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

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**.

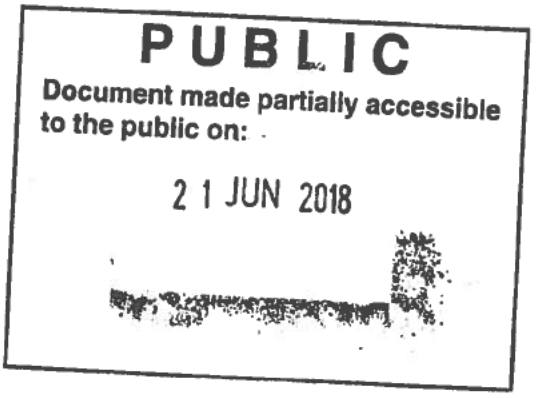
We thank you for your fruitful cooperation.

Yours sincerely,

[redacted]

Wojciech Rafał WIEWIÓROWSKI

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



Opinion ECB-O-2019-01 on the European Tracking Solution (ETS)

1. Background

On 9 February 2018, the EDPS issued an opinion in the context of its consultation by Europol in conformity with Article 39 of the Europol Regulation (ER) regarding the "European Tracking Solution" (ETS) (EDPS Case 2017-0876).

On 9 March 2018, the EDPS shared this Opinion with the Europol Cooperation Board (ECB) in accordance with Article 44(3) ER, given the use of ETS by national law enforcement authorities and the legal concerns that ETS may thus trigger from a domestic (data protection) perspective.

Following initial discussion during its 3rd meeting on 30 May 2018 and continued discussion during its 4th meeting of 3 October 2018, the ECB, in conformity with Article 45(4) ER, issues the Opinion expressed hereafter.

The recommendations contained in point (a) of this Opinion relate to the risk of unlawful cross-border exchange of geo-location data between Member States ("MS") or between MS and Third Parties ("TP") as envisaged under the ETS. They are thus addressed to Europol as designer of the tool and to national authorities as primary users of the system. ECB members are thus required to communicate this Opinion to the relevant competent authorities, according to their respective scopes of competences.

2. Opinion

In line with ETS' dual purpose, i.e. (a) the cross-border exchange of geo-location data between MS/TP with Europol as a so called mere service provider (primary purpose) and (b) the further processing of geo-location data for purposes of criminal analysis (strategic/thematic and operational) by Europol (secondary purpose), point (a) of the below Opinion relates to ETS' primary purpose, whilst point (b) relates to its secondary purpose.

a. Risks of unlawful cross-border exchange of geo-location data

1. *Introduction*

In checking compliance of ETS' primary purpose, the EDPS opinion already pointed out that the development of ETS 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" (Article 4(1)(h) ER).

The EDPS opinion labeled Europol's role in this context as the one of an "IT service provider", a "host" of the tool, an "administrator", and therefore as a "co-controller". The opinion continued by – again rightly – pointing out, as stipulated in Article 38(7) ER, that Europol is not responsible for the "bilateral exchange of data using Europol's infrastructure between Member States, Union bodies, third countries and international organisations, to which Europol has no access" and that "such bilateral exchanges shall take place under the responsibility of the entities concerned and in accordance with their law".

On the basis of the above, the EDPS concluded that the primary purpose activities of ETS do not fall under the ER, but under Directive (EU) 2016/680, i.e. the Law Enforcement Directive (LED), with a sole role for Europol to ensure the security of exchanges in accordance with Article 32 ER (ex Article 38(7)).

Equally, the EDPS has stressed the responsibility of Europol in the context of ETS' primary purpose activities as a co-controller, implying that Europol, in its quality of designer and developer of ETS, should support MS in complying with the requirements of the LED and related national transposition laws.

In particular, national law enforcement authorities will have to perform a data protection impact assessment before being authorised, at national level, to use ETS as the cross-border exchange of geo-location data 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" (see section 3 infra).

