Opinion 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

1. PROCEEDINGS

On 24 July 2020, 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 2017[1] ('the Regulation') regarding the Data Protection Impact Assessment (DPIA) on the Case Management System, 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:

[REDACTED]

The EDPS welcomes the fact that, as mentioned in the conclusion of the DPIA, the EPPO has taken into account data protection requirements during the CMS implementation and the design phase ([REDACTED]).

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 24 July 2020. Taking into account the complexity of the intended processing, the EDPS informed the EPPO on 18 August 2020 that the deadline would be extended by a month. The EDPS shall thus render his Opinion by **5 October 2020**.

2. DESCRIPTION OF THE PROCESSING

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.

[1] OJ L 283, 31.10.2017, p. 1–71

[2] According to Article 71(2) of the Regulation 'The assessment referred to in paragraph 1 shall contain at least a **general description of the envisaged processing operations**, an **assessment of the risks** to the rights and freedoms of data subjects, the **measures envisaged** to address those risks, **safeguards**, **security measures** and **mechanisms** to ensure the protection of operational personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of the data subjects and other persons concerned.'

As an EU body, which carries out activities which fall 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.

The EPPO's CMS is established in accordance with Article 44 of the Regulation, which provides that it will be managed in accordance with the provisions included in the Regulation and the EPPO's internal rules of procedure. In accordance with Article 44(4) of the Regulation, the CMS shall contain: a register of information obtained by the EPPO in accordance with Article 24; an index of all case files; and all information from the case files stored electronically. The EPPO intends to have its CMS operational in the next months.

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.

As indicated in the DPIA[3], the processing of operational data in the CMS serves a law enforcement and judicial purpose, which is by definition a processing operation that has an inherent high risk to the data subjects. In addition, the DPIA shows high risks in the absence of any measures taken by the EPPO to mitigate the risks identified. This therefore triggers the obligation for the EPPO to consult the EDPS, in line with Article 72(1)(a) of the Regulation. In addition, there is also a need for prior consultation under 71(1)(b) considering that this type of processing, which uses new mechanisms and procedures, involves *per se* a high risk to the rights and freedoms of data subjects because of the nature of data processed and their potential impact on data subjects' right to data protection and other fundamental rights such as non-discrimination, the right to an effective remedy and to a fair trial, the presumption of innocence and the right of defence.

3.2. Scope of the Opinion

The Opinion of the EDPS on this prior consultation **only concerns the DPIA as described in the notification** of 24 July 2020 (V4.0) and appended documentation.

[3] page 5.

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

The EDPS will 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 Internal Rules of procedure [EDPS case: 2020-0781] and EPPO's Rules concerning the processing of personal data [EDPS case: 2020-0782][4]. The EDPS welcomes any subsequent request for consultation from the EPPO.

The EDPS notes that the DPIA does not contain provisions as regards access to information available in EPPO's CMS on the basis of a hit/no-hit system by Eurojust and OLAF (as provided for in Articles 100(3) and 101(5) respectively of the Regulation). Should EPPO implement such a feature in its CMS, the EDPS expects to be consulted on the basis of Article 72 of the Regulation.

The EDPS also 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 CMS.

3.3. Legal basis of the processing

The purpose of the processing falls under **Article 44** of the Regulation, which provides that the EPPO shall establish a case management system for the purposes of:

a) supporting the management of investigations and prosecutions conducted by the EPPO;
b) ensuring secure access to information on investigations and prosecutions at the Central Office and by the European Delegated Prosecutors;
c) allowing for the cross-referencing of information and the extraction of data for operational analysis and statistical purposes;
d) facilitating monitoring to ensure that the processing of operational personal data is lawful and complies with the relevant provisions of this Regulation.

3.4. Assessment of the DPIA

The EPPO identified a number of risks to data subjects. The mitigation measures addressing the risk identified include, according to the DPIA, technical (design specifications and structure of the CMS), organisational, or legal measures (implementing rules carrying legal value within the EPPO, such as Internal Rules of Procedure; Internal Rules on the Processing of Personal Data; Rules on the Protection of Sensitive Non-Classified Information).

[4] cF letter from the Supervisor to the European Chief Prosecutor of 17 September 2020 and enclosed sets of comments.

The EPPO concluded that the 'the measures in place, be they organisational, technical or legal in nature, reduce the residual and overall risks to a level which is acceptable and proportionate to the aim of the processing operations and for the EPPO [...]'[5].

