EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
ASSISTANT SUPERVISOR

Mr Priit PARKNA
Chairperson
Europol Management Board
Europol Management Board Secretariat
Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

Brussels, 09 February 2018
WW/[redacted] **C 2017-0876**
Please use edps@edps.europa.eu for all correspondence

Subject: **Opinion on the prior consultation regarding "European Tracking Solution" (ETS), EDPS Case 2017-0876**

Dear Mr Parkna,

1. PROCEEDINGS

On **11 October** 2017, the European Data Protection Supervisor (EDPS) received a request for prior consultation under Article 39 of Regulation (EU) No 2016/794 ("the Europol Regulation")[1] regarding the system "European Tracking Solution" (ETS) from the Data Protection Function ("DPF") of Europol.[2]

The request for prior consultation has been filed under EDPS case number 2017-0876 and, in accordance with Article 39(4) of the Europol Regulation, it has been included in the register of processing operations notified by Europol to the EDPS under Article 39(1).

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, 24.5.2016, p. 53-114.

2 "Notification to the EDPS regarding new type of processing operation "ETS", EDOC#919054v2.

The notification sent by Europol included a general description of the envisaged processing operation as an introductory part of a document structured into 20 questions and answers.[3] The first question (Q1) indicates which of the purposes mentioned in Article 18(2) of the Europol Regulation ETS will serve. The other questions (Q2-20) list the "risks, safeguards, security measures and mechanisms to ensure the protection of personal data". In addition, the ETS Requirements[4] were attached to the notification as supporting documentation.

On **31 October** 2017 the EDPS, following a first assessment of the processing operations, sent to Europol's DPF a draft description of the processing with a list of points for which the EDPS required confirmation, further information and clarifications. On **12 January** 2018, Europol's DPF replied to the EDPS' request.[5]

On **2 February** 2018, the EDPS sent to Europol a draft Opinion for comments.

On **8 February** 2018 the EDPS received the comments of Europol.[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 he may have requested[7] up to a maximum of four months; the deadline within which the EDPS shall issue his Opinion in this case is **12 February** 2018.

2. DESCRIPTION OF THE PROCESSING

ETS will be a tool enabling specialist units in Member States (MS) and operational third parties (TP) ("users") to **exchange geo-location data in near real time for the purpose of tracking and tracing objects/subjects** of common interest in the context of "red force" and "blue force" operations. "Red force" operations refer to the tracking of data subjects on the offenders' side such as suspects, associates or potential future criminals. "Blue force" operations refers to the tracking of data subjects on the law enforcement's side such as victims, witnesses and covert police officers. Initially ETS will be tracking red-force only. Gradually however the objects of interest are expected to be: 90% red-force, 10% blue force.

ETS is intended to allow a more efficient and effective tracking of data subjects (suspects, victims, witnesses and covert officers).[8] A surveillance unit on one side of the border will be

---

3 According to Article 39(2) of the Europol Regulation, the notification to the EDPS by Europol DPO shall be accompanied by at least: the **general description** of the envisaged processing operations; the **assessment of the risks** to the rights and freedoms of data subjects; the **measures envisaged** to address those risks; **safeguards** and **security measures** and **mechanisms** to ensure the protection of personal data and to demonstrate compliance with the Europol Regulation, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

4 EDOC#901702v4

5 EDOC#930648v3

6 EDOC#947171

7 In the present case, the deadline was suspended: from 31 October 2017 until 12 January 2018.

8 ETS Requirements, BNEED-16481, p.4

able to make use of a beacon[9] which has already been placed in an object[10] at the other side of the border. ETS will also maximise the exchange and availability of criminal information. ETS can support any cross-border operation making use of tracking beacon data. This can include operations conducted in the context of Joint Investigation Teams, controlled deliveries cross-border surveillances, etc. The MS/TP will have the choice to use ETS when the need to share near real time tracking data arises, on a case-by-case basis. ETS will thus support the provision of effective co-ordination of cross-border operations by Europol when requested to MS and TPs.[11]

MS/TP agreeing to receive such geo-location data can either pull the data from ETS and view it on their own infrastructure or view the data directly from ETS using a secure access (web viewer functionality). The first purpose of ETS is thus to facilitate information exchange between operational partners.

