les autorités françaises remercient la Présidence pour la prise en compte de leur proposition d'amendement.</p>

Council Decision 2000/642/JHA (OJ L 186, 11.7.2019, p. 122).”	
<p><u>Article 1(2)(a)(iii)</u></p> <p>« 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 ».</p>	<p>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.</p>
<p><u>Article 1(2)(a)(iv)</u></p> <p>« 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 ».</p>	

<p><u>Article 1(12)(a)</u></p> <p>“ 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.</p>	<p>Les autorités françaises saluent cette proposition équilibrée de la Commission. Toutefois, elles rappellent que <u>la coopération entre Europol et les parties privées doit être transparente envers les États membres</u> et proposent à cet effet deux nouvelles dispositions (cf. fin de document).</p>
--	--

<p>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.”</p>	
<p><u>Article 26 (6b)</u></p> <p>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.</p>	<p>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.</p>
<p><u>Article 1 (13) :</u></p> <p><u>Article 26</u></p> <p>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).</p> <p>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.</p>	<p>Les autorités françaises remercient la Présidence pour la prise en compte de leur remarque et la modification subséquente de cet article.</p> <p>Par ailleurs, à l’article 26a “<i>Exchanges of personal data with private parties in online crisis situations</i>”, 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.</p>

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.

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.

<p>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.”</p>	
---	--

Les autorités françaises proposent en complément des articles additionnels :

Les autorités françaises estimerait 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.

<p><u>Considérant 12:</u></p> <p>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</p>	<p>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.</p> <p>Les autorités françaises proposent donc la suppression de ce considérant et de l'article afférent</p>
--	---

<p><u>Considérant 37 :</u></p> <p>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, <u>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</u></p>	<p>Les autorités françaises remercient la Présidence pour la prise en compte de leurs remarques s'agissant de la coopération avec les autres agences JAI.</p>
--	--

<p><u>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 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.</u></p>	
<p><u>Considérant 40:</u></p> <p>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.</p>	<p>Afin de suivre et d’enrichir les travaux de l’agence, cette information annuelle doit être communiquée aux États membres.</p> <p>Les autorités françaises proposent de modifier le considérant comme suit :</p> <p><i>« 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 ».</i></p>
<p><u>Article 1 (2) d)</u></p> <p><u>Tasks</u></p> <p>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.</p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 12.</p> <p><u>Pour mémoire</u> : 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.</p>

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 :

<p><u>Considérant 24:</u></p> <p><i>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.</i></p>	<p>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 : <i>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).</i></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Proposition d'amendements :</p> <p><i>Serious crime and terrorism often have links beyond the territory of the Union. Europol can exchange personal data with third countries <u>within the agreement of the management board</u> while safeguarding the protection of privacy and fundamental rights and freedoms of the data subjects.</i></p>
<p><u>Article 1 (6) :</u></p> <p><u>Article 18a(4) :</u></p> <p><i>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</i></p>	<p>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.</p> <p>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.</p>

<p><i>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...</i></p>	<p>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 Etat tiers.</p> <p>Or, Europol est une agence qui soutient <u>en priorité</u> 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.</p> <p>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.</p>
<p><u>Article 1 (11)</u></p> <p><u>Article 25</u></p> <p><u>Transfer of personal data to third countries and international organisations</u></p> <p><i>(a) In paragraph 5, the introductory phrase is replaced by the following:</i></p> <p><i>"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:</i></p> <p><i>(b) In paragraph 8, the following sentence is deleted :</i></p> <p><i>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.</i></p>	<p>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.</p> <p>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.</p> <p>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.</p>

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 maîtrise 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 apparaît 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.

	<p>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.</p>
<p><u>Article 1 (3)</u></p> <p><u>Request by Europol for the initiation of a criminal investigation</u></p> <p><i>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.</i></p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 14.</p> <p>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.</p> <p><u>Pour mémoire :</u></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Elles relèvent enfin que la préservation de l'efficacité des choix des stratégies d'entrave milite en faveur de la maîtrise du dialogue entre services enquêteurs et autorités judiciaires.</p> <p>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 ».</p>

	<p>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.</p> <p>Or il apparaît 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.</p> <p>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.</p> <p>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.</p>
--	---

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".