First of all, the EDPS would like to underline the excellent quality of the DPIA with regards to the methodology used (including risk factors and matrix on likelihood and impact) as well as on substance (description of the situation and analysis, in particular the data subjects being the focus of any risk). The EDPS especially appreciates that the EPPO has focused its analysis on the risks to the data subjects.

The EDPS will consider hereinafter the **main data protection issues** concerning the processing of personal data at stake, having regard to the measures envisaged by the EPPO to address data protection risks. Furthermore, the impact on data subjects' **other fundamental rights** is also considered. The EDPS takes note that, when identifying and describing the risks, the EPPO has considered (although not specifically naming them) risks to other fundamental rights than data protection.

While acknowledging the overall quality of the DPIA, the EDPS has a number of specific comments and recommendations on the methodology (Section 3.4.1.) and on the risks identified by the EPPO (Section 3.4.2.).

3.4.1. DPIA methodology

a) 'Events' and 'Risks' are bundled together

The DPIA contains a column entitled '**Event / Risk**'. 'Events' and 'Risks' are however two different concepts: while an 'event' is an occurrence with its impact and likelihood, a 'risk' stems from an event and is a possible outcome (mostly negative) of an event. Thus, the terminology in the document should be adapted to ensure that events are not mixed with risks (column 2 of Table 7.2. of the DPIA should refer exclusively on 'events'). Furthermore, the content of the 4 ('Risk to data subject') of Table 7.2. of the DPIA should describe and focus solely on the risks associated to each event.

Recommendation 1: Adapt the DPIA to account for the conceptual difference between 'events' and 'risks'.

b) Mitigation measures are as a rule not sufficiently described

In most of the cases, the mitigation measures included in the DPIA remain at a relatively high level and thus do not specify in concrete terms how the identified risk will be addressed and which concrete mitigation measure will be applied specifically. This is partly due to the above-

[5] Page 5.

mentioned issue in relation to 'events' and 'risks, and to the fact that at times the analysis does not describe how a risk can materialise and thus, the mitigation measure cannot be sufficiently specific. In particular although specific rules included in the EPPO's internal rules (such as Internal Rules of Procedure or Internal Rules on Processing of Personal Data or Rules on the Data Protection Officer) might address the identified risks, it is often unclear which specific provision of the above-mentioned rules will be applicable in a particular case and how the risk will be mitigated in concrete terms.

For example, **risk no. 34** identified in the DPIA refers to the fact that '**Personal data Breaches are not duly notified and acted upon**'. Its mitigation measures contains 'Rules on Processing Personal Data, Internal Rules of Procedure, procedural involvement and consultation of DPO'.

Recommendation 2: Include in the mitigation section of each risk identified, where it has not been made already, the description of specific measures designed to address the particular risk (such as technical and organisational measures and, whenever this is implemented in CMS, the mitigation should describe the functionality) and the specific reference to the applicable internal rules.

Recommendation 3: In order to duly notify and, where applicable, communicate personal data breaches and to act accordingly so as to mitigate the risks to the data subjects, design and establish a **personal data breach policy** addressing and containing key features, such as roles and functions to be involved in case of a security incident or personal data breach, risk assessment, processes of notification to the EDPS and, where applicable, communication to data subjects, as well as appropriate mitigation measures.

c) **Column title - 'Underlying Data Protection Principle' - not reflecting its content**

The content of the column 'Underlying Data Protection Principle' of Table 7.2. does not refer only to data protection principles, which are *stricto sensu* the principles listed in Article 47 of the Regulation. This column also includes for example, references to exercise of data subject rights, communication of data breach, transfers, i.e. data protection rules in general.

Recommendation 4: Adapt the title of the above-mentioned column to reflect that it refers to data protection rules in general.

d) **Key aspects related to DPIA review missing**

[REDACTED]

Despite referring to the need to review the DPIA in certain circumstances, the DPIA lacks information as to the periodicity of its periodic review, the criteria triggering a non-periodic review, as well as the entities in charge of the review.

Recommendation 5: Include a **reference to the periodicity of the DPIA review** after CMS goes live. Taking into account the above-mentioned considerations, the EDPS recommends

that the DPIA be reviewed every year as well as every time a major development impacting the DPIA has taken place. The DPIA shall also clarify the **entity(ies) responsible** for initiating the review process and carrying out the update (i.e. the controller, the project owner) as well as the **criteria for non-periodic review** (i.e. in case a proposal for introducing significant changes to CMS functionality has been made; serious security incidents or changes in the security context).

3.4.2. Risks

a) Some risks identified in the DPIA need to be clarified

The EPPO should further clarify some of the risks identified in the DPIA.

- **Risk 10** refers to not properly **informing data subjects** about the processing of their data. The mitigation included in the DPIA refers to indicating in CMS as to whether information has been provided or, if that is not the case, why a restriction has been applied. However, the mitigation measures mentioned do not account for situations where 'the suspension or delay of informing the data subject' (as provided for in Article 4(5) of the EPPO Internal Rules on data protection) is no longer valid and where the data subject would still not have been informed.

Recommendation 6: Analyse and clarify further situations where the **deferment of information** to data subjects is no longer valid and as a result design and implement appropriate mitigation measures to avoid that data subject would not be duly informed in those situations.

- **Risk 12** refers to informing data subjects about a '**security breach'**.

  Article 75(1) of the Regulation provides that: 'Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the EPPO shall communicate the personal data breach to the data subject without undue delay.' Article 8 of the EPPO Internal Rules on data protection further stipulate the conditions referring to informing data subjects on a personal data breach affecting their personal data. For the sake of clarity, the EPPO should also align the terminology, i.e. the description of the event should refer to a 'personal data breach' instead of a 'security breach".

Recommendation 7: Clarify that:

- the event refers to a 'personal data breach';

- the risk refers to informing data subjects about a **personal data breach** affecting their personal data where the personal data breach is likely to result in a high risk to the rights and freedoms of concerned natural persons.

- **Risk 22** ('**Personal data is inserted into the CMS without context / distinctions between e.g. data subjects role**') contains the following description of the risk to data subject 'Data

subjects who are listed as e.g. suspects, rather than witnesses, or witnesses who are not identified as such, but be subjected to more invasive processing'.

While the risk definition refers to situations where personal data is inserted without distinction between data subjects role, the risk description refers to the possibility of misidentifying data subjects. Furthermore, mitigation does not address the issue as mentioned in the risk definition but only situations where data/metadata is missing, while an important risk refers to situations where data subjects' identification is incorrect.

Recommendation 8: Clarify the risk(s) as regards personal data insertion into the CMS. In the EDPS' view, both a lack of metadata and a misidentification of data subjects are possible and should be addressed properly as separate risks to data subjects with appropriate mitigation measures for each of them.

- **Risk 24** ('**Personal data known to be inaccurate, incomplete, or unlawfully processed are transferred / provided to third parties**') contains the following description of the risk to data subject 'Where a data subject's data has been improperly processed, it is not the responsibility of the data subject to address themselves to other recipients, but that of the EPPO'.

  The risk description does not correspond to the event identified. For example, a risk to data subjects is the fact that they might be subject to investigations and/or misjudgements by the recipient of the data should the data transferred be inaccurate.

Recommendation 9: Clarify the risk description so that the risk to the data subjects is properly identified, described and addressed.

- **Risk 25** 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 10: 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 28** refers to the fact that '**EPPO DPO [is] unable to access personal data needed to exercise their function**'. The risk description is the following: 'The ability of the DPO 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'.

  While the focus of the risk identified is on supervision carried out by the DPO, 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 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 11: 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 29** refers to the fact that the '**Ability to grant targeted personal access is not present, so everyone can have access**'. The risk description is: 'The unnecessary disclosure of personal data increases residual risk compared to non-disclosure'.

Recommendation 12: Clarify the definition and the description of this risk identified, for example by referring to the fact that access levels are not accurately defined on the basis of need to know. Also, clarify the description of the risk by focusing on the risk to data subjects.

- **Risk 32** refers to the fact that '**Special categories of personal data are being processed without justification**'. Its description is: 'Specific restrictions apply to the processing of special categories of personal data. Where these are not identified as such, they may have less protection'.

  From the risk definition and description is it unclear whether the risk refers to unlawful processing of special categories of personal data (as mentioned in the definition) or to the fact that special categories of personal data 'are not identified as such' (as mentioned in the description).

Recommendation 13: Clarify the definition and the description of the above-mentioned risk, identifying and emphasising precisely the risks to the data subjects, which can include (but is not limited to) the fact that, if not correctly categorised as a special categories of personal data, data subjects might have less protection.

b) Some risks have been overlooked in the DPIA

The EDPS recommends that EPPO considers a number of additional risks. The EDPS has identified these extra risks based on the process description in the DPIA, the risks mentioned in the DPIA and the reference documentation submitted. Nevertheless, the EDPS does not consider that, by adding these risks to the DPIA, the risks analysis would be necessarily exhaustive. The EPPO is invited to consider, at this stage and later on, whether this personal data processing entitles other risks to the data subjects that should be included and addressed in a future review of the DPIA.

- **Additional risk 1: Non-compliance with the obligation to process only data relevant to EPPO's field of competence (Lawfulness)**

  Article 24(7) of the Regulation provides that, 'Where upon verification the EPPO decides that there are no grounds to initiate an investigation [...] or to exercise its right of evocation [...] the reasons shall be noted in the case management system.' Also, in paragraph 2 of the same legal provision, it is stated that 'The EPPO shall inform the authority that reported the criminal

conduct in accordance with paragraph 1 or 2, as well as crime victims and if so provided by national law, other persons who reported the criminal conduct.' Furthermore, Article 24(8) of the Regulation provides that, 'where it comes to the knowledge of the EPPO that a criminal offence outside of the scope of the competence of the EPPO may have been committed, it shall without undue delay inform the competent national authorities and forward all relevant evidence to them.'

In accordance with Article 49(4) of the Regulation, 'the EPPO may temporarily process operational personal data for the purpose of determining whether such data are relevant to its tasks and [...] purposes. The College [...] after consulting the European Data Protection Supervisor, shall further specify the conditions relating to the conditions relating to the processing of such operational data, in particular with respect to access to and the use of the data, as well as time limits for the storage and deletion of the data.'

Article 37(6) of the draft EPPO's Internal Rules of Procedure specifies that '[REDACTED]'

In section 5.*7.1. Insertion and registration of operational personal data, Figure 18 - Table for verification and registration overview* of the DPIA, it is stated that 'Information stored is assessed by appropriate EPPO Staff if it falls within mandate. If not, information is rejected and possibly provider informed, and / or data submitted to competent authority, EU body or other action.'

In relation to the verification process as to whether personal data received relates to the EPPO's tasks and purposes', the DPIA identifies the following risk: risk 1: 'Personal data is processed unlawfully without any legal basis for the processing' with the subsequent risk to data subject: 'Unlawfully processed personal data does not provide any protection or assurance to the data subject, and deprives him of his rights to protection of personal data'. Mitigation measures include: 'detailed process for insertion of personal data into CMS in Title III, IRPs (Art. 37ff)'.

From the description included in the DPIA and more specifically in *Figure 18* as well as the provisions included in Article 37(6) of the draft EPPO's Internal Rules of Procedure and in order to address properly the risks to the data subjects and avoid risks that might arise from procedural ambiguity, further clarifications with regards to personal data received by the EPPO but not falling within its competence are required.

Recommendation 14: Include as a risk the possibility that unclear procedures on how to process personal data received and processed temporarily by the EPPO but not falling within its mandate might create risks for data subjects (for example, there is no precise workflow for such data and more specifically, unclear procedure 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).

- **Additional risk 2: Non-compliance with the obligation to respond accurately to data subjects' requests**

  Article 59 of the Regulation provides that data subjects have the right to obtain from the EPPO 'confirmation as to whether or not operational personal data concerning him/her are being processed, and, where that is the case, access to the operational personal data' and certain specific information.

  In section 5.*7.1. Insertion and registration of operational personal data, Figure 18 - Table for verification and registration overview* of the DPIA, it is stated that '[REDACTED]. Similarly,

in section *6 Necessity and Proportionality*, it is stated '[...] data that is stored in the CMS, but not yet registered / verified, is not accessible for any user conducting a search.'

We take note of the fact that this procedural step is designed to ensure verification that the EPPO only processes data relevant to the fulfilment of its tasks, in line with the provisions of Article 49(4) of the Regulation. We also take note of Title III – Operational Matters/Chapter 1 – Registration and Verification of Information of the draft Internal Rules of Procedure, further specifying the applicable provisions to this temporary processing of personal data[6].

In any case, even though temporary, this represents a processing of personal data and as a result, data protection provisions are fully applicable. For example, in case a data subject inquires whether or not operational personal data concerning him/her are being processed and/requests access to his/her personal data, the EPPO should be able to accurately conclude whether it processes any personal data of the applicant.

