FRONTEX

Warsaw, 16 November 2021
Reg. No 11364a
Ref: DPO/ /11364a/2021

Opinion of the Data Protection Officer- part II

Draft Implementing Rules on Operational Personal Data

1. Introduction

The purpose of this document is to provide the Management Board and the Executive Director with the second DPO Opinion on the Implementing rules of the Agency for the processing of operational personal data.

2. Analysis

- As a general comment, the DPO cannot refrain from pointing out that such rules should be included in the legal text of the Decision rather than in an annex.
- Recital 6 needs rewording - it needs to explain that the Agency processes personal data under the DPR for the purposes of fulfilling its tasks of Article 10 for the implementation of IBM as defined in Article 87 EBCG. However, when those tasks relate to the exchange of data with Europol and Eurojust (so they can fulfil their mandate) and with MSs LE (for the purpose of detection, prevention, investigation, prosecution of criminal offenses) the Agency shall process operational personal data in accordance with Chapter IX EUI DPR and 90, thus establishing a clear link that the only task for which it can be using Chapter IX is the task of Article 10(1)(q). The way the current wording stands is confusing and seems to assume that the task of Article 10(1)(q) empowers the Agency to do prevention, detection, investigation and prosecution of cross-border crime. However, a careful examination of the task laid down in Article 10(1)(q) states the extend of the task for which Frontex may use Chapter IX EUI DPR, that is when cooperating with Europol, Eurojust and MSs in circumstances that require an increased technical and operational assistance at the external border for the fight against CBC and terrorism.
- Recital 8 does not provide the required necessary causation to demonstrate that special categories are strictly necessary for the identification of a suspect of cross border crime, as required by Article 76 EUI DPR. The DPO would like to highlight that the legal threshold to be met is not a “nice to have” but a strict necessity. Therefore, the Agency needs to demonstrate that without these data categories, the purpose cannot be achieved. The DPO advices that specific cases are described (if there is any) where sexual orientation information has been necessary to conduct an identification (i.e.: should we have known this person was homosexual we would have been able to distinctively identify the individual). It can do so building up on its past experience, where for instance some special data categories were not allowed by the EDPS. If the Agency indeed has this strict necessity, it would be able to recall occasions where the lack of this information jeopardized the attainment of its purpose.
  Back in 2015, Frontex already stated to the EDPS that ethnicity and sexual orientation was necessary to, respectively, “uncover connections between traffickers/smugglers as they sometimes mostly smuggle/traffic persons of their own ethnic group (“homophily”) and that migrants are routinely sexually abused by smugglers/traffickers”. It is important to point out that at that time, the Agency could use personal data for the purpose of risk analysis, which may allow to use a wider range of data categories. In relation to the processing of ethnicity, the EDPS stated that appropriate safeguards should be contained in Frontex rules to ensure, in the absence of such safeguards in the Frontex Regulation itself, that the data is not used to conduct discriminatory practices. Therefore the DPO recommends adding safeguards to the draft rules , for example, stating that whilst searches purely based on sensitive personal data is forbidden, the DPO will check that no such searches are conducted; additionally, the DPO recommends to include as a safeguard, as another example, that when ethnicity is used, to specifically state of what data subjects would it be applied to - only

for suspects, not for victims or witnesses -, and to include specific and shortened retention periods to sensitive data).

As per sexual orientation data, the EDPS considered that the justification provided by Frontex (the possible abuse conducted by smugglers) would constitute information about a suspected criminal offence, not about the sexual orientation of the suspected offender. The recital fails at explaining why this data category is necessary, only states that it is important. Equally, the recital fails at explaining why philosophical beliefs, religion or political opinions are necessary to the purpose of identifying a suspect of cross border crime.