<p><u>Article 7(12)</u></p> <p><u>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;</u></p>	<p>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.</p> <p>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).)</p>
--	--

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.

<p><u>Considérant 41:</u></p> <p>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.</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>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 <i>ab initio</i>.</p>
<p><u>Article 1 (38)</u></p> <p><u>Article 57</u></p> <p><u>Budget</u></p> <p><i>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</i></p>	<p>Les autorités françaises réitèrent leurs commentaires précédents sur le considérant 41.</p> <p><u>Pour mémoire :</u></p> <p>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</p>

<p><i>Europol within the scope of Europol's objectives and tasks. The amount of the contribution shall be determined in the respective agreement.</i></p>	<p>l'agence et la confiance que les états-membres placent en elle.</p> <p>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.</p> <p>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.</p> <p>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 <i>ab initio</i>.</p> <p>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.</p>
---	--

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 consult 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 analysing 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			
<p><u>With reference to recital 3:</u></p> <p><i>“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”.</i></p>	<p>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.</p> <table><tr><td>We therefore propose a revised version of recital 3:</td></tr><tr><td><p><i>These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal, <u>mafia-style and family based</u> organised crime groups that engage in a wide range of criminal activities.</i></p></td></tr></table>	We therefore propose a revised version of recital 3:	<p><i>These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal, <u>mafia-style and family based</u> organised crime groups that engage in a wide range of criminal activities.</i></p>
We therefore propose a revised version of recital 3:			
<p><i>These threats spread across borders, cutting across a variety of crimes that they facilitate, and manifest themselves in poly-criminal, <u>mafia-style and family based</u> organised crime groups that engage in a wide range of criminal activities.</i></p>			
<p><u>With reference to recital 6:</u></p> <p><i>“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,</i></p>	<p>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.</p> <p>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.</p>		

<p><i>their criminal activities and the members of their criminal networks”.</i></p>	
<p><u>With reference to recital 12 and connected new paragraph 4b of art.4</u></p> <p><i>“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.”</i></p>	<p>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.</p>
<p>ARTICLES</p>	
<p><u>With reference to the amendment of art 2 (f)</u></p> <p><i>(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;</i></p> <p><i>(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);</i></p>	<p>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”.</p> <p>This would avoid any misinterpretation and would facilitate the cooperation among all stakeholders involved in the matter.</p>
<p><u>With reference to the amendment of art.4 h) and connected recital 4</u></p> <p><i>“support Member States’ cross-border information exchange activities, operations and investigations, as well as joint investigation teams, and special</i></p>	<p>Given the specific nature of the special intervention units, it would be preferable to specify the operational support given by Europol.</p>

<p><i>intervention units, including by providing <u>operational</u>, technical and financial support;</i></p>	<p>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.</p> <p><u>We propose to rephrase the sentence as follows:</u></p> <p><i>"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 <u>operational</u>, technical and financial support"</i></p>
<p><u>With reference to the amendment of art.4 m)</u></p> <p><i>"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 <u>coordination of law enforcement authorities'</u> response to cyberattacks, <u>the taking down</u> 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;"</i></p>	<p>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 <u>to coordinate</u> (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 <u>supporting</u> member States and not coordinating them.</p> <p>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.</p> <p>As a consequence we propose the following wording:</p> <p><i>"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 <u>coordination of law enforcement authorities'</u> response to cyberattacks, <u>the taking down</u> 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;</i></p>