Recommendation 15: Include as a risk the possibility of non-compliance with the obligation to respond accurately to data subjects' requests. The EDPS **recommends** that the EPPO make a distinction between registered personal data (pending verification) and non-registered personal data, and considers risks related to each of the two instances. Furthermore, EPPO should consider distinguishing between registration and verification as these two steps might raise different risks.

- **Additional risk 3: Non-compliance with the storage limitation principle**

In accordance with the principle of 'storage limitation' (Article 47(1)(e)), 'personal data shall be [...] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'.

From the DPIA and the enclosed documentation it is unclear for how long personal data '[...] that is stored in the CMS, but not yet registered / verified' will be retained before it is assessed by appropriate EPPO staff if it falls within mandate and a decision is taken in this regard. Article 49(4) of the Regulation specifies indeed 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 [...].' Moreover, it also provides that, following a specific procedure that include consultation of the EDPS, the EPPO College 'shall further specify the conditions relating to the processing of such operational personal data, in particular with respect to access to and the use of the data, as well as **time limits for the storage and deletion**[7] of the data.'

Recommendation 16: Include as a risk the possibility that data stored temporarily in CMS for the purpose of being registered / verified as to whether or not it falls within the EPPO's competence is stored in breach of the storage limitation principle. As a mitigation measure EDPS recommends defining specific retention periods applicable to data before being registered, as well as to data that has been registered but not yet verified.

[6] cF letter from the Supervisor to the European Chief Prosecutor of 17 September 2020 and enclosed sets of comments [2020-0781 and 2020-0782].
[7] underlined by us.

- **Additional risk 4: Inaccurate data might determine flawed decisions concerning the data subject under investigation**

  In **risk 3** (**'Inaccurate data may be processed**'), the DPIA makes the following description of the risk to the data subject: 'If the personal data is inaccurate, it may lead to a different data subject becoming the focus of law enforcement attention and potential investigative measure against them'.

Recommendation 17: Address another risk that might arise due to processing of inaccurate data, namely the fact that flawed decisions concerning the data subject under investigation might be taken.

- **Additional risk 5: Unlawful transfers**

  The risk of EPPO **transferring** operational personal data to a non-EU Member State or an international organisation unlawfully, i.e. in the absence of adequacy or appropriate safeguards or derogations in specific situation is not included and addressed in the DPIA.

Recommendation 18: Include and address the risk of transferring operational personal data to a third country or an international organisation unlawfully.

- **Additional risk(s) 6: (Joint) controllership**

  The DPIA does not cover risks arising from unclear understanding and definition of roles related to controllership and/or joint controllership between the EPPO and the participating Member States. Indeed, the possibility of laws overlapping (at EU and national level) is mentioned in the DPIA, 'as national laws continue to apply and govern the investigations and the prosecutions'.

Recommendation 19: Include risks arising from unclear understanding and definition of **controllership and/or joint controllership** roles between the EPPO and the participating Member States.

- **Additional risk(s) 7: Use of processors/sub-processors**

  The DPIA does not cover risks arising from the use of processors and, if applicable, sub-processors by the EPPO. The use of processor and sub-processors increase the risk of personal data processing and as a result, they should be considered in the DPIA.

Recommendation 20: Include risks related to the use by EPPO of processors and, if applicable, sub-processors.

- **Additional risk(s) 8: Access rights**

  Risk 29 identified by in the DPIA refers to the fact that the '**Ability to grant targeted personal access is not present, so everyone can have access**'. A number of additional risks related to CMS access rights should be addressed such as: access has been granted by error to individuals

who should not have that kind of credentials; access is not removed when someone is not involved a particular case anymore; no periodical check of assignment of roles is performed.

Recommendation 21: Addresses in the DPIA the above-mentioned risks related to CMS access rights.

c) Risks' impact seems in certain cases underrated

The EDPS recommends that EPPO reconsider the evaluation of the impact of the following risks included in the DPIA.

- **Risk impact to be reconsidered 1:**

In **risk 3** (**'Inaccurate data may be processed**'), the DPIA makes the following description of the risk to the data subject: 'If the personal data is inaccurate, it may lead to a different data subject becoming the focus of law enforcement attention and potential investigative measure against them'. The impact identified in the DPIA is 3.

