OPINION ON THE DATA PROTECTION IMPACT ASSESSMENT REGARDING EPPO'S PRE-ASSESSMENT ENVIRONMENT

(Case 2021-0422)

1. PROCEEDINGS

1. On 9 April 2021, the European Data Protection Supervisor (EDPS) received a request for prior consultation under Article 72(1)(a) of the Regulation (EU) 2017/1939 of 12 October 20171 ('the Regulation') regarding the Data Protection Impact Assessment (DPIA) on the Pre-Assessment Environment (PAE) of information provided by private parties, carried out in accordance with Article 71 of the Regulation. The notification sent by the European Public Prosecutor's Office ('the EPPO') contained a description of the processing environment, an assessment of the necessity and proportionality and a risk analysis and mitigation.

2. Together with the DPIA, the EPPO submitted the following documentation:

   a. College Decision 003/2020 - Internal Rules of Procedure of the European Public Prosecutor's Office ('IRP').

   b. College Decision 005/2020 – Rules concerning the Data Protection Officer of the European Public Prosecutor's Office ('RDPO').

   c. College Decision 009/2020 – Rules concerning the Processing of Personal Data by the European Public Prosecutor's Office ('RPPD').

   d. College Decision 012/2021 – Internal Rules of the European Public Prosecutors' Office on the protection of Sensitive Non-Classified Information ('RPSNC').

   e. EPPO CMS Solution Architecture v 1.0 of 17 April 2020.

   f. European Public Prosecutor's Office (EPPO) Case Management System (CMS) - Data Protection Implementation Analysis – FINAL, 23 July 2020.

   g. List of types of Information required in the web form.

3. According to Article 72(4) of the Regulation, the EDPS has to provide his Opinion within a period of up to 6 weeks of receipt of the request for consultation, with a possible extension by one month. The notification was received on 9 April 2021, thus the EDPS should render his Opinion by 25 May 2021.[1]

2. DESCRIPTION OF THE PROCESSING

1. The EPPO has been established by the Regulation with the competence to investigate, prosecute and bring to judgment crimes against the EU budget, such as fraud, corruption or serious cross-border VAT fraud.

2. As an EU body, which carries out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU, the EPPO processes operational personal data in line with the rules established in the Regulation and in its internal rules of procedure. The operational personal data will be processed in a case management system (CMS), pursuant to Article 44 of the Regulation.

3. The Regulation provides also a legal basis for temporary processing of operational personal data by the EPPO "*for the purposes of determining whether such data are relevant to its tasks*" (Article 49(4)). EPPO's internal rules and procedures have further defined this pre-assessment process, which will take place within a dedicated environment, namely the 'Pre-Assessment Environment' (PAE). The pre-assessment applies only to the information provided by private parties (natural or legal persons), as such submissions, according to the EPPO, are most likely to include irrelevant personal data.

4. The pre-assessment phase starts from the moment a private party provides personal data to the EPPO and ends when such personal data is either inserted in the CMS for operational purposes or rejected as manifestly outside the competence of the EPPO and either forwarded to other competent authorities, or returned, or deleted.

5. The PAE offers private parties the possibility to submit a Crime Report (CR) online, via a dedicated web form on the EPPO web site. While this form is considered as the primary channel by which private parties should report crimes to the EPPO, the possibility to accept traditional mail is not excluded. The on-line submissions, converted into PDF files, are stored on an SMTP server until the moment an assessment is performed.

6. The Crime Report is assessed by EPPO's authorised staff in order to determine whether it contains sufficient information to justify the opening of a registration case in the CMS. If affirmative, the EPPO staff will proceed with the registration of a CMS case in accordance with the provisions of Article 38 of the IRP and Article 24 of the Regulation. If, on the contrary, it is determined that the reported crime falls

[1] *According to the Regulation 1182/71 of the Council of 3 June 1971 determining the rules applicable to periods, dates and time limits (OJ L 124 8.6.1971, p. 1).*

manifestly outside the competence of the EPPO, such pre-assessment needs to be confirmed by a competent European Delegated Prosecutor or European Prosecutor (EDP/EP), in line with Article 17(4) of the RPPD. In such a case, a dossier is created in LogReg application, including justification and proposed decision, and the competent EDP/EP is notified to take decision. If the EDP/EP confirms the pre-assessment, he adopts the appropriate decision on the CR (return to sender, transfer to competent national authority or another EU institution, body, office or agency) and the CR is deleted from PAE. If the EDP/EP disagrees with the assessment, s/he will open a case in the CMS and the operational personal data will be deleted from the LogReg in the PAE.