ETS will also allow Europol to process geo location data, **upon request of MS/TPs, for purposes of analysis** (strategic/thematic analysis, operational analysis), on a specific dataset. The request will be sent via the established secure communication channel (SIENA). Europol will then extract the relevant dataset from ETS and insert it into the Europol Analysis System (EAS). This second purpose of ETS will enrich the Europol Analysis System (EAS) with data on time and movement. This is listed as one of the business functionality of ETS. .[12]

ETS still is a project under development. The aim for 2017-2018 is to implement ETS as a "Beta version". Although the system will be ready to support cross-border operations, not all functionalities will be immediately available, e.g. the web viewer functionality will not be activated yet and the down-time could potentially be too long to guarantee operational continuity. [13] Europol however did not provide any additional information in this regard.

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 the following processing operations to prior consultation by the EDPS:

(a) processing of special categories of personal data as referred to in Article 30(2)[14]; 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.[15]

---

9 A beacon is a small object with a radio frequency transmitter which sends signals to a receiver to indicate relative direction and distance to the transmitter.

10 In most of the cases an object will be a car or any other means of transport (truck, boat etc.), or also other objects like a parcel for example that have been determined by operational needs.

11 ETS Requirements, BFNC-16483, p.5

12 ETS Requirements, BNEED-16482, p.4 and BFNC-16502, p.5

13 EDOC#930648v3, p.7

14 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.

15 According to recital 50 of the Europol Regulation, this obligation does not refer 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 notification[16] indicates that "*the envisaged new type of processing operation* (...) *includes the processing of data that present a specific risk for the fundamental rights and freedoms of data subjects.*" The risk is triggered by the fact that "*near real time tracking of objects or subjects using electronic devices might be considered as an intrusive form of technical surveillance.*"

The main risks to the rights and freedoms of data subjects stem from the processing of geo-location data. ETS will be a tool designed to enable cross-border tracking of data subjects put under surveillance in near real time. It thus facilitates the sharing of geo-location data between law enforcement authorities and with Europol.

The processing of geo-location data entails *per se* specific risks for data subjects as they inform about places visited during a given period of time. The further processing of tracking data may thus reveal information about the data subject's health (visits to doctors, hospitals), political opinions (visits to the offices of political parties), religious beliefs (visits to churches of a given confession), trade union membership (visits to the offices of trade unions) and sex life. In the present case, this risk is increased as ETS will allow users to upload on the platform additional information such as video footage or CCTV. This should help users identifying locations frequently visited by the person of interest and indicating their relevance for surveillance purposes.[17]

The use of ETS as a tool to exchange geo-location data (first purpose) will only involve the "NMEA+ standard"[18] data string, which does not contain sensitive persona data. [19] In addition, the notification initially indicated the possibility for MS/TPs to add contextual information such asvideo footage or CCTV. [20] Europol however further specified in its comments that this functionality was no longer foreseen in the current ETS setup.[21]

ETS also contains a function which allows users to export these geo-location data to the EAS for purposes of criminal analysis (second purpose). The use of ETS thus facilitates in practice the sharing with Europol of geo-location data of persons put under surveillance at national level.

The tool has thus a potential high impact on individuals' rights to privacy and to data protection (Articles 7 and 8 of the EU Charter of Fundamental Rights - "the Charter" - respectively) but also on other rights and freedoms. The further processing of geo-location data for purposes of criminal analysis could entail interferences into individuals' freedom of thoughts, freedom or religion (Article 10 of the Charter) and freedom of assembly and association (Article 12 of the Charter) in case information about political opinions, religious beliefs or trade union memberships is inferred from the data, and into their right to non-discrimination (Article 21 of the Charter) if such information is used to base decisions which produce adverse legal effects concerning them.

As regard the duration of the processing, geo-location data of individuals being tracked will be processed on the ETS platform "*as long as it is necessary for the purpose of sharing the*

---

16 At page 2

17 ETS Requirements, STORY-22428, p.12-13.

18 National Marine Electronic Association. The NMEA has developed a specification that defines the interface between various pieces of marine electronic equipment. The standard permits marine electronics to send information to computers and to other marine equipment. GPS receiver communication is defined within this specification.(source: http://www.gpsinformation.org/dale/nmea.htm).

19 Notification form, p 4

20 ETS Requirements, STORY-22428 Additional relevant information.

21 EDOC#947171, p.1

information" and is related with an on-going cross border investigation. If the data is shared with other MS or TPs making use of the web viewer, the duration of the processing is defined by the data owner when the request is formulated. After the end of that duration (an on-going investigation) the data are not available anymore. For system to system sharing (i.e. data pulled from ETS by the user and viewed on its own infrastructure), the national tracking systems of the MS/TP will be able to send data to ETS and vice versa. However, once the data are exported to the EAS, the processing of the geo-location data will fall under the Europol Regulation and Europol's internal policies. This means that the data will be subject to the three years' review process.

Since ETS relates to the use of new technologies, which present specific risks to the rights and freedom of individuals, the EDPS considers that ETS **is subject to prior consultation** in accordance with **Article 39(1)(b)** of the Europol Regulation.

3.2. Scope of the Opinion

The Opinion of the EDPS on this prior consultation **only concerns ETS as described in the notification** of 11 October 2017[22] and appended documentation, i.e. as a tool to process geo-location data.

3.3. Legal basis of the processing

ETS will give rise to two distinct personal data processing activities:
(1) Cross-border exchange of geo-location data between MS/TP;
(2) Further processing of geo-location data for purposes of criminal analysis (strategic/thematic/operational) by Europol.

While ETS is primarily a tool implemented for the purpose of facilitating exchanges of geo-location data between MS/TPs, the possibility to export this information from ETS to the EAS will facilitate the transfer and further processing of geo-location data by MS/TP to Europol, eventually enriching the EAS with data of a very sensitive nature and allowing their transfer on a bigger scale. The two data processing activities are thus assessed separately.

3.3.1. Cross-border exchange of geo-location data

ETS will be a tool made available by Europol to MS and TPs to share geo-location data about suspects, potential future criminals, victims, witnesses and covert police officers.

As mentioned above, the ETS can support any cross-border operation making use of tracking beacon data. This can include operations conducted in the context of Joint Investigation Teams, controlled deliveries, cross-border surveillances, etc.[23] MS/TPs have the choice to use ETS when the need to share near real time tracking data arises or on a case by case basis.

---

22 EDOC#919054v2
23 EDOC#930648v3, p.2

The development of ETS thus relates to Europol's task to "*support Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, including by providing* (...) *technical* (...) *support*"[24].

In that context, Europol acts as IT service provider. Europol designs and develops the tool, deciding on the purpose and means. Once the tool is operational, Europol will not take part in the exchange of information but will host the tool and act as administrator. In that sense, Europol is responsible for processing the requests of use submitted by MS/TPs, for configuring the tool accordingly and for ensuring the security of the personal data processed within ETS, as well as their auditability. Europol and MS/TPs thus act as co-controllers.

As long as Europol does not take part in the exchange of information, such data processing activities do not fall under the Europol Regulation but under the Council Framework Decision 2008/977/JHA[25], which will be repealed on 6 May 2018 by the Directive (EU) 2016/680[26] ("the Law Enforcement Directive"). Article 21 of the Law Enforcement Directive stipulates that in case of joint controllership, the allocation of responsibilities should be determined in a transparent manner or in accordance with the Union and MS law to which the controllers are subject. In that regard, Article 38(7) of the Europol Regulation states that Europol shall not be responsible for the bilateral exchanges of data using Europol's infrastructure between Member States, Union bodies, third countries and international organisations, to which Europol has no access. These bilateral exchanges take place under the responsibility of the entities concerned and in accordance with their national law. However, Europol should ensure the security of the exchanges in accordance with Article 32 of the Europol Regulation.

In addition, under the principle of data protection by design, both included in the Law Enforcement Directive[27] and the Europol Regulation[28], Europol, in its quality of designer and developer of the system, should ensure that ETS complies with the provisions of the Law Enforcement Directive and related transposition laws.

In particular, as the use of ETS will imply a "*type of processing, in particular using new technologies*" which will "*result in high risk to the rights and freedoms of natural persons*"[29], national law enforcement authorities will have to perform a data protection impact assessment prior to the use of ETS. Such data processing activities will further have to be notified to the supervisory authority for prior consultation in accordance with Article 28 of the Law Enforcement Directive. Europol should thus support MS in this obligation.

The EDPS therefore recommends Europol to support MS in complying with the requirements of **the Law Enforcement Directive and related national transposition laws**. This task falls outside the scope of competences of the EDPS.

---

24 Article 4(1)(h) of the Europol Regulation

25 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p.60-71

26 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131. See Article 59(1)

27 Article 20

28 Article 33

29 Article 27 of the Law Enforcement Directive

3.3.2. Processing of geo-location data for purposes of criminal analysis

The geo-location data shared by MS/TP on ETS can be further extracted and imported into the EAS, upon request. Analysis (strategic, thematic or operational) will not be performed within ETS. The request will be handled as a standard analysis request.

The processing of ETS data for criminal analysis purposes will thus fall under regular Europol's tasks as defined in Article 4(1) of the Europol Regulation. The basis for these data processing activities will be Article 18(2)(b) or (c) of the Europol Regulation, depending on the purpose of the request.

3.4. Assessment of specific data protection aspects

In this Opinion, we will consider the **main data protection issues** concerning the processing of personal data at stake, having regard to the measures envisaged by Europol to address data protection risks. The most relevant provisions of the Europol Regulation in this context are in particular Articles 30(1) (processing of specific categories of data subjects), Article 30(2) (processing of sensitive data), Article 32(2)(f),(g) and (h) (auditability) and Article 40 (logging).

3.4.1. Export of the data to EAS

The Export function will facilitate and encourage further use of geo-location data for purposes of criminal analysis. It is foreseen that data from ETS can be exported into the EAS upon a specific request from MS/TP directed through SIENA[30], but as of now, the function has not been fully developed. ETS will initially allow any user, who has access to a beacon, to export the beacon history in an excel format and then send this information by a SIENA message to Europol for the purposes of criminal analysis.

This file contains the information transmitted by the beacon, namely: data time, comment, object reference, message time, status, speed, GPS fix.[31] This excel sheet can be further shared with Europol through the regular channels of collaboration. [32] We understand from the documentation provided that the user cannot export any additional information.

The application roles can be configured to remove the ability to export data. [33]

We also understand from the description provided by Europol that both the data owner and data recipient will be given the option to export the data and to send it to Europol. As mentioned above, the processing of geo-location data in the context of ETS falls under the provisions of the Law Enforcement Directive. Article 4(2) will apply to data exchange between MS and to the further processing of such data for purposes of criminal analysis. This article requires, in particular, that the further processing is necessary and proportionate. Further processing by TPs will be subject to the provisions of the instrument regulating the initial data exchange. This

---

30 Notification form, Q1, Q8
31 EDOC#930648v3, p.7
32 EDOC#930648v3, p.7
33 EDOC#930648v3, p.7

assessment is under the responsibility of the MS/TP which decides to export the data from ETS towards Europol.

However, given the sensitivity of the information processed, the EDPS recommends that the **possibility to export the data from ETS to the EAS** is **only given to the data owner**, i.e. to the MS/TP which placed the beacon and required specific authorization to do so.

3.4.2. Processing of specific categories of data subjects for criminal analysis purposes[34]

ETS will involve the processing of geo-location data related to suspects ("red force" data subjects), and of data related to victims, witnesses and covert police officers (covert operative) ("blue force" data subjects). Further processing by Europol of data related to victims and witnesses will fall under Article 30(2) of the Europol Regulation and should be allowed only if strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives. The import into the EAS will be subject to the provisions of the Opening Order of the Analysis Project to which they are sent.

The legal basis for the processing of personal data related to covert police officers is however not clear. Annex II.B.(1)(f) of the Europol Regulation foresees the processing of personal data of "*persons who can provide information on the criminal offences under consideration*", a specific category of data subjects which refers to "informants"[35]. Informants however usually refer to members of criminal organisations, not to covert police officers.

The EDPS thus recommends to **prevent the export of personal data relating to covert police officers** from ETS to the EAS.

3.4.3. Processing of sensitive data for criminal analysis purposes[36]

ETS will not directly involve the processing of sensitive data. ETS will only process the GPS coordinates of the beacon placed by the competent authority of the MS/TP of origin to track the data subjects. ETS only processes the NMEA+ data string, which includes ID, time, sentence, receiver latitude, latitude, longitude, speed, heading, date, magnetic variation and checksum.[37]

The beacon can be placed in a car, but also on any object, container, means of transport could theory be traced e.g. parcel, container, truck, boat, motorbike, etc. The place where the beacon is installed is determined by operational needs, tactical conditions and the applicable national law.[38]

The further extraction of geo-location data from ETS for its import into the EAS may reveal sensitive data, in particular data about religious beliefs, political opinions or trade union membership or even sex life. In those cases, Article 30(2) of the Europol Regulation will apply.

---

34 Article 30(1) of Europol Regulation.

35 See in that sense Europol portfolio of Opening Decisions of Operational Analysis Projects from 24 November 2017, EDOC#930815.