- On Article 2(k), the DPO recommends using the widely accepted definition of deletion, referring to it as "hard deletion" (also aligned with COM comments), to make sure that no soft deletion takes place. It is not clear what it is meant by "irreversible" deletion, considering that it may disappear from the database, yet be contained in the server. The deletion in both database and server is usually referred to as hard deletion and that is how the definition should be formulated. The concept linked to "reversible" or "Irreversible" is used for the anonymization or pseudonymization of personal data. Therefore, that word should be used in the appropriate definition on anonymization.
- On Article 2(l) the DPO recommends using the widely accepted definition of anonymous data given by the GDPR, the European Data Protection Board, the EDPS and the AEPD (Spanish Data Protection Authority)[1]: information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable". If you want to use it as a verb, define it as the "process of rendering"[2].
- On the title of Article 3: the title reads "data controller responsibilities of the Agency", the DPO would like to reiterate the incongruence of the title, as controllership entails data protection responsibilities. Consequently, the title is a repetition. The DPO prompts the Legal unit to change the title to "Frontex as Data Controller" or "Data Protection responsibilities of the Agency".
- On Article 4, on Joint Controllership, it is still not clear what entity is responsible for what. Consequently, although in full agreement with COM and DK comments that implementing rules cannot create effective obligations to sovereign MSs, there is still a need to distinguish in these rules when MSs are controllers and when the Agency is controller in order to effectively assert the data protection responsibilities of the Agency and distinguish those from MSs. This need is further highlighted by the fact that Frontex may collect personal data while conducting border management activities, which fall under the scope of the general part of the EUI DPR, and conduct subsequent processing activities related to the identification of suspects under Chapter IX. This entails that the main bulk of the personal data, at collection time, would be collected under Article 88, where controllership at national level may differ from the authorities referred to under Article 90. This point is not clarified. Further, Article 4 does not give a clear understanding on who is responsible for what and what legislation applies in particular in relation to Article 4(b). Clarification in this regard is necessary, particularly in relation to the application of the data protection principles, the exercise of data subject rights, the data protection legislation covering the processing activities covered (collection, transmission) and what supervisory body is competent for what.

  Already in 2018, when the EDPS provided formal comments on the first proposal for the new EBCG Regulation, the Supervisor highlighted the lack of specification in relation to controllership: "Given the increase in the operational activities to be performed by the EBCG, and the associated increase in terms of EBCG's direct responsibilities, the EDPS considers that all (each and every) activities should be clearly specified having regard to: (i) the responsible entity (the EBCG, the Member States, the third Countries, international organization); (ii) the applicable data protection law (Regulation 1725 vs the General Data Protection Regulation or the Law Enforcement Directive); (iii) the data protection supervision system (the competent data protection authorities responsible, alone or jointly, for the oversight of the data processing)"[3]. This is also emphasized by COM comment pointing out at the moment of shifting responsibilities.

  Equally relevant is to point out that there cannot be a joint controllership with other Agencies. The DPO would like to remind that a controller is the entity that decides (wholly or partly) on what the purpose of processing is and what the means to conduct that processing are. A Joint controllership is when two parties (not necessarily in an equivalent manner) decide together on purpose and means. The purpose for Frontex is already provided by law ('the identification of suspects'). The means is decided by Frontex and/or the MSs,

[1] https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf
[2] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
[3] https://edps.europa.eu/sites/edp/files/publication/18-11-30_comments_proposal_regulation_european_border_coast_guard_en.pdf

as we can see in the discussions ongoing with these Implementing Rules. MSs and the Agency have joint operations in common, and a shared responsibility for the implementation of integrated border management. There is no joint or shared responsibility with Europol or Eurojust. Neither there is no situation where Frontex would decide together with them on purposes or means. Consequently, the reference of having a possible joint controllership with Europol and/or Eurojust is incorrect and must be removed from the text.
Considering that the issue of joint controllership impacts not only OPD but also the data processed under Article 88, and considering the far fetching consequences that the establishment of this Article has for the European Border and Coast Guard, including the Member States, the DPO strongly advices the Agency to consult these rules with the EDPS prior to approval via written procedure, as there may be the necessity to further discuss some aspects with national data protection authorities, particularly on the issue of division of controllership and supervision.