> LED | Article 27. Data protection impact assessment
>
> 1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

The measures envisaged to address those impacts will involve the implementation of organizational and technical measures. It follows that the responsibility of national law enforcement authorities and of Europol to comply with the principle of data protection by design, both included in the LED (Article 20) and the ER (Article 33) takes particular significance in that context:

> LED | Article 20. Data protection by design […]
>
> 2. Member States shall provide for the controller, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Directive and protect the rights of data subjects.
> 3. […]
>
> Europol Regulation | Article 33. Data protection by design
>
> Europol shall implement appropriate technical and organisational measures and procedures in such a way that the data processing will comply with this Regulation and protect the rights of the data subjects concerned.

2. *Limited scope to allow ETS use by operational Third Parties*

ETS is explicitly open for use by so called operational TP. The notion of TP has not been defined, but seems to target law enforcement authorities from third countries or international organisations with which Europol has concluded an operational cooperation agreement allowing for the transfer of personal data.

The question arises to which extent Europol may lawfully host or administer ETS for use by so called TP.

It may be the case that, in accordance with Article 13(12) EU MLA Convention,[1] "to the extent that the laws of the MS concerned or the provisions of any legal instrument applicable between them permit" so, representatives of third states or of bodies set up pursuant to the TEU, like Europol, take part in the activities of a joint investigation team (JIT).

The case being, Europol staff, in accordance with Article 5(2) ER, "within the limits of the laws of the Member States in which [the] joint team is operating" may assist in all activities and exchanges of information with all members of the joint team".

Since ETS, in its current beta or demo stage, does not require MS to *ascertain/certify on a case-by-case basis* that a TP they wish to share geo-location tracking data with is effectively participating in a JIT and that such participation is permitted under and within the limits of their laws, there is a risk that the processing of geo-location data under ETS is unlawful. Under the principle of privacy by design (supra), national law enforcement authorities and Europol should implement appropriate technical and organisational measures to minimise that risk.

Europol proposes to tackle this risk by routing access requests to ETS tracking data through Siena. According to the information provided by Europol to the EDPS, "MS/TPs will have to officially request the use of ETS over SIENA, confirming legality, indicating the desired partners and potentially including additional instructions/restrictions/authorisations". This request could also contain contextual or case related data, which would not be transferred or made available within the ETS.

It thus seems that the TP with which the possibility of data sharing is actually foreseen, are only TP that Europol has concluded an operational cooperation with, since Siena has only been rolled out to TP that have concluded an operational or strategic cooperation agreement with Europol.

Given that the primary purpose activities of ETS do not fall under the ER, but the LED, the fact that Europol has concluded an operational cooperation agreement with a certain TP does not legitimize sharing ETS data with the latter.

The LED leaves it to the MS to assess whether they can actually exchange personal data with third countries or organisations, based on either an adequacy decision by the European Commission (Article 36 LED), a positive MS assessment of appropriate safeguards (Article 37 LED) or in case of specific, derogative situations (Article 38 LED), whilst currently none of the above seem to be in place or apply, except for – possibly – a possible MS assessment in the sense of Article 37, which then needs to be checked beforehand in order for ETS to comply with the principle of privacy by design.

Hence, it seems that the current, Siena-request based possibility to share geo-location tracking data through ETS with Europol operational TP does not seem sufficient to minimise the risk of unlawful processing of geo-location data within ETS. Additional mechanisms should be put in place to ensure that:

- **the cross-border exchange of geo-location data is situated in the context of a JIT in which participation by the TP concerned is permitted under and within the limits of the laws of the sharing MS, and**

[1] Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ 12 July 2000, C 197.

- **the TP concerned qualifies as adequate TP from a MS perspective under the LED, i.e. based on either an adequacy decision by the European Commission (Article 36 LED), a positive MS assessment of appropriate safeguards (Article 37 LED) or in case of specific, derogative situations (Article 38 LED).**

Consequently, in order to prevent the risk of unlawful sharing of ETS data with TP, the ECB recommends Europol to enhance ETS' design so as to not allow ETS geo-location tracking data sharing with TP unless the sharing MS has ascertained/certified on a case-by-case basis that the above conditions have been fulfilled. This will allow national authorities to minimise the risks of unlawful cross-border exchange of geo-location data when making use of ETS.