<p><u>With reference to the amendment of art.4 par.1 (u)</u></p> <p><i>“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”.</i></p>	<p>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.</p> <p>Therefore we propose to amend the text as follows:</p> <p><i>“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”</i></p>
<p><u>With reference to the amendment of art.4 new paragraph 4b and connected recital 12:</u></p> <p><i>“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”</i></p>	<p>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.</p> <p>Italy believes that the provision of granting specific attributions to Europol in this sector seems to lay outside of the Law Enforcement prerogatives considering:</p> <ul style="list-style-type: none"> -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. <p>Italy thinks that further discussion, apart from the approval of Europol new Regulation, are necessary on this matter.</p>

<p><u>With reference to the new proposed version of Article 6 and connected recital 14:</u></p> <p><i>“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.”</i></p>	<p>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”.</p> <p>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.</p> <p>Italy believes that the proposal moves the focus for the request of the investigation from the cross border approach to the common interest approach.</p> <p>As this would be an important and crucial transformation of the role of the Agency Italy believes that further discussion and explanations are required.</p> <p>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.</p> <p>Italy believes that no modification should involve art. 6 of the Europol actual Regulation.</p>
<p><u>With reference to the new article 18 3a:</u></p> <p><i>“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.”</i></p>	<p>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.</p> <div data-bbox="727 1422 1362 1460" style="border: 1px solid black; padding: 2px;"> <p>Therefore, we propose the following rephrasing:</p> </div> <p><i>“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”.</i></p>

<p><u>With reference with the new Article 25 paragraph 5, replaced by the following:</u></p> <p><i>"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:"</i></p>	<p>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?</p> <p>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).</p> <p>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.</p>
<p><u>With reference to the Article 26 paragraph 2 that would be replaced by the following:</u></p> <p><i>"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</i></p>	<p>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.</p> <p>Any direct exchange of information of Europol with PP should involve only Private Parties based in Third Countries.</p> <p>Italy believes that the first part of the article should be reworded according to the following version:</p> <div data-bbox="727 1326 1362 1426" style="border: 1px solid black; padding: 5px;"> <p><i>"Europol may only receive personal data directly from private parties, based on third countries, in compliance with national legal framework ..."</i></p> </div>

<p><i>accordance with Article 19(1) within four months after the transfer takes place.”</i></p>	
<p><u>Regarding the new paragraphs 6a and 6b of art. 26:</u></p> <p><i>“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...”</i></p> <p><i>(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.</i></p>	<p>In order to avoid any overlapping with the domestic legislation Italy believes that it would be better to replace the part”...<i>under their applicable laws..</i>” with the part “<i>in accordance with the national legal framework</i>”.</p> <div data-bbox="719 629 1362 983" style="border: 1px solid black; padding: 5px;"> <p>If agreed the new version would be the following:</p> <p><i>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...</i></p> </div> <p>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.</p>
<p><u>With regard to the new art. 26a</u></p> <p><i>“Exchanges of personal data with private parties in online crisis situations</i></p> <p><i>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)”.</i></p>	<p>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.</p>

LATVIA

LV written comments regarding the Commission (COM) proposal amending Europol Regulation¹ (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.

- Article (1)(12)(d) (new Article 26(6a) 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

LV **welcomes** PRES changes in the related Recital 31 that clarify that Member States are not obliged to reply to Europol's requests on private 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 Member 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”.

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

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

<p><i>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.</i></p>	<p><u>Comment:</u></p> <p>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.</p>
---	--

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

<p>(3) <i>in Article 6, paragraph 1 is replaced by the following:</i></p> <p><i>"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."</i></p>	<p><u>Comment:</u></p> <p>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.</p>
--	---

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

<p><u>(4bis) In Article 7, the following paragraph 12 is added:</u></p> <p><u>"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;"</u></p>	<p><u>Comment:</u></p> <p>In our opinion, it could be considered to supplement the provision with names of the institutions to which the report will be addressed.</p>
--	--

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.

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:

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

*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.

**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 officers 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 frontline 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 2¹ 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.

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

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

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 proposal⁴ 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. 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.

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))

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 from 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.

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 last 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 Presidency 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!

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.
