FRONTEX

Warsaw, 3 December 2021
Reg. No 13609
Ref: DPO/ /13609/2021

# Opinion of the Data Protection Officer

## Draft on General Personal Data Processing Implementing Rules

## 1. Introduction

The purpose of this document is to provide the Management Board and the Executive Director with the DPO Opinion on the Agency's general data personal processing implementing rules.

## 2. Background

On October 18, the DPO was consulted on the scope that these general rules would contain and was given as deadline for answering the 21 October. The DPO provided what aspects, it its opinion, the rules should cover.
On 26 November, the DPO received a text from the Legal Unit, with the request for the DPO to provide comments not later than 3 December. While the DPO notes that on this occasion, the agency has given more time to comment on the presented rules, the DPO notes that the obligation of consultation "properly", as mandated by the DPR, has not been followed. The DPO is aware that consultation with business units has taken place, however the DPO has not been invited to participate in them. The DPO would like to point out that these implementing rules (IR) bind the agency for the processing of personal data in general, including for the purpose of completion of administrative or operational tasks that fall under the general part of the DPR. Consequently, it has a far-reaching impact, and early involvement of the DPO would have been desirable to ensure a balanced text.

Further, the DPO would like to point out that the exclusion of EUROSUR from the scope of these rules gravely affects the application of the implementing rules. As communicated on several occasions, EUROSUR has a dual nature for the purpose it intends, as per Article 18 EBCG Regulation. Its exclusion from these rules brings numerous uncertainties to the correct application of the DP acquis for the Agency. Equally missing, there is no internal transfer mechanism that caters for the transmission of data collected under Article 88 to Article 90. There should be a reference to this possibility.

## 3. 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. Also, would like to bring to the attention the change of wording convention on the title of the rules. This serves the purpose to link its scope with the correct part of the DPR, giving it its overarching nature.
- On recitals:
    - (3) The DPO suggests rewording and make specific reference to the application of Chapter IX for OPD.
    - (4) this recital seems superfluous – IBM does not necessarily need to be linked to processing of all the data the Agency is allowed to process, including those administrative tasks. The agency processes PD for the purposes stated in article 87.
    - (5) The DPO suggests linking this recital to the recital above, linking the purpose of administrative tasks to the establishment and monitoring of the SC, including for ensuring compliance with FR and the Charter, which may cater for a certain level of intrusion upon privacy of the members of the SC and other individuals.
    - (6) The DPO has serious concerns over the legal basis giving a new purpose not foreseen in the EBCG Regulation. Art 88 does not explicitly foresee the purpose of identification of vulnerable groups, but

allows the processing for risk analysis, organizing JOs, returns, facilitation of information and EUROSUR (following Article 88(1) para.2). Considering that the purpose needs to be explicit, and legitimate, the DPO sees a high risk of non-compliance with the EBCG regulation when creating a new purpose of identification of vulnerable groups, (and its individuals), and a possible violation, should it go ahead, of the principle of necessity and data minimization. Those same serious concerns apply to the processing of special data categories, including the medical data referred to in the next recital.

- (7) The DPO would like to point out that there is no purpose limitation embedded in this processing activity. This recital refers to transmission, and such processing activity cannot be a blank transmission as it would not respect the principles of necessity and proportionality. The DPO suggests adding specific provision stating that the transmission shall be done following those principles, following a case-by-case basis assessment. Additionally, then the reference to deletion can be added, although it seems superfluous considering its already an obligation catered by the EBCG Reg.
- (8) Repetition of EBCG Reg – the DPO suggests deleting.
- (9) the recital seems to establish what the purpose of having implementing rules is. It is unclear what this provision intends. Suggestion to delete.
- (10) Repetition of above recital which establishes that excluded OPD from scope. Suggestion to delete.
- (11) Please see that the last draft on OPD rules seen by the DPO contain provisions affecting the issue of controllership. Consequently, reference to those IR should also be mentioned here.

