Opinion of the Data Protection Officer

Draft Implementing Rules on Operational Personal Data

1. Purpose and introduction

The purpose of this opinion is to provide the Executive Director and the Management Board with advice on the compliance of the draft[1] Management Board Decision adopting the rules on processing operational personal data (hereinafter OPD) with the Data Protection Regulation (EUI DPR) and EU data protection acquis.

The EBCG regulation requires implementing rules for the application of the EUI DPR. The EBCG Regulation, in its Article 90, states that the Agency processes operational personal data and, when doing so, Chapter IX of the EUI DPR shall be applied. Consequently, Article 86(2) of the EBCG Regulation requires the Management Board to adopt implementing rules for the application of Chapter IX of the EUI DPR.

Chapter IX EUI DPR contains general rules applicable to the processing of operational personal data when this data is processed by EU institutions when they carry out activities in the fields of judicial cooperation in criminal matters and police cooperation. The application of Chapter IX relates only to those activities of Frontex which fall under the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU (for the purposes of prevention, detection, investigation or prosecution of criminal offences). Frontex is established under Chapter 2 TFEU. In particular, Article 77(2)(b) and (d) and Article 79(2)(c) are to checks on persons who cross the external borders, measures for the establishment of the integrated border management as well as for the implementation of measures against illegal immigration or unauthorised residence, including removal and repatriation of persons residing in the EU without authorisation. While the measures that Frontex need to implement may require the processing of personal data under police or judicial cooperation, such activities do not constitute the main activities of the Agency. Frontex is not established as the Agency whose main task is the prevention, detection, investigation or prosecution of criminal offences. Quite the contrary, the tasks that the Agency is awarded with by means of Article 10 EBCG Regulation contribute to the detection, prevention and combating of cross-border crime at the external borders, via border control activities, EUROSUR, Joint operations or liaison officers in third countries.

Consequently, it is of utmost importance to be able to identify those processing activities that the Agency carries out under the scope of Chapter IX EUI DPR, as only those processing activities would be covered by the application of the special rules for the processing of operational personal data. Regardless, the rules need to be consistent with the principles on data protection and should take due account of the provisions related to independent supervision, remedies, liability and penalties.

The DPO has conducted a review of the presented draft and assessed its merits, primarily against the data protection principles contained in Article 4 and 71 of the EUI DPR, the provisions contained in the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016) (also known as Law Enforcement Directive), informal consultation with the European Data Protection Supervisor, and after conducting a comparative analysis with Europol, Eurojust and EPPO's legal framework.

[1] *As presented on 4 October 2021*

2. Procedural aspects

The EBCG Regulation entered into force in December 2019. On 17 September 2019 the DPO provided the first of many regular updates to the agreed COM-Frontex Roadmap for the implementation of the EBCG Regulation. During the first update, the DPO highlighted the need to involve the DPO in the following topics:

- implementation of return activities,
- EUROSUR on the processing of personal data, both of vessel identification numbers and any other personal data processed under exceptional circumstances,
- media monitoring and open source intelligence,
- the implementation of the review and upgrade of the information management architectures and systems of the EBCGA,
- the redraft the Agency's Implementing Measures on data protection,
- the inclusion of data protection requirements in all Operational Plans,
- the determination of the entities responsible for compliance with personal data,
- the implementation of retention periods,
- traceability of personal data processing,
- the update of the Model Status Agreements,
- and mapping of the implementing measures that would be required to apply the EUI DPR.

During 2018 and 2019, the DPO had prepared the first draft of the rules on the processing of operational personal data based on the 2016 Frontex Regulation, which had been tabled for adoption to the Management Board in March 2019. Meanwhile, the EBCG Regulation entered into force in December 2019. On 20 October 2020 the DPO requested assistance of RAU PeDRA team to update the latest draft related to the processing of personal data collected in the context of joint operations, pilot projects, rapid border interventions and support management migration teams, which had been tabled for discussion to the Management Board in March 2019. The request included the points in the rules that would require modification considering the new EBCG regulation, namely: the new purpose of OPD (identification of suspects), the sources from which FX can obtain OPD and operational activities that the Agency undertakes in the context of prevention and detection of cross border crime, the types of data subjects and data categories, the channels of transmission not restricted to JORA, as well as persons who may process OPD, the criteria for reasonable grounds for a suspicion, the definition of suspect, witness and victim, the process of transmission and change of data subject category (from Article 88 to Article 90 EBCG Regulation), the conditions for exchange with Europol and Eurojust and the procedural aspects for the identification of national Law enforcement authorities of Member States.

On 21 January 2021, the DPO provided the first comments to the reworked draft implementing rules on OPD and held numerous meetings with RAU and CGLES discussing the Articles proposed as well as re-drafted the initial provisions and recitals, namely Articles related to the scope and definitions. However, it became clear throughout the discussions with the business units that managerial decisions needed to be taken particularly in relation to internal allocation of roles and responsibilities and the internal lifecycle of the data.

On March 2020 the DPO requested assistance to CAB to organise and engage different business units in order to have sufficient input to reflect it in the draft. The DPO highlighted the need for the Agency to have an operational concept that would cover the entire lifecycle of the processing of operational personal data within the Agency. To that end, the DPO prepared a questionnaire for internal usage that would allow to identify the processing activities undertaken by the Agency as well as the roles of each business units in relation to Article 90 EBCG Regulation.