- On Article 8, the DPO urges the Agency to specify, as it is the objective of the implementing rules, what operations the article refers to. Particularly, the DPO recommends deleting (e), as it would be difficult to circumscribe social media monitoring activities under an OPLAN for an ongoing JO. However, as already discussed with the EDPS and DG Home, the Agency could consider setting up media monitoring as a Pilot Project or a JO on itself. However, this possibility cannot be done with the current wording of this Article, as operational activities are reflected in Article 87 EBCG Regulation. The same lack of specification exists in Article 9. Therefore, the DPO urges to further specify what those processing activities are. This Article, in addition, lacks the part of transmission, for being able to pass personal data from Article 88 to Article 90. With the current wording, the Agency would not be able to transfer data from one legal regime to another, with the subsequent loss that would entail in terms of the assistance to Europol, Eurojust and MSs LE Authorities.
- On Article 10, firstly, it currently refers to "the controller". Considering there is an article on Joint Controllership, it is not clear to whom this obligation is expected from. The DPO recommends referring specifically to the Agency. Further, the DPO upholds its previous advice to simplify the criteria on what it is to be considered as relevant grounds to suspect, and leave that to the experience of the Staff member to introduce the reasoning why a person is considered a suspect. This would enhance transparency and comply with the principle of accountability demanded to the Agency, while at the same time, not imposing an impossible threshold as it is the case now with Article 10(2). The self-imposed requirement to have "evidence" or "facts" will effectively reduce the data intake. Additionally, the requirement of having "two different sources" leads this to the field of investigation, not being clear what "sources" the information needs to come from (i.e.: is the Agency expecting to have informants?). Lastly, the DPO would like to point out on this article that the Agency will perform a verification on the "reasonable grounds to suspect", even if the data has been provided by MSs LE authorities, Europol or Eurojust. The DPO has strong reservations with regard to the Agency's competence to verify if information provided by Competent Authorities has sufficient grounds to suspect a person is involved in cross border crime. The Agency should circumscribe the verification process to see whether it fits in the Agency's mandate and whether the data can be used for the "identification of a suspect". Therefore, the DPO strongly encourages the Agency to reword that article, to reduce the criterion for considering a person is suspected of involvement on cross border crime, and to delete the requirement of verifying whether national competent authorities have performed an assessment of the reasonable grounds to suspect a person is involved in cross border crime. Failure to re-word the Article runs the string risk to alienate national law enforcement authorities, as it seems to be questioning their experience and mandate.
- On Article 14 and for the sake of clarity and correctness, the DPO recommends deleting the reference to photograph as an "entity". For the purposes of identification (which is the purpose granted to the Agency), a photo is a special data category. An entity forms part of the chosen data model and photo is a component of the person entity. Misalignment on this aspect seems to stem from a lack of understanding on criminal database models. UMF stands for Universal Message Format and it is a standard or agreement on what the structure of the most important law enforcement concepts when they are exchanged across borders should be. In other words, UMF is a set of concepts (building blocks) to construct standard data exchanges for interconnecting dispersed law enforcement systems[4]. The UMF building blocks are the most important, usually exchanged, or cross-checked concepts from a law enforcement viewpoint: Person, Organisation, Location, Item, Connection, Event — creating the 'POLICE' Information Model. Failure to delete this and

[4] https://op.europa.eu/en/publication-detail/-/publication/3b2cc49f-72bb-419f-8742-eb21cd15e35c

include "photo" in the correct category and entity disrupts the entire format that has been widely promoted by both COM and Council (e.g.: DAPIX discussions back in the mid-late 2000's) and more importantly, disrupts the normal composition of the databases of the LE partners the Agency is supposed to cooperate with.