- On article 1: Should be further explained in the corresponding recital why OPD is excluded (in application of chapter IX) otherwise it is a mere repetition of the recital. Also please note that you cover all the purposes foreseen in the EBCG, including EUROSUR. Yet there is no article on EUROSUR, nor when it applies Chapter IX and the conditions to apply the general part of the DPR. Additionally, the scope also excludes the part on controllership as it is in another MB Decision, and this is not mentioned.
- On Article 2:
  - (a) Note that the EDPS commented on this definition, and alignment may be required.
  - (b) & (c) Ensure to align the definitions as the definitions foreseen in OPD IR.
- On Article 3:
  - (1) The DPO recommends not to use joint controllership in practice for practical reasons and delete the entire article. In specific terms as it would ultimately create an unparalleled level of bureaucracy within the agency. There is only one controller, which is the agency. The reason for utilizing controllership in practice is to specifically allocate responsibility within the agency, in particular who has to implement the measures required by law. However, when there is a joint controllership, the DPR obliges to establish joint controllership agreements, as per legal obligation. That would but the Agency in the position to be asked for the JC agreements within the agency. The DPO strongly encourages to use the recommended practice that when 2 or more entities jointly decide on purposes and means, that the DP responsibility is elevated to a superior entity (DED or ED if necessary) to ensure that the Agency, as controller, complies with its legal obligations. Controllership in practice is simply a specification of responsibility within the agency; ultimately, controllership lies on the agency as such, and it is all levels on decision making (which determines controllership) that is bound for compliance.
  - (2) The DPO has doubts on the possibility to use IR to state that a provision of the DPR does not apply. Additionally, the Record does not fulfil the purpose of determining the DP responsibilities, but serves as a transparency tool and assurance of lawfulness, and the content of it is determined by law. Controllership in practice is a fiction, as explained above, as ultimately the controllership lies on the Agency itself. In order to avoid the need to have internal agreements at all times, the DPO would welcome the deletion of this article.
  - If the Agency is adamant at maintaining a provision of internal JC, the DPO recommends to:
    - Move all the provisions on controllership from the DPO IR to these rules for reasons of consistency and having all articles referred to it under one single document, instead of different scattered implementing rules;
    - Complement then the provision of controllers in practice with the following wording:
      *(a) Designated Controllership shall be allocated on the basis of the factual influence exercised over the processing operation, by virtue of decision-making power in respect to determination of purposes ("why?") and essential elements of means ("how?") of processing.*

(b) *Access to personal data is not a prerequisite nor a determining factor for allocation of designated controllership.*

(c) *In the event of multiple designated controllers exercising factual influence over the means or the purpose of a processing operation, the responsibilities of each designated controller on the processing activity and particularly on the exercise of data subject rights will be documented and communicated to the DPO at the time of drawing up a Record for processing operation.*

- On Article 4:
  - (2) The obligation to have a processing agreement is already covered in the DPR. This provision is a repetition. Recommendation to delete.
  - (4) The DPO strongly suggests not having ED decisions for standardized templates. Firstly, because the templates change on a regular basis, depending on EDPS guidelines and DPO network work; Additionally, the content of the agreement is already catered by in the DPR. Secondly because in some cases those standardized templates are already given by means of a COM or EDPS decision in case of TC processors, which make it a legal obligation to follow. Suggestion is to refer that templates ate available (as they are) and to consult the DPO as per point 1 of this article, so the DPO can address which template can be used and provide the guidance on what parts need to be adapted.
- On Article 5:
  - (2) The DPO suggests deleting this reference of internal arrangements or guidance by means of an ED Decision. It is the task of the EDPS to provide guidance on ITDs, together with the EDPB. Additionally, in relation to internal arrangements to conduct ITDs, please note that the topic is highly volatile and that would oblige the agency to constantly amend such decisions depending on the different outcomes and discussions held by the DPOs network, COM, EDPS and EDPB, as well as pending ongoing cases at the ECJ. The agency requires sufficient flexibility to amend clauses or redrafting them depending on the ongoing developments. In order to achieve the necessary flexibility and the required compliance, the DPO suggests that the DPO will make the necessary templates available.
- On Article 6:
  - (1) Deletion is recommended, as per repetition of the DPR obligation.
  - (2) (a & b): it is recommended to add a provision that the result of such assessments will be provided to the DPO.
  - (3) Please note that you may be reducing the scope of the security policy by referring only to IT tools and systems, while a personal data breach may come from any security incident, including physical security incidents. Thus, the security policy to be adopted should also have within the scope physical security incidents, which are relevant for PDBs, for risk identification and mitigating measures in DPIAs (e.g.: physical loss of CVs or personal files).
  - (4) Obligation of the DPR – unnecessary repetition
  - (5) Please add reference to "before the start of the processing" to ensure that the measures specified below are implemented.
- On Article 7: Please use the correct terminology, which is "personal data breach", to distinguish for any other data breach that may not contain personal data.
  - (1) Unnecessary repetition of the DPR. The DPO would welcome here an ED decision adopting a PDB handling policy for the entire agency avoiding ad hoc practices.
  - (3) The documenting of a PDB is already adopted by means of the MB Decision, Article 5(7). Additionally, the guidelines for assessing risks are already given by the DPO under its tasks. Furthermore, each personal data breach has a different assessment of risk for the data subjects, and it depends on a case by case scenario, following the methodology adopted by ENISA, recommended by the EDPS. The necessity of notifying the DSs is already given in the DPR, and part of the notification of the PDB to the EDPS already includes the necessity to inform the data subjects, as it is within their remit to indicate whether it would be necessary to notify the data subjects. Additionally, it is recommended to leave the modalities of the notification of the breach to the affected data subjects in a flexible manner, as the identity of the DS may greatly affect such modality. i.e.: when the data subjects are suspects, it is obvious that the agency is not going to communicate a breach individually, but a different approach may be used for example, general communication on the webpage; however, if the DSs are candidates in a selection, an individual notification should be preferred. Considering the need to assess on a case-by-case basis how