Throughout the process, the DPO has been repeatedly highlighting that the staggering lack of resources in the DPO Office has a significant impact on the deliveries expected in relation to the provision of advice on different data processing activities undertaken by the agency, both covering "business as usual" activities and those tasks that came as an addition for the implementation of the EBCG Regulation and the COVID pandemic.

On April 2021, the Executive Director took the decision that business units would draft the implementing rules on data protection, and the DPO would advise the Executive Director on the drafts. Legal and Procurement Unit (LPU) was tasked with leading the process to prepare an MB decision adopting implementing rules concerning the processing of operational personal data. On 18 May, an Operational Board meeting took place where the Executive Director instructed that LPU would organize a workshop with Member States' experts. On 25 May there was an internal kick off meeting for drafting implementing rules of the EUI DPR, the DPO was not made aware of. On 19 June a meeting took place with internal stakeholders and Cabinet with DPO participation, where the DPO was made aware that an ED Decision for the setting up a project board for drafting OPD rules was being draft, to be approved that same day. The DPO provided comments on the same day, mainly introducing aspects related to its scope and reminding the Agency that the DPO cannot receive instructions on the performance of its tasks. The workshop with the Member States' experts took place on 24 June and was attended by the DPO.

In early August, meetings were held by LPU with the business units, who were requested to map their processing activities. Both SAM and ORD provided input listing all operational personal processing activities they would like to undertake, which the DPO commented upon on 11 August, mainly indicating in the mapping that several of the intended processing activities would be in clear violation of the EBCG Regulation (i.e.: transmission of OPD to international organisations and Third Countries). From August onwards, the DPO has been advising the Project Board on the provisions to be included in the implementing rules, as well as has participated in the project board meetings, adding comments to the proposed drafts or suggesting rewording and providing advice to meet compliance with the data protection acquis.

The DPO would like to draw management's attention to the fact that the process of drafting the OPD rules de facto encroaches the tasks legally assigned to the DPO, who is obliged by law to ensure compliance with all data protection obligations contained in different provisions of Union Law. When the DPO issues an opinion, such advice cannot be overruled or amended. This is one of the cornerstones of the independence granted to the DPO. If the Controller decides to disregard the opinion of the DPO, this should be decided by the controller at the end of the process, thus allowing the controller to take a fully informed decision. This, in turn, allows the Controller to being able to demonstrate compliance in line with the accountability principle of Article 4(2) EUI DPR. The methodology of seeking internal consensus following the requirements of business units at expense of the DPO advice deprives the Controller from taking its own decisions and makes the Controller vulnerable to demonstrate compliance. Lastly, the DPO would like to stress that the DPO is the competent function within an EUI to provide data protection advice, including on matters related to internal policies or processes and the assignment on data protection roles and responsibilities within an EUI.

3. Analysis and recommendations

As a general introductory comment, the DPO recommends that the text is contained in the Management Decision as such, instead as of an Annex. Firstly, because the text is not an annex to an empty shell but specially mandated by the EBCG Regulation for the Management Board to adopt internal rules for the application of the EUI DPR. Secondly, it provides consistency with the rules that are already under discussion referring to the DPO, thus aligning all rules under the same format.

(1) On the Recitals:

a. The DPO has some reservations about the utility of literally copying legal provisions from the EBCG Regulation into a text that implements a chapter of the Data Protection Regulation. Recitals should give background contextual information about the purpose of these implementing rules as well as sufficient information about the intention behind the articles as means to aid at interpretation. Therefore, **the DPO recommends deleting recital (2)**. If that is not considered, the DPO recommends that, after recital (2), an additional one should be added referring to Article 90(2) EBCG Regulation, considering that recital (1) copy/pastes Article 90(1) EBCG Regulation. If the legal text is literally going to copy legal provisions which are directly applicable to the Agency, then it is recommended that Article 90(2) EBCG Regulation is added should thus cover the exchange with competent national law enforcement authorities and with Europol and Eurojust.

b. On recital (3), **the DPO recommends adding that deletion is linked to the purpose of identification** of a suspect of cross border crime as specifically mandated in Article 90(1) EBCG regulation, in order to avoid any deviation from the purpose envisaged by the legislator.

c. On recital (6) the DPO recommends to explain the tasks undertaken by the Agency under Article 10(1)(q) and to explain that only when performing those tasks Chapter IX EUI DPR applies to the processing of data, as per strict application of the circumstances for which this Chapter can be applied and linking those activities to Chapter 4 or Chapter 5 of Title V of Part Three TFEU.