3. LEGAL AND TECHNICAL ASSESSMENT

3.1. Need for prior consultation pursuant to Article 72 of the Regulation

Article 72 of the Regulation subjects the processing that will form part of a new filing system to prior consultation by the EDPS where:

a) a data protection impact assessment as provided for in Article 71 indicates that the processing would result in a high risk in the absence of measures taken by the EPPO to mitigate the risk; or
b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

Generally, as indicated in the DPIA (page 5), the processing of operational data by the EPPO serves a law enforcement and judicial purpose. Such processing carries certain inherent risks to the data subjects. More specifically, the DPIA describes some high risks in the absence of any mitigation measures taken by the EPPO. Such high risks include for instance the unnecessary exposure to law enforcement attention and activities or disclosure of the personal data processed in the law enforcement context (which may lead to public embarrassment, intimidation, blackmail). This therefore triggers the obligation for the EPPO to consult the EDPS, in line with Article 72(1)(a) of the Regulation.

The EDPS recognizes that the PAE is a separate processing environment that merely serves the purpose of filtering out operational personal data manifestly outside of EPPO's competence. In this sense, not all the risks identified for the CMS are direct risks for the processing in PAE.

The EPPO also asks for confirmation, whether all processing of operational personal data for law enforcement purposes carries an inherent high risk to the data subject and, as such, is a type of processing that requires prior consultation in line with Article 72(1)(b) of the EPPO Regulation, regardless of any identified risks or their level. The EDPS considers such interpretation too extensive. Indeed, processing of operational personal data for law enforcement purposes carries inherent risks for the data subject. Some of these risks may also have a potential impact on other fundamental rights (such as freedom, non-

discrimination, right to a fair trail, presumption of innocence or the right to defence). However, such risks should not always be qualified as "high risk" in the meaning of Article 72(1)b of the Regulation. Assuming that any processing of operational personal data for law enforcement purposes involves always "high risks" for the data subject, would render the disposition of Article 72(1)b meaningless. It is the level of risk that plays a decisive role for the obligation to consult the EDPS prior to the processing.

3.2. Scope of the Opinion

The Opinion of the EDPS on this prior consultation only concerns the DPIA regarding PAE of information provided by private parties, as described in the notification of 9 April 2021 and annexed documentation.

This Opinion focuses on key aspects that raise issues of compliance with the applicable data protection legal framework or otherwise merit further analysis.

The EDPS does not provide at this time any specific comments on the documentation submitted together with the DPIA. The EDPS has already provided comments and recommendations on EPPO's CMS DPIA [EDPS case 2020-0568], EPPO's Internal Rules of procedure [EDPS case: 2020-0781], EPPO's Rules concerning the processing of personal data [EDPS case: 2020-0782] and EPPO's DPO implementing rules [EDPS case 2020-0804].

The EDPS expects to be consulted on any significant update of the DPIA as a result of a substantial modification of the personal data processing operations in the PAE or on any technological development affecting significantly the risks of the processing operations.

3.3. Legal basis for the processing

The purpose of the processing falls under **Article 49(4)** of the Regulation, which provides that the EPPO may temporarily process operational personal data for the purpose of determining whether such data are relevant to its tasks and for the purposes referred to in Article 49(1). Further, the provision stipulates that the conditions relating to the processing of such operational personal data should be specified by the College, acting on a proposal from the European Chief Prosecutor and after consulting the European Data Protection Supervisor.