36 Article 30(2) of Europol Regulation.

37 ETS Requirements, Annex A "NMEA+ Format".

38 EDOC#930648v3, p.5

Europol is aware of this risk and refers to two types of safeguards[39]:

(1) At national level the interpretation or further use of this information will be conducted in compliance with applicable national law which will in most scenarios include supervision by a judicial authority.

(2) At Europol the processing of sensitive personal data potentially deriving from further analysis of ETS beacon data will comply with Article 30(2) of the Europol Regulation, i.e. only where this is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol. The selection of a particular group of persons solely on the basis of such personal data is prohibited. To that end, full compliance with all safeguards established by means of the relevant analysis project portfolio will be ensured. In particular, this means that sensitive personal data in relation to beacon data will only be processed if this is foreseen in the data category tables of the respective operational analysis projects (EDOC#886096).

The EDPS is **satisfied** with the safeguards implemented to tackle the risks.

3.4.5. Auditability[40]

With regard to logging obligations, Article 40 of the Europol Regulation will apply to the data processing operations performed by Europol, while Article 25 of the Law Enforcement Directive will apply to the exchange of personal data by MS and TP. Both articles cover the same type of operations. Article 25 of the Law Enforcement Directive however specifies the minimum content of the logs (justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data).

The auditability of ETS will be ensured, in the long run, through Europol's Unified Audit Solution (UAS)[41]. In the meantime, ETS will have a specific auditing facility.[42] An auditor role is foreseen.

This auditing facility will ensure the possibility to verify *to which bodies* personal data may be or have been transmitted; *what data* have been inputted by which member of personnel and at what time; that detailed *records of all transfers* of personal data and of the grounds for such transfers are recorded (traceability of the requests and responses).[43]

Europol further indicated that the logging will be set up in accordance with Article 40 of the Europol Regulation.[44] These logs are intended to the DPF, and, upon request, to the EDPS and national supervisory authorities.

---

39 EDOC#930648v3, p.6

40 Article 32(2)(f), (g) and (h) and Article 40 of the Europol Regulation.

41 Notification form, Q16

42 Notification form, Q15

43 The grounds for the transfer of personal data will be recorded within the accompanying SIENA message detailing the context and/or conditions regarding data exchange. See Notification form, Q15.

44 EDOC#930648v3, p10

As mentioned above, the exchange of information between MS and TPs taken place in the context of ETS is subject to the provisions of the Law Enforcement Directive and national implementing laws. Such data processing activities should thus be logged in accordance with Article 25 of the Directive and include the minimum information referred to in this article.

The EDPS recommends that the **logs** shall be **available to MS/TPs, allowing** them to monitor the appropriate use of ETS.

The EDPS recommends that the **content of the logs reflects the minimum information referred to in Article 25 of the Law Enforcement Directive**, namely: justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

It is also advised that **automatic rules for tracing suspicious behaviour** shall be implemented into the logging system with real time notification to the appropriate staff of Europol and MS.

We also recommend that the **format of the logs** is **readable**, i.e. that it allows the DPF, the EDPS and national supervisory authorities to easily process the information they contain.

The EDPS also recommends that, **once a year**, given the sensitivity of the data processed, the DPF performs a **thorough review** of the data processing activities taking place under ETS.

3.4.6. Security of Processing

As far as security measures are concerned, Article 32 of the Europol Regulation applies. As this article mirrors Article 29 of the Law Enforcement Directive, and includes an additional obligation to implement access logs,[45] compliance with Article 32 of the Europol Regulation will ensure compliance with Article 29 of the Law Enforcement Directive.

The EDPS has requested more information from Europol in particular whether an analysis of the risks have been applied for the specific processing. Europol, in its reply, did not address the security aspects. Several safeguards are foreseen in the ETS Requirements to be applied in order protect the overall nature of the ETS infrastructure.

As ETS is currently under development, the documentation provided by Europol **is not sufficient to enable the EDPS to provide a comprehensive list of recommendations on security issues.** Therefore, EDPS requests that Europol submits more information on security aspects related to ETS when available.

In addition, the EDPS recommends that when Europol finalizes ETS requirements, it proceeds to a security risk assessment to identify the appropriate security measures and it informs the EDPS thereof.

Europol shall **proceed to a security risk assessment** for ETS to identify and apply the appropriate security measures. Europol shall inform the EDPS accordingly, after which the EDPS will assess whether the security issues are adequately addressed.