(2) On Article 1 (Subject and scope):

a. On Article 1(1): The DPO recommends modifying the scope and link it to the strict obligation vested upon the Agency, which is to implement the EUI DPR. **The DPO recommends to redraft the existing provision in order to reflect that the Management Board decision lays rules implementing Chapter IX of the EUI DPR and of Articles 90 and 91(3) of the EBCG Regulation**, to limit the scope of the implementing rules specifically to operational personal data processing. The DPO also recommends explaining in the recitals that Article 90 and 91(3) of the EBCG Regulation are lex specialis of the EUI DPR.

b. On Article 1(2): this is a quotation of Article 90 EBCG Regulation, which is referred to in the previous provision. **The DPO recommends not quoting the provisions that are directly applicable by the EBCG Regulation** and that additionally, are quoted in Article 1(1) and in the recitals. Instead, **the DPO recommends establishing as scope that Chapter IX referred to in the recommendation above establishes that the implementing rules shall only apply to the processing of personal data while Frontex conducts the task referred to in Article 10(1)(q)**.

(3) On Article 2: the DPO recommends to state that all definitions of Article 3 EUI DPR apply notwithstanding the further specifications for the purposes of these implementing rules.

a. On "operational personal data" the DPO recommends to delete from "Article 10(1)(q) onwards, as the definition in the EUI DPR refers to all personal data processed when the EUI founding regulation specifies a task related to the scope of Chapter IX EUI DPR.

b. On "witness", the DPO recommends amending the definition and align it with Article 90 EBCG Regulation. Particularly, Article 90 EBCG Regulation refers to the possibility to process personal data of victims or witnesses as long as their data complements the data of a suspect. Consequently, without such condition Frontex should not be able to process personal data of witnesses of cross border crime, but only those who provide information on a suspect. Consequently, **the DPO strongly recommends substituting "on cross border crime" to "suspects of cross border crime"**.

c. On "deletion", the definition provided is linked to the concept of anonymisation of data. Article 29 Working Party (currently the European Data Protection Board) provides, in its Opinion 05/2014 on Anonymisation Techniques, the definition on anonymisation which is still valid today. In their opinion Article 29 Working Party settled that, in order to consider personal data fully anonymised and consequently, be outside of the scope of Data Protection obligations, that data should not to allow the data subject to be identified via "all" "likely" and "reasonable" means, and that identification should not be possible. Consequently, the definition provided in the proposed draft would not meet the high standard set to consider personal data fully anonymised. **The DPO recommends to include provisions to ensure that deletion will delete not only personal data identifiers but any information that may lead, directly or indirectly, to the identification of the data subject**, thus being in line with the definition of personal data. Additionally, the DPO recommends further referring to standards on anonymisation in the recitals.

d. On "data collection plan" the definition explicitly states that there may be exceptional means for the exchange of personal data. This exception in the definition of data collection plan contradicts Article 12(4) of the proposed draft rules, as the channels mentioned therein only refer to JORA and SIENA for exchange and other channels to be used may be decided by means of an Executive Director Decision. The **DPO recommends adding a provision in Article 12 for the exchange of operational personal data that would allow the desired flexibility, but balanced for exceptional circumstances related to imminent danger** and deleting the exceptionality from the definition.

e. On "personal data breach" the DPO recommends using the legally defined definition established in Article 3(16) of the EUI DPR.

f. On "competent law enforcement authority of the Member State" the DPO recommends quoting the legal definition set in Article 3(7) of the Law Enforcement Directive, and then further specify that within Frontex exchange, those shall be listed in the data collection plan.

(4) On Article 3: **the DPO recommends renaming the Article to EBCGA as Data Controller**. Being a data controller entails the compliance with data protection obligations and bears the data protection responsibility.

Consequently, the DPO recommends amending the article title to reflect that these are responsibilities that the Agency undertakes as data controller.

a. On Article 3(1): the provision refers to the processing being done in accordance with “this Annex and Chapter IX EUI DPR”. **The DPO recommends inverting the order**, to highlight that the EUI DPR takes precedence and it is a higher hierarchical norm belonging to secondary legislation.
b. On Article 3(2), a reference is being made to the obligation set in the EBCG Regulation for the Agency to develop and maintain an information system that enables the exchange of operational personal data. The **DPO recommends moving this article to the current Article 3(4)**, so all provisions related to IT systems are grouped.
c. On Article 3(3)(a): the processing should refer to the processing of “operational personal data” not only to “personal data”, and the compliance should be first and foremost with the EUI DPR and then with the provisions ensuing in the MB Decision. Additionally, the provision refers to the obligation for the data controller to improve measures. It is not clear to what controller this provision is referring to, thus the **DPO recommends rewording it to “the Agency is responsible for choosing and implementing technical and organisational measures, taking into account the state of the art, the cost of implementation as well as the risks for the rights and freedoms of the data subjects”** to anchor the text in the EUI DPR which refers to this as an obligation of the data controller, particularly under Article 26 and 27.
d. On Article 3(3)(b): the provision constricts the role of the DPO to answer questions related to the protection of data processed through an information system, which is not specified. This provision is in conflict with Article 44 EUI DPR, which obliges the controller to address the DPO on any matter related to data protection and involve him or her properly and timely. **The DPO recommends aligning this provision with Article 44 EUI DPR**, by rewording: “the DPO shall be involved, in a properly and timely manner, in all issues related to data protection”.
e. On Article 3(3)(c): the DPO **recommends using the EUI DPR terminology and refer to “data protection impact assessment”** instead of privacy impact assessment. Additionally, as per obligation set in Article 89 EUI DPR, the **DPO recommends referring that the obligation to conduct a data protection impact assessment is conducted prior to the processing**.
f. On Article 3(4): for reasons of coherence, the DPO suggests moving provision 3(2) of the draft rules to this point in the text. Additionally, the presented Article 3(4) refers to the adoption of security measures. **The DPO recommends referring explicitly to the security measures referred to in Article 91 EUI DPR**.
g. On Article 3(4)(a): the provision states that operational personal data cannot be processed by IT administrators. By means of application of the definition of processing contained in Article 3(3) EUI DPR, IT Administrators will need to process operational personal data for the purpose of maintaining the IT systems the Agency operates with. **The DPO recommends deleting this provision and as a safeguard, include that the audit trail referred to in Article 23 of the presented draft establishes that IT administrator activities shall also be logged for monitoring purposes**.
h. On Article 3(4)(b): the Article sets the obligation as controller to ensure that the logs are reliable and accurate. By definition, audit logs must be reliable and accurate, otherwise the purpose of having an audit trail is rendered useless. **The DPO recommends deleting this provision** as it is irrelevant, the obligation is set in the EUI DPR and any breach of it in this regard should be dealt under the personal data breach procedure set in Article 92 EUI DPR.
i. On Article 3(5): the article states that the Agency shall only take data protection responsibility once the verification processed referred to in Article 13 of the presented draft is finalised and the data is accepted into Frontex processing files. This entails that the Agency bears no responsibility over the data being collected, rendering this part of the processing of operational personal data unaccountable. Considering the extensive powers granted to the Agency, in particular in relation to the collection of operational personal data by the Standing Corps, t**he DPO strongly recommends shifting data protection responsibility to include the moment of collection,** if that is done by Frontex capabilities. As a general remark, the DPO recommends that a through distinction is made between the Agency’s data protection responsibility and the MSs data protection responsibility. Article 3, 4 and 5 of the presented draft should aim at that.