Article 17 of the RPPD fulfils the disposition of Article 49(4) of the Regulation by further specifying the conditions for processing of operational personal data received from private parties.[2]

3.4. Necessity and proportionality of processing

As rightly observed by the EPPO, the need to temporarily process operational personal data "*for the purpose of determining whether such data are relevant to its tasks*" is expressly recognised in Article 49 of the Regulation. Temporary storage and initial assessment of the information received by the EPPO is necessary for the performance of its tasks as defined by Article 4 of the Regulation.

The need to further define the modalities for temporarily processing operational personal data was also confirmed by the EDPS in his opinion regarding EPPO's CMS. There, it was

[2] *For EDPS specific recommendations on the RPPD please see EDPS comments on the EPPO's draft revised rules on processing of personal data (Case 2020-0782).*

observed that there is no precise workflow for the personal data received and processed temporarily by the EPPO but not falling within its mandate. More specifically, unclear procedures for the return of the data to the provider, or on the transfer of the relevant data to the competent authorities and the specific conditions regarding these specific transfers, as well as the deletion of data were highlighted.[3] By the creation of PAE, the EPPO addresses some of the issues identified above.

The EPPO has designed a specific pre-assessment process and environment (PAE), tailored on information provided by private parties, in order to fulfil the obligation to process only data relevant to carrying out its tasks. This obligation, stipulated in Article 49(1) of the Regulation, is a permanent one and subject to supervision and judicial control. The creation of a separate environment (PAE) allows distinguishing between unverified data submitted by private parties and the operational personal data processed for investigation and prosecution purposes. At the same time, it prevents manifestly irrelevant data to be formally registered in the CMS. By this, it aims at ensuring that personal data processed by the EPPO is "*adequate, relevant and not excessive in relation to the purposes for which they are processed ('data minimisation')*".

By strengthening the adherence to the data minimisation principle, the PAE also helps to ensure the efficient use of EPPO's resources. Given EPPO's specific and rather narrow competence, data submitted by private parties is expected to be often inaccurate or irrelevant for the tasks of the body. Early identification of manifestly irrelevant data eliminates the burden of its further processing and protection.

It could be argued that the Regulation does not explicitly oblige the EPPO to create a separate pre-assessment environment. While it might be true, the EDPS observes that all the processing operations in PAE serve the purposes expressly enshrined in the regulation and the pre-assessment does not lead to additional processing of personal data (as such an assessment would be necessary anyway). Therefore, given the above described advantages of a dedicated environment, such solution appears to be proportionate.

3.5. DPIA assessment and recommendations

The EPPO identified a number of risks to data subjects, with some of them considered as high overall risk with high impact on data subject rights in the absence of any mitigating measures. The highest risks indicated in the table relate to the gaining of unauthorised access to personal data with malicious intentions. According to the DPIA, the mitigation measures addressing the risks identified consist of technical (the design specifications of the PAE) and legal measures (safeguards laid down in implementing rules referenced throughout the DPIA). The EPPO concludes that some residual risks remain, but "for them to materialise, a multiple number of factors play into this part, and a number of mitigating measures must have failed or been wilfully ignored."

The EDPS also notes that some of his general recommendations, issued on the occasion of previous prior consultation on the CMS[4], were taken into account and, where applicable, appropriately implemented in the PAE DPIA. This is demonstrated, inter alia, in a clear review calendar and policy, delineation of the events and risks as well as in improved description of the measures. Nevertheless, EDPS would like to make (or repeat) a number of

[3] *See the Opinion of 1 October 2020 on the European Public Prosecutor's Office's prior consultation on the risks identified in the Data Protection Impact Assessment carried out on its Case Management System [EDPS 2020-0568], in particular recommendation no. 14 .*

[4] *See footnote 3.*

specific comments and recommendations, concerning mainly description of processing and the risk assessment itself.

3.5.1. Description of processing (point 7 of the DPIA)

The description of the processing is well structured and allows for good understanding of the processing environment and operations. However, it seems that the DPIA would benefit from a more detailed description of certain aspects. This concerns primarily the provision of operational personal data to the EPPO by the private parties. The scope of the DPIA remains, understandably, focused on the on-line form, which is the encouraged form of submission (page 6). However, other forms of submission of operational personal data to EPPO (like traditional mail) are not excluded. It is also possible, that such operational personal data is submitted to the EPPO by private parties via publicly available e-mail addresses. While it might be estimated that such instance will not occur very often, in such cases a number of mitigation measures provided by the form might not be applicable. It is unclear, what will happen if the operational personal data is submitted by a private party outside of the web form - will it be processed outside of the pre-assessment environment or will it become part of PAE processing? Will the sender be asked to resubmit such information via the form or will it be introduced via the form by the EPPO staff? What will happen to the data afterwards?