3. Cross-border geo-location tracking: Not a mere law enforcement cooperation issue

The (near) real-time cross-border sharing between MS (and TP) of geo-location data is to be regarded as a coercive cross-border investigation measure, therefore being the prerogative of judicial authorities (and requiring mutual legal assistance (MLA) as a form of judicial cooperation in criminal matters), and not as a matter of mere information exchange between law enforcement authorities.

Hence, Europol, as the EU's Agency for *law enforcement* cooperation, must adapt ETS' design so as to prevent any use of it by law enforcement authorities of either the requesting/issuing or requested/executing state unless, on a case-by-case basis, all of them have ascertained/certified that the domestic conditions for cross-border geo-location tracking as an intrusive investigation measure, which is a matter of *judicial* cooperation in criminal matters, are fulfilled in the case at hand.

By means of (historical) background, there is merit in mapping the long EU track record in categorizing sensitive, special, coercive or intrusive cross-border forms of cooperation as judicial in nature, even where of course law enforcement authorities are involved.

This is the case for cross-border observation (see the 1990 Convention implementing the Schengen Agreement or the CoE's 2nd additional protocol of 2001 to the 1959 European Convention on Mutual Assistance), joint investigation teams, controlled deliveries, covert operations and interception of telecommunications (see the 2000 EU MLA Convention and the 2014 European Investigation Order).

Moreover, as far as specifically the cross-border use of technical equipment is concerned, it was at the repeated insistence of the German delegation that – in Spring 1996 – the idea was for the first time raised (and supported) to draw up a regulation in the context of MLA (as a form of *judicial* cooperation in criminal matters) for a number of specific modern forms of cross-border cooperation which practice was not yet familiar with at the time that the 1959 CoE European Convention on Mutual Assistance was drawn up, including *'the cross-border use of technical equipment and resources'*.[2] In practice, the cross-border use of observation equipment took place under conditions which differed greatly from MS to MS, without any (specific) basis in international cooperation instruments[3] – a situation which hasn't changed until date. The German delegation therefore

[2] In addition to other cooperation forms such as: cross-border observation and pursuit, controlled delivery, cross-border deployment of police infiltrators, cross-border use of informers and infiltrators and the deployment of joint investigation teams (some of which were eventually regulated in the EU Convention of 29 May 2000 on mutual assistance in criminal matters). See the orientation note drawn up by the German delegation at the request of the then EU Working Party on Mutual Assistance (COUNCIL, 6416/96 JUSTPEN 47, 10 April 1996, 5-6).

[3] Notwithstanding the absence of a specific basis in international law, Germany itself seemed nevertheless to be open to foreign requests in this respect. See: COUNCIL OF EUROPE, PC-OC / Inf 9, 2 February 1998, 19: "Particular

insisted on drawing up general rules for the use of such investigation methods and techniques, in particular in the case that it would not be possible, for reasons of urgency, to send a request for legal assistance to the other MS in time - i.e., in advance.[4] As a result, an explicit opening was retained in the 1996 working programme[5] of the then EU Working Party on Mutual Assistance (WPMA) to examine the use of such special investigation methods when drawing up the EU convention on mutual assistance (which eventually would be adopted on 29 May 2000).

Temporary momentum was gained when a working memorandum of the then Irish EU Presidency was very well received at the JHA Council of 28-29 November 1996. The document,[6] also supported by the European Council in December of that year (Dublin II Summit), referred to a number of modern methods which, according to the presidency, would result in an intensification of the fight against international organised crime. According to the memorandum, the possibilities with regard to […] *video and camera surveillance* […] were particularly important in this respect. The memorandum, appointing the mentioned methods and figures as 'means to deal with *judicial* [italics added] cooperation in an effective way', undeniably formed the run up to the later recommendations on the matter of the High Level Group (HLG) on Organised Crime established at the Dublin II Summit. Recommendation 16(b) of the HLG Action Plan[7] exhorted the WPMA to examine how legal grounds could be created for the cross-border application of the modern investigation methods concerned.