(5) On Article 4: equally to the previous Article, **the DPO recommends changing the title** and refer to controllership of the Member States, not necessarily to the law enforcement competent authorities as it is plausible that some of the authorities the Agency conducts operations with may not be considered at national level as competent authority for the purposes of implementation of the Law Enforcement Directive. Consequently, the DPO recommends maintaining the wording on this article neutral to allow MSs to decide in accordance with their national legislation and internal division of tasks and competencies. Additionally, **the DPO recommends referring to those obligations by explicitly referring to their equivalent provisions in the Law Enforcement Directive, particularly with its Article 7**. Additionally, the DPO suggests making direct reference to the obligations pertaining to data accuracy on the Law Enforcement Directive.

(6) On Article 5: This provision states that there may be cases where there is a joint controllership between the Agency and the Member States, and that shall be governed by Article 86 EUI DPR. Article 88 EBCG Regulation explicitly contemplates the possibility of having a Joint Controllerships. **The DPO recommends referring that a Joint Controllership may occur within the operational activities referred to in Article 88 EBCG Regulation**. The DPO also recommends that, should that occur and lead to the processing of operational personal data, **to include the reference to Article 86 EUI DPR applicable to Frontex and Article 21 of the Law Enforcement Directive for the Member States**.

   a. On Article 5(1): the provision refers that the data collection plan shall contain the necessary requirements needed when there is a joint controllership. However, it fails at referring the most important part of why an arrangement between joint controllers is needed, which is the assurance of data subject rights. **The DPO recommends adding to this provision that the data collection plan shall contain provisions in respect of the exercise of data subject rights and the roles of each party on that regard**. Additionally, the DPO recommends that the data collection plans are made available to the public to ensure the transparency principle.
   b. On article 5(2): the ensuing provisions intend to allocate responsibilities in the case of joint controllership. The presented draft is unclear in relation to what situation this division of responsibilities refers to. As mentioned above, joint controllership occurs in the framework of Article 88 EBCG Regulation. Consequently, the **DPO recommends clarifying when this division of data protection responsibilities occur**.
   c. On Article 5(2)(a) **the DPO recommends adding "when operational personal data is provided by Member States" and reviewing the moment of assumption of responsibility**. Additionally, the Agency cannot "ensure" the highest standards on systems which is not responsible for. Therefore, the DPO suggests rewording to "shall seek assurance".
   d. On Article 5(2)(b) **the DPO recommends adding "when operational personal data is provided by Member States"** and to consider the previous recommendations regarding controllership and its starting moment.
   e. On Article 5(2)(c) **the DPO recommends rewording the obligation to make it more assertive**, e.g.: "the Agency shall ensure that the information related to the processing of operational data and the exercise of data subject rights are clearly communicated on its website".
   f. On Article 5(2)(d): in line with the need to link the joint controllership to the reference provided in Article 88 EBCG Regulation, **the DPO recommends to address properly the division of responsibilities when notifying personal data breaches** to the corresponding data protection supervisor in these cases.

(7) On Article 7:

   a. On article 7(4): this provision states that the Executive Director may decide, in consultation with MSs, the extend under which the Agency's staff may process operational personal data. However, the Agency processes operational personal data in several situations where the participation of Member States may not be required (e.g.: when collecting it from social media monitoring or when receiving it from Europol or Eurojust). Consequently, the presented formulation puts an unnecessary burden on Member States to be consulted on processing activities that are purely carried out by the Agency. **The DPO recommends linking this need to those activities carried out under the operational activities referred to in Article 88 EBCG Regulation**. Additionally, the DPO recommends further detailing what processing activities the Agency's own staff would be further addressed by means of an Executive Director Decision, considering that the definition of "processing" entails almost any activity that can be conducted upon personal data.