Recommendation 1: consider the scope and completeness of the DPIA and examine, whether a specific procedure is needed for handling operational personal data submitted by private parties electronically outside of the web form or via the mail (physical files). If the processing of such information would take place within PAE, supplement the description and risk assessment (e.g. risks 9, 10, 12) accordingly.

3.5.2. RISKS ASSESMENT

- **Risk 1** - refers to processing personal data without any legal basis in a manner incompatible to the legitimate purposes; the PAE is supposed to mitigate this risk and the provided documentation includes the steps and roles of the main actors; however, the specific criteria for the assessment are not detailed.
-

Recommendation 2: Make sure that clear criteria for the pre-assessment are available to the authorized staff; this could also be part of the specific trainings or manuals to be provided.

- **Risk 10** - the description of risk in the "Risk" column refers to "data stored in the CMS"; the EDPS believes the risk in this case concerns data stored in the PAE.

Recommendation 3: amend the risk description to refer to the actual processing environment (PAE).

- **Risk 17** - refers to the event of special categories of operational personal data being processed without additional safeguards.[5] The mitigation column indicates that PAE does not allow to automatically flag special categories of data. While certain limitations may be inherent to the process (no control over the submitted data and limited purpose and time of processing in the PAE), the only tangible mitigation measure identified is the notification of the DPO. Provided that the DPO is informed about the processing of special categories of data, the EDPS assumes that such data is identified at the pre-assessment in PAE. The "Mitigation" column refers to a special mention regarding special categories of operational data. However, such mention cannot be found in the Annex IV to the DPIA (description of web form fields).

Recommendation 4: Reconsider the modalities and description of processing of special categories of personal data in the PAE; in particular assess, whether such data could/should be flagged (manually) already in the PAE; ensure that the contents of the "Mitigation" column correspond with the information in the web-form regarding special categories of data; ensure data protection awareness trainings for EPPO staff tasked with the pre-assessment of CRs and any relevant documentation of the process (detailed procedure, manuals etc) explicitly remind EPPO staff of the obligation to notify the DPO

- **Risk 19** - refers to the event where "the EPPO does not respond accurately and timely to data subjects' requests." However, the identified risk and the mitigation measures described only refer to the accuracy aspect. The "Mitigation" column does not list the mitigation measures regarding the time of the reply.

Recommendation 5: Supplement the description of the mitigating measures in risk 19 by adding the measures taken to ensure also timely reply from the DPO.

- **Risk 22** refers to the fact that the EDPS '**is unable to gain access to the personal data or processing logs it requested**'. The risk description is the following: 'The ability of the EDPS to supervise is compromised if the access it is entitled to is not able to be provided' and the 'Underlying Data Protection Principle' is 'Supervision by EDPS'.
  While the focus of the risk identified in the DPIA is on EDPS supervision, the risk to the data subject is not appropriately described. For example, one of the risks to data subjects is the fact that they might not be able to exercise their rights through EDPS as provided for in Article 62 of the Regulation.

Recommendation 6: Adapt the risk description to reflect the risk to the data subjects as well as the content of the column 'Underlying Data Protection Principle'.

- **Risk 23** - similarly as in Risk 22, the description of the risk focuses on the risk to the supervision (in this case the DPO); again, the actual risk to the data subject is not

[5] *As required by Article 55 of the Regulation*

appropriately described. For example, one of the risks to data subjects is the fact that they might not be able to benefit from the independent monitoring of compliance with the data protection legal framework carried out by the DPO as in detail provided in Article 79 of the Regulation.

Recommendation 7: Adapt the risk description to reflect the risk to the data subjects as well as the content of the column 'Underlying Data Protection Principle'.

Brussels, 25 May 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI