EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
SUPERVISOR

Mr [redacted]
Chairperson
Europol Management Board
Europol Management Board
Secretariat
Eisenhowerlaan 73
NL - 2517 KK The Hague

Brussels, 01 March 2021

WRW/PDL/KV/vm/ D(2021) 0432 **C 2020-1032**
Please use edps@edps.europa.eu
for all correspondence

Subject: **Opinion on a prior consultation by Europol regarding Europol's access to Visa Information System (VIS) data**

Dear [redacted],

The European Data Protection Supervisor ('EDPS'), having regard to Article 39 of Regulation (EU) 2016/794[1] ('the Europol Regulation', or 'ER' abbreviated)

Has issued the following opinion:

1. PROCEEDINGS

On **9 November 2020**, the EDPS received a request for prior consultation from Europol regarding Europol's access to VIS data.

The request for prior consultation was filed under EDPS case number 2020-1032 and, in accordance with Article 39(4) ER, it has been included in the register of processing operations notified by Europol to the EDPS.

Attached to the notification for prior consultation[2] were the following supporting documents:
- VIS integration in USE UI - high level overview of technical components,[3]

[1] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24 May 2016, p. 53-114.
[2] "Notification to the EDPS regarding new type of processing operation", EDOC#1130622 and EDOC#1130599.
[3] EDOC#1125355v1.

- Cross-check data and manage hits - process description.[4]

On **24 November 2020** the EDPS sent an additional list of questions to Europol for confirmation, further information and clarifications.

On **14 December 2020**, Europol provided its response to the EDPS' questions via the Data Protection Function ('DPF').[5]

On **22 December 2020 and 9 February 2021**, the EDPS requested further information, which was received via the DPF on **18 January and 16 February 2021.**[6]

Taking into account that, in accordance with Article 39(3) of the Europol Regulation, the EDPS shall deliver his Opinion to the Management Board within two months following receipt of the notification and that this period may be suspended until the EDPS has obtained any further information that may have been requested[7]; the deadline within which the EDPS shall issue his Opinion in this case is **1st March 2021**.

2. DESCRIPTION OF PROCESSING

2.1 The VIS legislative framework applying to Europol (Legal prerequisites)

The Visa Information System ('VIS') is an EU large scale information system containing personal data relating to applications for short-stay visas to visit, or to transit through, the Schengen Area.

The system was established by Council Decision 2004/512/EC [8], as completed by Regulation (EC) 767/2008 [9] ('VIS Regulation') for the purposes of improving the administration of the common visa policy by facilitating the exchange of data between Member States ('MS').

Article 3 of the VIS Regulation sets the grounds for the access by Europol and designated national authorities to data stored in the VIS ('VIS data') for law enforcement purposes. Council Decision 2008/633/JHA[10] ('VIS Decision') specifies and regulates such access.

Under Article 3(1) of the VIS Regulation, Europol may only access the VIS within the limits of its mandate and when necessary for the performance of ifs tasks.

Article 7(1) of the VIS Decision further determines the purposes for which Europol may access VIS data, i.e., a specific analysis or an analysis of a general nature and a strategic type. This corresponds to Article 18(2) (b) and (c) of the current Europol Regulation, namely analyses for

[4] EDOC#1085002v5.
[5] EDOC#1140710v2.
[6] EDOC#1146504v2 and EDOC#1153827v2.
[7] In the present case, the deadline was suspended for 54 days: from 24 November 2020 until 14 December 2020, from 22 December 2020 to 18 January 2021 and from 9 February 2021 to 16 February 2021.
[8] Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS), OJ, 15.06.2004, L213 p.5.
[9] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stays visas, OJ, 13.08.2008, L218, p.60.

either strategic/thematic purposes or specific operational analyses within an analysis project ('AP').
Article 7 (1) of the VIS Decision should also be read in light of Recital 8 of the same Decision, which gives more indications about the conditions for law enforcement authorities - including Europol - to access VIS data. This recital provides that: "For the purposes of protection of personal data, and in particular to exclude routine access, the processing of VIS data should only be on a case-by-case basis. Such a specific case exists in particular when the access for consultation is connected to a specific event or to a danger associated with serious crime, or to (a) specific person(s) in respect of whom there are serious grounds for believing that the person(s) will commit or has (have) committed terrorist offences or other serious criminal offences or that the person(s) has (have) a relevant connection with such (a) person(s). The designated authorities and Europol should thus only search data contained in the VIS when they have reasonable grounds to believe that such a search will provide information that will substantially assist them in preventing, detecting or investigating serious crime".