- In relation to Article 16, as pointed out by COM, the Agency will cross check data against its own data bases and open sources. The DPO wants to remind the Agency that any processing activity upon personal data requires to have a legal basis. For the processing of OPD, the legal basis is the EBCG Regulation. Whilst it seems natural that the Agency checks if information on that person already exists in its own criminal database, it is highly doubtful that the Agency has a mandate to cross check data of potential suspects against open sources, which would include social media. The EBCG Regulation only refers to open sources and social media monitoring in one Article, referring to the usage of Eurosur Fusion Services. However, through this current provision, the Agency seems to arrogate the capacity to police the internet and to use it as a source to conduct identification of suspects, which would be done in violation of the sources listed in Article 90 and the processing would be outside of mandate. For consistency, and as advised during the Meetings on this regard, the DPO again recommends to:

  - Specify what the open sources referred to, whether these refer exclusively to commercial databases, to publicly available sources public data and/or internet, or;
  - Following the recommendation above, reword Article 8 referring to "in the course of operations" and include the possibility to conduct an e-Joint Operation.

- On Article 23, the DPO wishes to reiterate that HC0 is not applicable to Frontex, as Frontex has no mandate for using the data for the prevention, detection, investigation or prosecution of cross-border crime. The said Handling Code entitles the receiver of the information to use it for prevention, detection, investigation or prosecution of cross border crime. Additionally, it also states that the information is to be used by the receiver in accordance with Article 90. This wording is incongruent as it would bind the receiver to the compliance of a Regulation that only affects Frontex. If Europol would receive a message marked with HC0 form Frontex, effectively it means that Frontex is telling Europol to use the information in accordance with Article 90 of the EBCG Regulation. The DPO prompts the Agency to use the implementing rules to state that those provisions are to be used in line with each party respective mandate, and that HC0 is not applicable to Frontex.

  Furthermore, the implementing rules remain silent on the purposes for which personal data can be received. The DPO recalls the obligation of Article 87(1) EBCG Regulation which states that "Member States and their law enforcement authorities, the Commission, the EEAS, and those Union bodies, offices and agencies and international organisations referred to in points (c) and (d) of paragraph 1, that provide personal data to the Agency shall determine the purpose or the purposes for which those data are to be processed as referred to in paragraph 1". Yet the implementing rules, and in particular this Article on Handling Codes, fail at indicating for which purpose (of those specifically allowed to Frontex under Article 87) the personal data is being sent. The Agency could consider amending the current HC0, considering that it is out of mandate for the Agency's usage, and include the effective implementation of the legal obligation stemming from Article 87(2) EBCG Regulation.

- In relation to the exercise of data subject rights in Article 25 and 26, the DPO would like to recall the recommendations issued by the EDPS on the Implementing Rules for the DPO of 10 November 2021. Recommendations 6, 7 and 8 deal on how the Agency has established the internal procedure for the response of data subject rights. In particular, the EDPS expects the Agency to have a centralized inventory of data subject requests, preferably under the responsibility of the DPO; the EDPS also expects an amendment aimed at clarifying how requests involving more than one entity will be handled by the Agency (not to mention then how would requests be handled by the Agency when these involve more than one entity and more than one MSs or JHA Agency) and lastly the EDPS expects the Agency to align all implementing rules. Consequently, once the rules on the DPO and designated controllers are amended, should either refer to the procedures also related to OPD data subject rights, or these rules on OPD should already contain similar provisions to ensure that both rules are aligned.

3. Conclusions

On 7 October, the DPO issued close to hundred recommendations on the first draft OPD rules, for which the Agency only took onboard roughly half of them, with no subsequent communication or information after the release of the

first DPO Opinion. The DPO would like to highlight that while interests of the Business Units are undeniably important, these interests cannot be achieved by breaching compliance with EU legislation.
The main concerns on OPD remain: there is a serious risk of function creep in relation to the Agency's mandate, there is a lack of clarity in relation of roles and responsibilities, and the actions that the Agency intends to perform on OPD are not following the principle of purpose limitation.
In case the Agency intends to approve these implementing rules in its current shape, the DPO recommends to consult the EDPS prior to adoption, to ensure that the Agency fulfils its obligations in respect of the EBCG and the EUI DP regulations, as well as to avoid unnecessary delays and the need to amend the decision shortly after its adoption.

==========