[45] Article 32 (2)(h)

However, based on the current ETS Requirements some specific recommendations can be provided.

ETS is an IT infrastructure enabling specialist units in MS and operational TP to exchange geo-location data in near real time for the purpose of tracking and tracing objects/subjects of common interest. In the context of ETS, Europol acts as a service provider only hosting the IT infrastructure. Thus, the main purpose of the processing operation is limited to the facilitation of information exchange between operational partners. Most of the Europol Security Policies are applied as ETS will be installed and secured at Europol premises.

As described in the ETS Requirements, the national tracking systems of the MS/TPs will be configured to feed the ETS (and receive from) real time data revealing geo-location of a beacon when there is a need for an on-going surveillance investigation. A MS will also be able to view the data via a secure access directly from ETS. The technical details and especially the security of the possible inter-connection or transfer of data between national systems and ETS shall be carefully designed.

Europol shall provide **guidelines for the implementation of secure technical measures for the protection of the transfer of data** between ETS and the national systems of the Member States and Third Parties.

3.4.7.1 User management and Authentication

As the access management is a critical aspect for the use of ETS, a role based access control model has been defined by Europol to apply a need-to-know access policy for the users. Europol and every law enforcement partner will have at least one PoC (Point of Contact) managing the data shared by them and coordinating/further dispatching the data shared with them. Moreover, standard users from the specialised units in Europol and MS/TP will have viewing rights only based on a case-by-case basis.

Currently user management is provided by the Europol Platform of Experts (EPE) and in the future will be provided by a dedicated identity and access management (IAM) solution.

For the user authentication, Europol considers to apply a two factor authentication[46]. The EDPS is supporting the enforcement of this measure.

Following the ETS Requirements and based on the sensitivity of the specific context of the processing, the EDPS requests that Europol applies to ETS a **two factor authentication scheme**.

3.4.7.2 Encryption

ETS data are not encrypted in the current ETS requirements. For transmission of ETS data between the MS a VPN is foreseen to protect beacon information. The EDPS recommends that Europol considers applying full encryption for ETS.

The EDPS recommends that Europol considers applying **full encryption** for ETS.

46 ETS Requirements, p11

* *
*

In the light of all of the above, the EDPS considers that the notified processing is compliant with the Europol Regulation (with reference to point **3.2.** of this Opinion).

In addition, the EDPS formulate 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. Support MS in ensuring full compliance with the Law Enforcement Directive and related national laws transposing the Directive when using ETS.

2. Restrict the possibility to export the data from ETS to the EAS to data owners, i.e. the MS/TP which placed the beacon to export the data to the EAS.

3. Prevent personal data relating to covert police officers to be exported from ETS to the EAS.

4. Ensure that the format of the logs reflects the minimum information referred to in Article 25 of the Law Enforcement Directive, namely: justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

5. Implement automatic rules for tracing suspicious behaviour into the logging system with real time notification to the appropriate staff of Europol and MS.

6. Ensure that logs are available to MS/TP and enable them to monitor the appropriate use of ETS

7. Ensure that the format of the logs is available and readable, i.e. that it allows the DPF, the EDPS or national supervisory authorities to easily process the information they contain for the purpose of verification of the legality of the processing operation.

8. Have an annual audit of the data processing activities taking place under ETS performed by the DPF.

9. Conduct a security risk assessment to identify and apply the appropriate security measures and inform the EDPS accordingly.

10. Provide guidelines for the implementation of secure technical measures for the protection of the transfer of data between ETS and the national systems of the MS and TPs.

11. Apply a two factor authentication scheme for user authentication.

12. Consider applying full encryption for ETS.

Finally, given that ETS is a tool which will permit the exchange of information between MS and TPs subject to the provisions of the Law Enforcement Directive, the EDPS will inform the national supervisory authorities about this Opinion pursuant to Article 44(3) of the Europol Regulation.

The EDPS expects to be informed about the follow up of the above-recommendations **within six months.**

Please also note that the EDPS asks you to provide a **new notification in case Europol** would envisage **substantial changes to ETS**.

We thank you for your fruitful cooperation.

Yours sincerely,

[redacted]

Wojciech Rafał WIEWIÓROWSKI

Cc: Mr Robert WAINWRIGHT, Executive Director, Europol
Mr Daniel DREWER, Data Protection Officer, Europol