If Europol intends to process these data for purposes of analysis of a general nature and of a strategic type ("strategic analysis"), Article 7(1)(b) of the VIS Decision further requires that Europol renders VIS data anonymous prior to their processing and retains them in a form in which identification of the data subjects is no longer possible.

Pursuant to Article 3(2) of the VIS Regulation, the VIS consultation must be carried out through Central Access Point(s) ('CAP') which shall be responsible for ensuring strict compliance with the conditions for access and the procedures established in the VIS Decision. In an exceptional case of urgency, the central access point may receive written, electronic or oral requests and only verify *ex-post* whether all the conditions for access are fulfilled, including whether an exceptional case of urgency existed. The *ex-post* verification shall take place without undue delay after the processing of the request.[11]

Article 7 (3) of the VIS Decision specifies that Europol must designate a specialized unit with duly empowered Europol officials to act as the central access point to access the VIS for consultation.

Under the VIS legislative framework, Europol may transfer VIS data to third countries or international organisations only in an exceptional case of urgency, subject to the prior consent of the Member States and exclusively for law enforcement purposes.[12]

Before being authorized to process data stored in the VIS, the staff of the authorities having a right to access the VIS must receive appropriate training about data security and data protection rules and must be informed of any relevant criminal offences and penalties.[13]

2.2. Description of envisaged processing of VIS data by Europol

According to Europol's request for prior consultation and subsequent answers to EDPS questions, Europol is planning to consult VIS for the purpose of operational analyses (Article 18(2)(c) ER) and analyses of strategic or thematic nature (Article 18(2)(b) ER)[14].
According to the information provided by Europol, the envisaged processing is applied in three possible contexts:

[11] Article 3 (2) of the VIS Regulation and Article 4(2) of the VIS Decision.
[12] Article 3 (3) of the VIS Regulation and Article 8 (4) of the VIS Decision. [13] Article 8(8) of the VIS Decision.
[13] Article 8(8) of the VIS Decision.

a) When taking in operational data provided by a non-Schengen country or an international organization (for the purpose of operational analysis):

O1-1 Operational Centre staff will be able to consult VIS at the end of the intake process, after any other search in Europol systems or Schengen Information System ('SIS II') and regardless of their results, in case they have reasonable grounds to consider such a consultation would contribute to the analysis project.

b) When taking in operational data provided by a non-Schengen country or an international organization (for the purpose of strategic or thematic nature):

When, at the end of the intake process, personal data would not fit within one of Europol's APs O1-1 Europol staff may decide to consult the VIS, follow-up with the MS and eventually store the relevant VIS personal data in Europol analysis System ('EAS') for thematic and strategic analysis, to complete its overall picture of a certain crime area.