to conduct the notification, flexibility depending on each situation may be necessary, and an ED decision would not grant the sufficient flexibility and adaptability to each of the different situations that may arise.

- On Article 8
  - (3) Please note the missing reference.
- On Article 9
  - (2) The DPO welcomes the provision on logging. However, the DPO recommends rewording this provision as it may give room for interpreting that no logging would be required, despite of posing serious risks for the data subjects, if that logging is deemed disproportionate.
- On Article 10
  - (3) It is unclear what data subjects is this article referring to, as it can be also on the persons deployed within these operations. Recommendation to specify in this regard whose data subjects are we referring to. Additionally, there is no purpose specification in this provision, which covers exchange with the host MSs. However, there are other recipients of the data foreseen in the EBCG regulation, and Art. 88 establishes the purposes for exchange with those. Either there is a reference to article 88(2) or there is a concretion of the entities and the purposes following article 88(2).
  - (4) Please note that following article 87(2), TCs are not foreseen to transmit PD to the agency. Also said article foresees more actors transmitting PD than a host MSs.
- On Article 11: ensure that the provisions of OPD and these are aligned, as both rules refer to JOs as a source of PD collection.
  - (2) Please take into account the comment of DG JUST as per the JC agreement and the OPLAN.
- On Article 12: Please note that you are excluding voice recording, the DPO is not sure if this omission is done on purpose. The DPO welcomes the introduction of this article; however, the DPO would encourage the agency, in line with the recommendation above, to emphasize that this continuous monitoring serves the purpose of assurance of FR and as evidence gathering during UoF and SIRs. Additionally, it is not clear under whose controllership this processing operation. the DPO would welcome further specification in this regard.
- On Article 13: it is not clear the objective of this article. Please clarify.
- On Articles 14 & 15: there is a lack of specification on what data subjects we are referring to. Also, the DPO has reservations about the necessity to conclude here a data model, considering the variety of purposes, which may also be deployed and utilized in the context of JO. The DPO recommends deleting these articles and to use the flexibility of the Records and DPIAs for establishing the data categories and its possible amendment depending on operational needs, similarly to what it has been successfully done by ECRET. However, the DPO would very much welcome having reflected in these rules that Processing activities occurring under Article 88 also require Records and DPIAs accordingly.

  Further, please note that principle of data minimization applies in relation to its purpose. The Agency is thereby carving on IR a set of data categories with no assessment on necessity and proportionality depending on each purpose. The DPO proposes to delete and use the already existing tools foreseen in the DPR for regulating the processing of PD, thus gaining flexibility depending on operational needs.

# 4. Conclusions

Some of the earlier expressed concerns of the DPO remain here. There is a lack of clarity on the determination of internal responsibility, now scattered within three different implementing rules.
Further, there are omissions on these rules that will not bring any benefit to the Agency, such as the lack of foreseeing EUROSUR or the mechanism to transform a person who has cross the border without authorization to the umbrella of Article 90.

As conclusion, the DPO considers that these rules are not yet mature for presenting to the Management Board, and that more drafting is necessary for clarification and completion purposes.

==========