(8) On Article 8: this article strongly relies on processing of personal data that has been originated by the usage of EUROSUR capabilities or within the EUROSUR framework. The DPO has repeatedly advised the Agency to consult the EDPS with regard to the processing activities that can be undertaken under EUROSUR framework, considering the existing inconsistencies between Article 18, 28, 89 and 90 EBCG Regulation.

a. On Article 8(2): This provision refers to the activation of EUROSUR Fusion Services when these are requested by Member States, and in order to allow the processing of personal data that would consequently occur, and following informal consultation with the EDPS, the DPO advised the Agency to establish that Frontex acts as a processor when the Member States makes an EUROSUR Fusion Service request. In this light, the provision refers to those requests being under the “ownership” of the requesting Member State. The reference to “ownership” has not been defined in the text and may lead to misunderstandings. **The DPO recommends adding a provision under Article 4 of the presented draft referring that Member States retain the ownership of their data**, following the principle of ownership, also embedded in the Europol Regulation.

(9) On Article 9: The Article’s title refers to the obtention of operational personal data “in the course of operations”. However, throughout the article those operations are not referred to. Through several meetings the Agency has been adamant in expressing its views that “operations” refer to any activity conducted by the Agency. Thereupon, there is no specification in this article besides stating it may do so while fulfilling all its tasks. However, Chapter IX only applies when the Agency undertakes the task of Article 10(1)(q), which consists in cooperating with Europol and Eurojust and providing support to Member States when requiring operational and technical assistance at the external border. Article 87 EBCG Regulation lays down the purposes for which the Agency is legally entitled to process personal data. The operational activities referred therein refer only to the processing within joint operations, pilot projects, rapid border interventions and migration management support teams only. Consequently, **the DPO recommends that “in the course of operations” is directly linked with the processing activities referred to in Article 87 and 88 EBCG Regulation** where the Agency may process operational personal data while carrying them out.

a. On Article 9(b): the provision entitles the collection of operational personal data while conducting border surveillance. However, the provision is worded in such a way that may lead to the understanding that the Agency conducts border surveillance for the prevention, detection and fight of cross border crime. Border surveillance is conducted, in accordance to the Article 13 of the Schengen Border Code, to prevent unauthorised border crossings, to counter cross-border criminality and to take measures against persons who have crossed the border illegally. The Schengen Border Code is the secondary legislation that implements Article 77(2) of the Treaty on the Functioning of the European Union (TFEU), which falls under Chapter 2, Part Three, Chapter V that sets the area of free movement and calls for a harmonised border control. The proposed wording may act as a function creep of the mandate given to the Agency, which is primarily related to border management and border control to assist Member States. Consequently, **the DPO recommends to redraft the provision referring to the detection, prevention and fight of cross border crime** and link it specifically to the tasks of the Agency in relation to usage of border surveillance in accordance with Articles 87, 88 and 89 EBCG Regulation.

b. On Article 9(d) the DPO **suggests adding “in accordance with Article 8 provisions”** to ensure that the processing of personal data obtained in the framework of EUROSUR is complied with also under the course of operations.

c. On Article 9(e) the DPO **recommends adding the reference to the purpose limitation embedded in Article 87 and the operational activities referred to in Article 88 EBCG Regulation**.

d. On Article 9(f) the **DPO recommends, similarly to the above, to limit it in line with the purpose limitation and the operational activities of articles 87 and 88 EBCG regulation respectively**.

(10) On Article 10: The presented article is unclear, in particular in relation to the last part of the paragraph stating, “risk analysis for the purpose of identifying suspects of cross border crime”. **The DPO recommends clarifying whether the Agency will undertake risk analysis activities as defined in Article 29 EBCG Regulation on the processing of operational personal data**. If that is the case, the DPO recommends elaborating these rules further into the risk analysis activities undertaken which must be in line with Article 29 EBCG Regulation.

(11) On Article 11: The outcome of the workshop organised with the Member States in August 2021 brought forward the common understanding that in the national positive law there is no provision referring to criteria to consider a person to be involved, on reasonable grounds, in the commission of a criminal offence. Equally, the Regulations of Europol and Eurojust do not have any specific criteria to define “reasonable grounds to suspect”. **The DPO**

considers this entire provision should be deleted. And only add a justification to provide sufficient information as to the reasons why a person is suspected of involvement in cross border crime in Article 12, referring to general conditions.

a. On Article 11(3): the provision states that the Agency shall verify the reasonable grounds to indicate a person as a suspect, regardless of whether the data has been provided by Member States, Europol or Eurojust. The Agency may be able to assess whether they are competent for the processing of operational personal data, but it is highly doubtful the agency has the capacity to verify whether an individual is suspected of being involved in cross border crime under national law by a national competent authority. **The DPO recommends this provision only applies when the data is collected by the Agency's own staff**. Additionally, Article 13 of the present rules does not contain any provision related to the verification of the "reasonable grounds to suspect".
b. On Article 11(4): equally to above, **the DPO recommends wording that provision as a positive obligation both to the Agency and the Member States**. For the latter, the corresponding provision (Article 7 of the Law Enforcement Directive) should be referred. Both provisions in **Article 11(3) and (4) should be in the general conditions for the processing of operational personal data**.