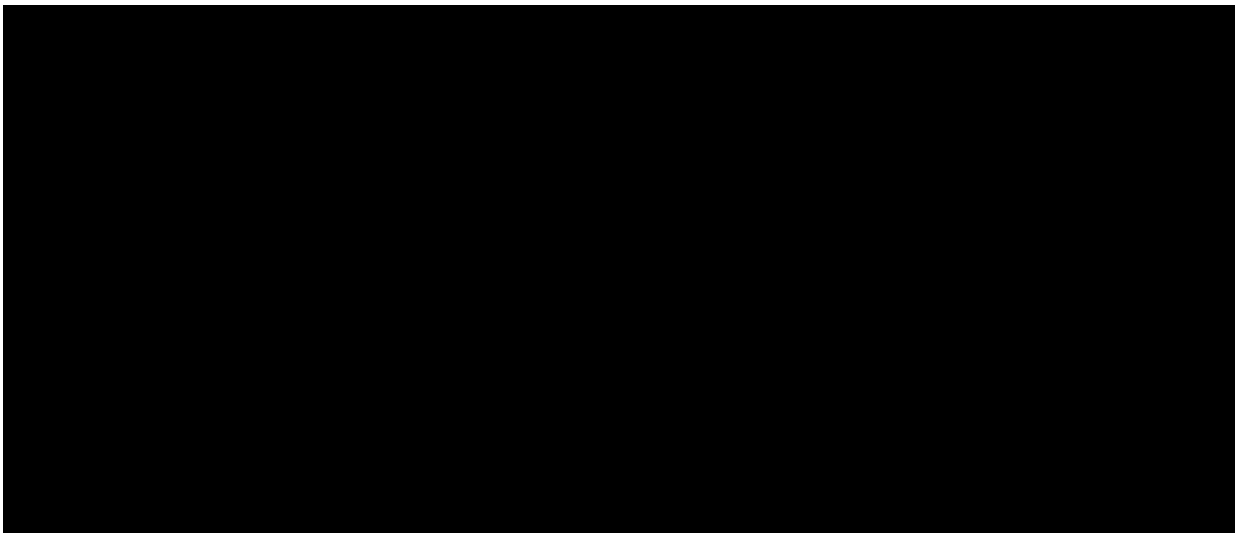
Based on these data, a strategic/thematic report is drafted in which no personal information will be included.

c) On an on-going basis throughout the operational analysis process (for the purpose of operational analysis):

The operational analyst assigned a specific analysis case in EAS will be able to consult VIS, to enhance the operational intelligence picture in this specific case.

In all the above scenarios, the following cumulative criteria will trigger Europol staff to search in VIS:

- The personal data refer to a data subject that is national of a country whose citizens are required VISA to enter the EU (or nationality is unknown or the person is declared as stateless);
- The Europol staff concludes there are factual indications or reasonable grounds to believe that this person might have travelled or might want to travel to the EU;
- The Europol staff concludes that access to VIS is required to prevent, detect, investigate or prosecute a terrorist offence or other serious criminal offence.



When the Europol Officer (user) performs a search in VIS, the first retrieved results consist of a list of potential matches (First Name, Family name, Date of Birth). The user can browse this list and assess which of these entries may correspond to the data subject they are searching for, based on the similarity of the returned data.

Only when the users decide that a data subject corresponds to their search they retrieve the remaining information from VIS about this person.
Once the user retrieves the remaining information from VIS about a data subject, they assess whether this information is valuable to prevent, detect, investigate or prosecute a terrorist offence or other serious criminal offence. Europol then proceeds to ask the owner of the information in VIS (MS) for permission to store information in EAS and process according to article 18(2) b) and/or c) ER. Permission is requested via a SIENA message, in which the analyst provides background information to the MS on the investigation of the case. Only when the Europol's user receives permission from the MS, he or she may proceed with storing the information in EAS, along with the respective SIENA message identifier.

3. LEGAL AND TECHNICAL ASSESSMENT

3.1. Need for prior consultation pursuant to Article 39 of the Europol Regulation

Article 39 of the Europol Regulation subjects some processing operations to prior consultation by the EDPS.

According to Article 39(1) of the Europol Regulation, the **scope** of application of the prior consultation requirement covers:
(a) processing of special categories of personal data as referred to in Article 30(2)[17]; or
(b) types of processing, in particular using new technologies, mechanisms or procedures, presenting specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.

Furthermore, according to Recital 50 of the Europol Regulation: '*the prior consultation mechanism is an important safeguard for new types of processing operations. This should not apply to specific individual operational activities, such as operational analysis projects, but to the use of new IT systems for the processing of personal data and any substantial changes thereto*.'

The VIS is an EU centralised database that contains information about millions of individuals. In 2019, 32,951,987 visa applications were registered in the VIS.[18] The database contains information about visa applicants but also on persons issuing an invitation and/or liable to pay the applicants subsistence costs during their stay in the EU. As such, the VIS does not contain special categories of data as referred to in Article 30 (2) of the Europol Regulation (i.e. on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health data or data related to sex life).

Accessing VIS data by Europol will be a new functionality [redacted] to enhance Europol's operational analysis capabilities by increasing accessibility to data managed by external systems. Europol mentioned that this new type of processing might entail risks for concerned data subjects, non-criminals visa applicants whose data may be accessed by Europol staff. Europol identified the following risks:
- unauthorised access to VIS data with a loss of confidentiality of personal data,
- disclosure of information the relevance of which for the prevention and combating of serious crime and terrorism may not always be evident ,

[17] Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, concerning a person's sex life or health, plus genetic data.
[18] EU LISA Report on the technical functioning of the Visa Information System (VIS), August 2020 available at: https://www.eulisa.europa.eu/Publications/Reports/2019%20VIS%20Report.pdf

- unneeded access to non-criminals data,
- wrongful identification of a person and inclusion of this person in an operational report sent to a Europol member state,
- unnecessary storage of data.[19]

The EDPS notes that the new functionality entails a significant change in Europol's processes for operational and thematic/strategic analysis as a new source of information will be consulted. Furthermore, this new source (VIS) is a database that has been set up and developed to facilitate the exchange of data between Schengen States on visa applications in order to ease procedures, prevent "visa shopping" and assist in the fight against fraud. It has not been developed as a law enforcement tool with the related specific features of such tool (e.g. distinction between the categories of data subjects, reliability of the source, etc.).

The EDPS stresses that because of the access by Europol to data stored in the VIS, a large amount of individuals who are not suspected to be linked to any crime run the risk of being incorrectly included in Europol's databases, which may give rise to discrimination, damage to reputation or financial loss

In light of the above, the EDPS considers that the conditions set in Article 39 (1) (b) of the Europol Regulation are met and that Europol access to the personal data stored in the VIS is subject to prior consultation in accordance with the Europol Regulation.

3.2 Format of process description provided as part of the prior consultation request

The establishment of the context and description of the processing operations is the foundation for the rest of the prior consultation process. As outlined in the EDPS accountability on the ground toolkit[20], a systematic description of the process should include the following four elements:

- data flow diagrams of the processes,
- the purpose(s) of the (different parts of the) processes,
- a description of their interactions with other processes and
- a description of the supporting infrastructure.

In the context of the current prior consultation, the EPDS received from Europol the process description for VIS consultation[21] and an overview of the technical components involved in the process of search to VIS[22]. Also, the description of the process steps contains information on the main involved systems (e.g. cross check data [redacted] against VIS in order to see if there is related information in the VIS, Ask data owner in VIS for permission to use the information by providing them via SIENA with relevant contextual information for the decision making).

The EDPS welcomes that Europol provided a flowchart as part of the VIS consultation process, in which steps and relevant actors are described. This allows the EDPS to trace the flow of personal data (here VIS data) throughout Europol's processing of this data for the purpose of

[redacted]

[20] https://edps.europa.eu/data-protection/our-work/publications/guidelines/accountability-ground-provisional-guidance_en

[redacted]

operational analysis. The EDPS also welcomes that each technical components involved in each step of the process were clearly indicated.

The EDPS however notes a lack of detail in the process description (e.g. in this consultation the Central Access Point validation of the query legality was missing).

In addition, the EDPS notes that the strategic and thematic analysis processes do not appear either in the SIPOC table or in the flowchart[23] contrary to the operational analysis which appears both at the input and the output sides of the process. In response to the EDPS' questions, Europol stated that the provided process applies to both data sent for operational analysis as well as for thematic and strategic analysis.[24] Nevertheless, this lack of detail resulted in difficulty in establishing the flow of personal data (here VIS data) throughout Europol's processing of this data for the purpose of thematic or strategic analysis. This aspect is still not clear at the end of the prior consultation process.

Knowing which process applies to which step is crucial, as the extent of Europol's processing capability is dependent on (and limited by) the purpose that the processing is meant to serve, under the VIS Regulation (Regulation (EC) 767/2008 and VIS council Decision 2008/633/JHA). The EDPS asks Europol for future prior consultations **to provide a data flow diagram for each purpose of the processing**, to fully clarify the legal framework in which it operates. He also asks Europol **to include in the process all applicable control measures (e.g. similar to the Central Access Point controls in this consultation).**

As regards the interaction with other processes, the EDPS asks Europol for future prior consultations to **specifically describe the scenarios that would trigger the process under consultation and to indicate any processes interacting with the process at stake.**

3.3. Scope of the Opinion

The Opinion of the EDPS on this prior consultation concerns the implementation of the VIS Regulation and the VIS Decision as described in the notification of 9 November 2020 and subsequent answers provided on 14 December 2020, 18 January 2021 and 16 February 2021. The EDPS notes that this is the first phase of the implementation of Europol's access to VIS. Future implementation will include new functionalities to search and retrieve fingerprints and photos stored in the VIS.[25] Besides, the EDPS notes that the future developments and implementation of the VIS recast regulation including the establishment of the interoperability between VIS and other large scale EU systems may impact Europol's access to VIS data.[26]

In this context, the EDPS asks Europol to provide a **new notification in case Europol** would envisage **substantial changes to its access to and use of VIS data**.

3.4. Lawfulness of the processing

The VIS legislative framework allows Europol to process data within the limit of its mandate and for the performance of its tasks pursuant to Article 3(1) point 2 of the Europol Convention

[redacted]

[26] See for instance Article 7 (1a) of the VIS Decision.

(i.e. to obtain, collate and analyse information and intelligence). This corresponds to Article 4 (a) of the current Europol Regulation which provides that Europol shall collect, store, process, analyse and exchange information including criminal intelligence.

The VIS Decision limits Europol's access to VIS data for the purpose of either specific analysis or an analysis of a general nature and a strategic type.[27] This corresponds to Article 18(2)(b) and (c) of the current Europol Regulation, namely analyses for either strategic/thematic purposes or specific operational analyses within an analysis project ('AP').
The system and processes notified by Europol will be limited to the purpose of analyses of a strategic or thematic nature and of operational analyses. They address the implementation of a specific legal competence given to Europol under the VIS Regulation and the VIS Decision.

As such, there is a clear legal basis for the Agency to perform searches in VIS.

3.5. Assessment of specific data protection aspects

3.5.1. - Processing for strategic and/or thematic analyses

Article 7 (1) (b) of the VIS Decision, requires that Europol renders VIS data anonymous prior to their processing for analysis of a general nature and of a strategic type and retains them in a form in which identification of the data subjects is no longer possible. According to Article 2(k) of the Europol Regulation, "processing" should be understood as any operation or set of operations which is performed upon personal data or sets of data, whether or not by automated means, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.
The EDPS understands from the information provided in the context of the prior consultation, [redacted]

It remains unclear why Europol staff need to consult the VIS at an early stage (i.e. when Europol receives contribution from a non-Schengen country or an international organization) and not only when the Europol analyst is processing the data in view of the drafting of the strategic/thematic report. Further, this implies that non-anonymized VIS data are processed, which includes the storage of the data by Europol for purposes of thematic and strategic analysis, during the analysis and/or after the adoption of the final strategic/thematic report.

The EDPS considers that anonymising the VIS data only in the final strategic and/or thematic report is not sufficient to comply with the legal requirement of Article 7(1) (b) of the VIS Regulation. **The anonymization of VIS data should be conducted as soon as the personal**

[27] Article 3(1) of the VIS Regulation and Article 7 of the VIS Decision.
[redacted]

data are processed (including if it is only stored) for those purposes of thematic and/or strategic analysis.
In this context, the EDPS recommends including a preparatory step in the process of strategic and thematic analysis, in which the analyst consults VIS and immediately anonymises received data that are necessary for the thematic/strategic analysis. Non-anonymized VIS data should not be processed in later steps of the thematic/strategic analysis or stored after this immediate anonymization.
The EDPS **asks that Europol provides more information on the exact steps of the process in which data obtained from VIS are anonymised as well as on the anonymization methods applied**.

3.5.2 -Role of the central access point ('CAP')

[redacted]

The EDPS recalls that the key role of the central access point under the VIS legal framework is to check the legality of the access to the VIS. Only in an exceptional case of urgency, the central access point may receive written, electronic or oral requests and only verify *ex-post* whether all the conditions for access are fulfilled, including whether an exceptional case of urgency existed.

In this context, Europol mentioned that the process to access VIS data currently includes neither specific tasks for the Central Access Point to verify whether the legal conditions of each crosscheck against VIS are complied with nor does it include a workflow for urgency cases. Europol conducted several internal meetings and is in the process to designate a Central Access Point that will cover all systems (VIS, Eurodac and future EES, VIS Recast and ETIAS). Europol mentioned that it will submit to EDPS, updated documentation (process description and any other available documentation) that will include detailed information about verifying the legal conditions of each crosscheck against VIS are met and also an urgency procedure.[31] It further specified that it will have a decision regarding the designation of a common CAP for VIS and for the other administrative systems (EES, EURODAC, ETIAS) in the beginning of March. The CAP will act fully independently of the Designated Authority. Europol will update accordingly the business process for "accessing VIS data" and will make it available to EDPS on the 5th of March.[32]

The EDPS reminds that **the establishment of the Central Access Point is a legal prerequisite of the processing of VIS data**. Therefore, **Europol should postpone processing until the appointment of the Central Access Point is clarified and its tasks and processes are established**.

[redacted]

In addition, the EDPS recommends establishing a **clear process for the CAP to verify the legality and necessity of each query to VIS**. This verification cannot be performed 'ex post', unless the urgency procedure as provided for in Article 3 of VIS regulation is justified, and should be supported by the relevant technical functionality. The EDPS recommends establishing a clear set of criteria under which the urgency procedure would be justified and to apply additional controls (e.g. audit by the DPF) to ensure this opportunity is not abused.

The EDPS expects to be informed of the updated process to consult VIS and the processes of the CAP, before the start of the processing.

3.5.3 Logging/Accountability

As noted earlier, the search functionality to VIS will be provided to Europol Officials via the USE UI, which is also integrated with [redacted]. All search parameters and justification for each query in VIS will be saved in [redacted], as well as any access to the detailed records from the list of matches.

The EDPS welcomes the fact that the actual returned personal data from VIS are not logged in the [redacted] but that the identifier of the VIS record will be used instead.

When defining the process related to the verification of the necessity of each query by the CAP (see point 3.4.2), the EDPS recommends **also logging in** [redacted] **any action** related to the CAP's authorisation to query the VIS.

3.5.4 Conditions of accessing VIS data

a) Access rights

Before assigning an access role via IAM, the O1-24 team validates that each analyst is assigned cases with a crime area or typology which normally require access to VIS.

The EDPS asks to receive supporting documents identifying crime areas or typologies which normally require access to VIS.

[redacted] also ensures that the user has undergone the appropriate training before being granted access rights.[33]

The EDPS welcomes that, in addition to the training to get VIS access rights, Europol will also organise regular trainings on data protection for the staff authorised to access the VIS.[34]

b) Conditions for each query

The EDPS notes that parameters to search in VIS will be limited to first name and family name (with optional date of birth) of suspects, criminal or future criminals and that Europol will not perform searches in VIS from any of the special categories of data subjects (victims, witnesses, contacts or minors).

[redacted]

The EDPS welcomes that the Europol analyst completes an electronic form containing details on the reasoning performing the search in VIS.[35] At the moment, this is provided by a free text field, in which the analyst provides the respective SIENA message number.[36] The reasoning of the access request is a key element to verify the legality of the access. In this context, the EDPS considers that the mere reference to the SIENA message number may not be sufficient for such verification as the conclusion by the analyst on the need to consult the VIS may be triggered by additional elements read together with those included in the SIENA message. He notes that Europol is working on defining a template format of the value to be entered by the analyst so the CAP can assess the legality of the request.[37]

The EDPS recommends that the justification of the access request to the VIS is sufficiently substantiated to assess its legality. This could be done for instance by requiring the user to complete the free text field and/or including in the template format mandatory criteria justifying the access to be selected (e.g. a suspect who is national of a country whose citizens required a visa to enter the EU, there are factual indications or reasonable grounds to believe that this person might have travelled or might want to travel to the EU, etc.[38]) The EDPS further asks Europol to provide him with the template format when it is defined.

3.5.6 Transfers to third countries or international organisation

Under the VIS legislative framework, Europol may transfer VIS data to third countries or international organisations only in an exceptional case of urgency, subject to the prior consent of the Member States and exclusively for law enforcement purposes.[39]

Europol indicated that data obtained from the VIS will only be transferred to a third party if as a result of an ad-hoc assessment it results that this transfer is strictly required in an exceptional case of urgency to prevent or detect terrorist offences or other serious criminal offences in respect of what Europol is competent. The dissemination will be done in accordance with article 3 of the VIS Regulation, as well as with the Europol Regulation dissemination restrictions and will only take place with the explicit permission of the MS that owns the information stored in VIS.[40]

Europol further indicates that actions related to the dissemination of the data to non-Schengen country will be logged via SIENA (as they are not directly related to the search in VIS, but are 'follow-up' actions where needed).[41]

The EDPS recommends ensuring that **the justification of the exceptional case of urgency to disseminate the VIS data to non-Schengen country is provided (e.g. in the SIENA message to the MS having entered the data in the VIS)**

[redacted]

IV. CONCLUSION

As a general comment, the EDPS asks for future prior consultations that Europol:
- provides a data flow diagram for each purpose of the processing to fully clarify the legal framework in which it operates,
- includes in the process all applicable control measures,
- specifically describes the scenarios that would trigger the process under consultation and to indicate any processes interacting with the process at stake.

In light of all of the above, the EDPS considers that the notified processing operations will only comply with the provisions of the Europol Regulation and the VIS legislative framework when the two following conditions are met:

1) **Europol has established a Central Access Point** (CAP) **and a clear process** for the CAP to verify the compliance with the legal requirements to access VIS set up in the VIS Regulation and the VIS Decision **before starting the processing operations.**

This verification cannot be performed 'ex post', unless the urgency procedure as provided for in Article 3 of VIS regulation is justified, and should be supported by the relevant technical functionality.

2) **Europol has implemented mechanisms to anonymize VIS data before processing these data for strategic and thematic analyses**.

In addition, the EDPS formulates a series of recommendations, aimed at improving the level of safeguards implemented to tackle the specific risks of the processing. In particular, Europol should:

1. establish a clear set of criteria under which the urgency procedure would be justified and to apply additional controls (e.g. audit by the DPF) to ensure this opportunity is not abused,
2. log in [redacted] any action related to the CAP's authorisation to query the VIS,
3. ensure that the justification of the access request to the VIS is sufficiently substantiated to assess its legality,
4. ensure that the justification of the exceptional case of urgency to disseminate the VIS data to non-Schengen country is provided (e.g. in the SIENA message to the MS having entered the data in the VIS).

The EDPS asks to be provided with the following documentation before the start of the processing:

- copies of the documents describing the anonymization process and methods when processing VIS for the purpose of thematic/strategic analysis (see point 3.5.1),
- confirmation of the appointment of the Central Access Point (CAP) (see point 3.5.2),
- copies of the documents describing the process for CAP to verify the legal conditions of each crosscheck against VIS including the documentation of the urgency procedure as provided for in Article 3 of VIS regulation for the ex-post verification of a query's legality (see point 3.5.2),
- supporting documents as regards the crime area or typologies which normally require access to VIS and the template of validation criteria (see point 3.5.4).

Finally, the EDPS would like to point out that the evaluation of data protection risks is not a one-off exercise but a process. The EDPS recommends -as a general rule to be adapted to all relevant circumstances (in particular, taking into account the level of data protection risks)- a review cycle of 2 years.

We thank you for your fruitful cooperation.

Yours sincerely,

[e-signed]

Wojciech Rafał WIEWIÓROWSKI

cc.: Ms Catherine DE BOLLE, Executive Director, Europol
Mr Daniel DREWER, Data Protection Officer, Europol