Recommendation 22: Re-evaluate the impact of this risk (and the additional one proposed by the EDPS in relation to processing inaccurate data) and consider whether the impact of taking decisions on inaccurate data might not be higher for the data subjects. Should EPPO consider that the impact is indeed 3, the EDPS expects a justification in this sense.

- **Risk impact to be reconsidered 2:**

In **risk 4** ('**Personal data may continue to be processed beyond the time limits foreseen or where no longer necessary**'), the DPIA makes the following description of the risk to the data subject: '[...] As the lack of necessity in any event indicates though the lack of any focus on the data, no concrete additional data emanates from such a continued processing'. The impact identified in the DPIA is 1.

The EDPS considers that, by not implementing the appropriate retention period, the impact on concerned data subjects, might be higher. Furthermore, defining and implementing appropriate retention periods and mechanisms in the CMS for flagging and deletion of data when no longer necessary is essential.

Recommendation 23: Re-evaluate the impact of the risk related to excessive retention and consider whether its impact to the data subjects might not higher. Should the EPPO consider that the impact is indeed 1, the EDPS expects a justification in this sense.

d) Residual likelihood of materialisation after mitigation is underrated (risk 14 - Uncertainty around the applicable legal framework)

According to the DPIA, after mitigation, the residual likelihood of the **risk 14 ('Uncertainty about applicable legal framework to the processing of their personal data')** is 1 (initial

likelihood before mitigation is 4). Considering the complexity of the applicable legal framework (EU-level legal framework and national laws applicable - laws implementing LED in addition to applicable national procedural laws as well the possibility of having multiple national laws applicable, such as criminal procedural laws), the EDPS wonders whether the residual risk is not underestimated.

Recommendation 24: Re-evaluate whether the residual likelihood of materialisation can indeed be reduced to 1 after mitigation measures are applied, in the context of uncertainty about the applicable legal framework.

e) Risk mitigation does not decrease the residual likelihood of materialisation (risk 25 - inability for the EDPS to access to the personal data/logs)

According to the DPIA, after mitigation, the residual likelihood of materialisation of the **risk 25** (EDPS '**is unable to gain access to the personal data or processing logs it requested**') remains to the same value, namely 2.

Recommendation 25: Re-evaluate the mitigation measures so that the residual likelihood of the risk materialising after mitigation is reduced.

3.5. Information security risk assessment

[REDACTED]

Recommendation 26: [REDACTED]

***

4. RECOMMENDATIONS

Firstly, the EPDS would like to underline the overall quality of the DPIA. While acknowledging this positive aspect, in this Opinion, the EDPS has made several recommendations to ensure compliance with the Regulation. The EDPS expects **implementation of the above-mentioned recommendations (summarised further down) and documentary evidence** of this implementation to be provided within **three months** of the date of this Opinion.

1. Ensure that the DPIA is adapted to account for the conceptual difference between '**events**' and '**risks**' (recommendation 1).

2. Ensure that the **mitigation** section of each risk identified includes the description of specific measures designed to address the particular risk identified (recommendations 2 and 3).
3. Adapt the tile of the column '**Underlying Data Protection Principle**' so that it refers to data protection rules in general (recommendation 4).
4. Ensure that the DPIA includes a reference to the periodicity of the DPIA **review** after CMS goes live, as well as to the **entities** responsible for initiating the review process and carry out the update and the **criteria for irregular review** (recommendation 5).
5. Clarify the **risks** as mentioned in section e) of the Opinion (recommendations 6-13).
6. Consider the **additional risks** mentioned in section f) of the Opinion (recommendations 14-22).
7. Re-evaluate the **impact** of certain risks mentioned in section g) of the Opinion (recommendations 23 and 24). For these recommendations, the EDPS expects to receive either a justification of the current impact identified in the DPIA or documentary evidence of implementation.
8. Re-evaluate whether in the case of risk 14 the **residual likelihood** of materialisation can indeed be reduced to 1 after mitigation measures are applied (recommendation 25).
9. Re-evaluate the mitigation measures of risk 25 so that the **residual likelihood** of materialisation after mitigation is reduced (recommendation 26).
10. Carry out an **information security risk assessment** and employ existing technical solutions incorporated in the CMS and their **security** features (recommendation 27).

Done at Brussels, 1 October 2020

Wojciech Rafał WIEWIÓROWSKI