(12) On Article 12:

a. On Article 12(2): the provision states that the Executive Director may establish the template of the data collection plan. Considering that the data collection plan may to be part of the operational plan, **the DPO recommends that the template, if necessary, is to be consulted with the Member States**.
b. On Article 12(3)(a): the provision states that further conditions upon the exchanging of operational personal data may be contained in the working arrangements to be concluded with Europol and Eurojust, and in accordance with Article 68 EBCG Regulation. **The DPO recommends removing the "and"** as it may lead to a different interpretation.
c. On Article 12(5): the provision further specifies the repurposing allowed in Article 87(2) EBCG Regulation. **The DPO recommends adding that the required compatibility assessment shall be done in consultation with the DPO**.
d. On Article 12(6): the provision indicates that exchanges on operational personal data done via outside the established channels shall be logged for monitoring and evaluation purposes. The **DPO recommends moving the part referring to logging data sent outside the agreed channels under the Article referred to logging**. Additionally **the DPO recommends to add further clarification in regard to the monitoring** (It can only be assumed that is data protection compliance monitoring, yet not explicit) **and logging for evaluation purposes** (it is not clear what is to be evaluated and it may enter in contradiction with the article referred to logging).

(13) On Article 13: for reasons of clarity and a proper allocation of competencies, the **DPO recommends splitting this Article into two articles**, one referring on the verification of the data collected by the Agency and a second one on the acceptance of the data received by the Member States, Europol and Eurojust.

a. On Article 13(2): the provision states that operational personal data shall remain in a restricted database during the process of verification and that it shall be separated from other data sets. **The DPO recommends not to refer to databases as it would not be technological neutral. Equally, the DPO recommends specifying what it is meant by restricted**, as it may lead to understanding that the information is classified or contained in a classified network. If that is the case, the provision should be clearly stating that. Lastly, it is not clear what is meant by "other data sets", so the **DPO recommends clarifying whether it refers to sets in the same repository regardless of the verification phase or whether it refers to data files**.
b. On Article 13(5): the provision states that the Agency may reject reports containing operational personal data. **The DPO recommends deleting the reference to reports**, as the operational personal data may not necessarily come in that format. If the Agency wishes to receive reports, it should state so in a positive obligation under general conditions for the processing of operational personal data.
c. On Article 13(6), the **DPO recommends rewording the entire provision to make it grammatically correct. Additionally, in the second sentence, "additional material" should be changed to "additional information"**, as "material" is an unclear concept. **Lastly, the reference to "if applicable" should read as "when requested"**.
d. On Article 13(8), the provision establishes the need for the Agency to inform the host Member State. As the Agency may obtain operational personal data from other sources not particularly linked to a Joint

Operation, **the DPO recommends linking this obligation to the cases where there is a host Member State**, by referencing Article 88 EBCG Regulation. This recommendation is issued notwithstanding the general recommendation related to the scope of “in the course of operations”. The DPO recommends rewording the entire provision, stating that the host member state shall be informed of the outcome of the verification process and of any further transmission of their operational personal data.

(14) On Article 14: the reference of access to the operational personal data by the Agency is not clear. The DPO recommends clarifying if the access referred to relates to access controls and permissions granted. Additionally, the principle of “need to know”, which is embedded under the principle of “Integrity and confidentiality” of Article 71 EUI DPR, and the measures on equipment access control, data media control, user control, data access control and storage control are not sufficiently implemented in this provision. **The DPO recommends establishing different access levels and controls in relation to the different processing activities to be undertaken by the Agency’s staff** (i.e.: a member of the Standing Corps should not have the same level of access as a member of the unit that will be entrusted to provide data to law enforcement authorities).

a. On Article 14(2) **the DPO recommends deleting the expression “on behalf of the data controller”** as that expression denotes a processor in data protection terms. Internal entities of the Agency cannot act as processor of the Agency.

b. On Article 14(3): the provision states “for the purpose of analysis and transmission of operational personal data”. The provision seems to introduce an additional purpose which is not catered by Article 90 EBCG regulation. **The DPO recommends deleting it the “purpose of analysis”** as it is not compatible with the EBCG Regulation.

(15) On Article 15: **The DPO recommends to delete the data entity “photograph”**, as per the purpose under which is going to be used (the identification of individuals in an unique manner), the photograph should be considered as a special data category and as such is already reflected under Article 16 of the presented draft rules. Additionally, a photograph should be part of the person entity in the data model.

(16) On Article 16: the DPO **recommends including an additional point related to the obligation embedded in Article 76 EUI DPR to inform the DPO without delay when using special categories of operational personal data**.

a. On Article 16(1)(f) **the DPO recommends adding that the physical characteristics referred to are not likely to change** (e.g.: tattoo or missing finger). The reason is that, for the purpose of identification of a data subject, the processing of physical characteristics likely to change may render the purpose impossible in order to cater for matches in the database.

b. On Article 16(1)(g) **the DPO recommends deleting the reference to Article 3(18) on the definition of biometric data**. As stated above, the definitions of the EUI DPR apply.

c. On Article 16(2)(e) th**e DPO holds strong reservations about the necessity to process data related to sexual orientation** for the purpose of identifying suspects of cross border crime.

(17) On Article 18: **The DPO recommends clarifying whether all conditions mentioned in 18(1) and 18(2) are cumulative** or whether any of the criteria can indicate that identification has been achieved.

(18) On Article 19:

a. On Article 19(3)(a)(**III**) **the DPO recommends adding that the submission of a justified request by a Member State, Europol or Eurojust is done in writing** and the provision states it explicitly, to avoid the so-called “fishing expeditions” and maintain necessity and proportionality principles.

(19) On Article 20: **the DPO recommends adding a provision under 20(1) that the exchanges between these agencies will be further detailed in the working arrangement foreseen in Article 68 EBCG Regulation and adding in a recital tha this article only applies to the transmissions performed by Frontex**.

a. On Article 20(3) **The DPO recommends clarifying that this provision refers to the Agency, not to the data controller**, as Europol and Eurojust may also act as data controllers for their own data.

b. On Article 20(4): **The DPO recommends that this provision is removed from the text** and reused in the text of the working arrangement.

c. On Article 20(5): this provision seems to give carte blanche to bulk transmissions to Europol and Eurojust as long as one of the criteria mentioned above is used, which in practice would qualify for the majority of the data processed by Frontex. This provision depletes the principle of necessity and proportionality, which should be done on a case-by-case assessment. **The DPO recommends deleting it or to modify it to ensure that the transmission is fulfilling the condition of necessity** for the performance of the other agencies’ tasks and proportionality for the envisaged purpose. Additionally, this provision contradicts Article 13 on the verification and acceptance process.

d. On Article 20(6) **the DPO suggests rewording or deleting this provision**, as it is unclear what it the provisions intended for.
e. On Article 20(7) **the DPO recommends deleting this provision and reuse it in the working arrangements** with these agencies as it seems to be a provision related to the administrative practices to be held by the agencies. Precisely, the reference "for monitoring purpose" seems unclear what it intends to monitor, the performance of the arrangements, the exchange, or the compliance.
f. On Article 20(8): this provision links onward transmissions performed by Europol or Eurojust to the need to have a working arrangement as mandated by Article 68 EBCG Regulation. Article 68 covers the transfers made by Frontex to these agencies but does not cover specifically onward transmissions by these agencies to, for example, third countries. **The DPO recommends rewording this article to state that onward transmissions by those agencies shall be covered in the details of the working arrangements and shall be performed in full compliance with fundamental rights, including data protection**.

(20) On Article 21: The DPO suggests adding a recital on the processing of personal data of minors. Additionally, **the DPO strongly recommends aligning these provisions with the he European Parliament and the Council adopted Directive (EU) 2016/800 on procedural safeguards for children who are suspects or accused persons in criminal proceedings**, passed on 11 May 2016. The protection of the privacy of children who are suspects or accused persons in criminal proceedings is very important. The necessity of such protection is also recognised in international standards such as the UN Convention of Rights of the Child. Involvement in criminal proceedings risks stigmatising children and may have – even more than for adult suspects and accused persons – a detrimental impact on their chances for (re-)integration into society and on their future professional and social life[2]. According to its Recital 56, "the privacy of children during criminal proceedings should be ensured in the best possible way with a view, inter alia, to facilitating the reintegration of children into society". Consequently, the processing of children suspected of involvement of cross border crime should come with sufficient safeguards to facilitate this reintegration and should avoid as much as possible blank transmission to law enforcement authorities, Europol or Eurojust. The presented provision makes a distinction to limit its processing only for those minors between 15 and 18 years old, which the DPO finds balanced when paired with the need to strictly justify the reasons for its processing. The DPO would additionally welcome an extra safeguard related to data retention, to ensure that the data held by the Agency does not remain in the processing systems for an unlimited or excessive period of time and that once it is promptly forwarded to competent authorities, the data is deleted.
Furthermore, considering the international standards on the rights of the children, the DPO sees the processing of minors being victims or witnesses excessive and not proportional to the purpose of identifying a suspect and thus **recommends to amend the draft article, banning the processing of data of minors when these are victims or witnesses**.

(21) On Article 22: **the DPO recommends splitting the Article in two different Articles**, one related to the conditions of review and storage, and another one on the conditions for deletion and anonymisation of data, for clarity of the reader.

a. On Article 22(1) the DPO **suggests rewording the article and link it with previous recommendations establishing the ownership of data to the provider** (e.g.: The Agency shall store the data in a way that allows establishing the ownership of the data"). .
b. On Article 22(2), in line with previous recommendations, **the DPO recommends that the time retention period does not start at the moment of verification or acceptance of the data**, but at the moment of the effective processing of the data, in line with Article 91(3) EBCG Regulation, that states that the review shall start at the moment of the initial processing of the data. By means of application of the definition of "processing", that means either when the Agency collects the data by its own staff or when it receives the data by the Member States, Europol or Eurojust. Additionally, the DPO recommends simplifying the provision when using the wording "data will be stored (…) until its purpose is achieved or where the identification of the suspect has not been successful, until data expiry". The wording should clearly state that the Agency is adopting additional safeguards stating that, when identification is not possible within a specific time frame (24 months) the data will be deleted regardless. Furthermore, **the DPO recommends adding, in line with the recommendation related to minors, the safeguard that minors' data will be deleted once the data has been transmitted to national competent law enforcement authorities**.

[2] https://www.corteidh.or.cr/tablas/r35645.pdf

c. On Article 22(3): the provision states that the business units shall undertake the duty to review the need for continuous storing. In line with point 2 of this opinion, the draft suffers from a clear picture of who does what internally. Consequently, the vague reference to business units undertaking the duty of review cannot establish the internal accountability required by the EUI DPR in terms of compliance with data protection obligations. The accountability principle is even more important when processing personal data which is very sensitive in nature and when, like in this case, there are multiple entities participating in its processing under different roles, be it when collecting, structuring, retrieving, altering, storing, or transmitting operational personal data, to name a few examples. **The DPO strongly recommends to clearly allocate internal responsibility for ensuring retention obligations** or at least to refer that such internal allocation of responsibilities will be established by means of an Executive Director Decision.
d. On Article 22(4) a reference is made to stricter retention periods being applied since the moment of verification. **The DPO recommends establishing the start of the retention period at the moment of the initial start of processing**, in line with Article 91(3) EBCG Regulation and the recommendation issued under draft Article 22(2) above.
e. On Article 22(5): the provision links the continuous storage of personal data of victims and witnesses to the condition obtaining the identification of the suspect. However, Article 90 conditions the processing of personal data of victims and witnesses to the fact that their data must supplement the data of a suspect. **The DPO recommends that the review and subsequent deletion of personal data of victims and witnesses is conditional to providing additional information on a suspect**, and if that fails, their data should be deleted at a shorter span following a review, in order to avoid undesirable consequences for being in a pan-European criminal database, such as revictimization.
f. On Article 22(6) and (7) **the DPO recommends their deletion** as it repeats the provisions above.
g. On Article 22(8) the DPO recommends, in line with comments above on anonymisation, **to amend the article and indicate that the anonymisation must prevent direct or indirect identification of the suspect by Frontex when the Agency conducts its tasks**, in line with the definition of personal data of Article 3(1) EUI DPR.
h. On Article 22(10), **the DPO recommends further clarifying the wording** "entry for compliance checks" is or rewording it as "the system shall create an entry on flagged data for data protection compliance checks".
i. On Article 22(12) the DPO **recommends to explaining what this logbook is**, as it is a concept that is newly introduced in the text. It can be done, for example, by means of a recital. Additionally, the DPO recommends stating what the minimum content of such logbook should be, by whom should it be kept, who is authorised to perform manual deletion and to further clarify the reference to checks being performed. Alternatively, the DPO recommends to state that such concepts will be further elaborated by means of an Executive Director Decision.

(22) On Article 23(3), **the DPO recommends aligning the wording of this provision to the tasks granted to the DPO in Article 45 EUI DPR**, which is the assurance of compliance with data protection obligations, instead to "control purposes".

(23) On Article 24, **the DPO recommends moving this Article to general conditions** for the processing of operational personal data, as it is not linked to the title of the Chapter (Data Retention) and it is applicable to all parties processing operational personal data. Additionally, the DPO would like to point out that the Agency cannot receive operational personal data marked as HC0. In case a provider of data would indicate this Handling Code, it would mean that it is stating that the Agency can only use the information provided for the prevention, detection investigation or prosecution of cross border crime, which would fall out of the mandate of Frontex. **The DPO suggests rewording this Handling Code with an alternative**: "For the prevention, detection, investigation or prosecution of cross border crime in accordance to national legislation or for the purposes of Article 90 EBCG Regulation".

(24) On Article 25: equally to the above, **the DPO recommends shifting this Article to the general conditions** for the processing of operational personal data.

(25) On Article 26(1): The **DPO recommends adding a reference that the privacy statement is made in compliance with Article 79 EUI DPR**.

(26) On Article 27(1): The **DPO recommends that the register of documented restrictions is kept by the DPO**, equally to the register of processing operations, of international data transfers or of personal data breaches.

(27) On Article 28 and 29, **the DPO recommends the provision is added to the Article referring to the Agency as Data Controller** (Article 3 of the presented draft), as it is already referred to in that provision and to delete then Articles 28 and 29.

(28) On Article 30: The draft basically repeats the provisions of notification of personal data breaches contained in Article 92 EUI DPR, which are directly applicable to the Agency. Additionally, the register of personal data breaches is kept in a centralised manner by the DPO, contrary to what it is stated in Article 30(2). **The DPO recommends deleting the Article**.

(29) On Article 31: Similarly to the above, the notification of a personal data breach is well established and detailed in Article 93 EUI DPR. **The DPO recommends deleting this Article and refer to the obligation to notify jointly with the Member States only for those cases where there is a joint controllership,** and that the procedure of notifying data subjects should be contained within the joint controllership agreement.

==