Background information[8] used by the WPMA revealed that the MS made widespread use of a number of the investigation methods referred to. However, in the light of the important differences revealed both in the regulations and in the practice of the various MS, and given the fact that in practice, not *all* of the methods referred to were used in all of the MS, the general conviction developed in the WPMA that detailed rules did *not* have to be drawn up for each of the investigation methods referred to, at the level of the EU.[9] For that reason, it was decided to only examine the following investigation methods in more detail in the WPMA: controlled deliveries, *the cross-border use of technical equipment for monitoring vehicles or objects*, and the use of undercover agents. During the WPMA meeting of 26-27 February 1997, the plans were further adjusted in the sense that only controlled deliveries and cross-border activities of police infiltrators would be regulated in the EU MLA *Convention* (of 29 May 2000).[10] After the importance and efficiency of techniques such as *electronic surveillance*[11] had once again been emphasised in the pre-accession pact on organised

attention should be afforded to requests for the following assistance measures for which [...] there is as yet no provision under international law: [...] 12. cross-border deployment of technical equipment, such as direction finders on suspicious vehicles, […]".

[4] COUNCIL, 8634/95 JUSTPEN 100, 29 June 1995, 4; COUNCIL, 10198/95 JUSTPEN 128, 7 November 1995, 4.

[5] COUNCIL, 12854/95 JUSTPEN 169, 19 December 1995, 4.

[6] COUNCIL, 11564/2/96 REV 2, CK4 53, 26 November 1996, 5-7; COUNCIL, 11564/4/96 REV 4 CK4 53, 4 December 1996, 5-7.

[7] See also the previous (draft) versions of the HLG report: COUNCIL, 6276/3/97 REV 3 JAI 7, 2 April 1997, 25; COUNCIL, 6276/4/97 REV 3 JAI 7, 9 April 1997, 24. The preparatory documents of the meeting of the HLG of 20 February 1997 already pointed out that the (future) draft convention on mutual legal assistance should contain a legal basis for the use of investigative methods, sucha as the deployment of *undercover*-agents (police infiltrators) and the interception of various forms of telecommunication (COUNCIL, 5869/97 JAI 4, 11 February 1997, 22).

[8] Namely: *Manuel de l'Union européenne sur les livraisons surveillées* (COUNCIL, 10465/1/96 REV 1 ENFOPOL 151) and EUROPOL DRUGS UNIT, 1996, 53 p.

[9] COUNCIL, 5816/97 JUSTPEN 9, 13 February 1997, 3-4.

[10] COUNCIL, 6556/97 JUSTPEN 18, 11 March 1997, 2.

[11] Also: infiltrations and controlled delivery.

crime between the MS of the EU, the CCEEs and Cyprus,[12] drawn up at the instigation of the Multidisciplinary Group on Organised Crime (GMD), the WPMA decided that a regulation for *the use of technical equipment for observation purposes*, and possibly also for the use of supergrasses and informers (civilian infiltrators) would be included in the Additional Protocol to the EU MLA Convention (negotiated in parallel with the final negotiation phase of the Convention itself, and eventually adopted on 16 October 2001). The fact that, ultimately, the 2001 Protocol, for reasons of mere hastiness to conclude it, did not regulate the cross-border use of technical equipment after all, does *not* mean such use is *not* to be seen in the context of MLA as a form of *judicial* cooperation in criminal matters.

This is all the more confirmed by the 1990 Convention Implementing the Schengen Agreement (CISA) (Article 39.1)[13] and the so called 2006 Swedish Framework Decision[14] (Articles 1.5 and 1.6), which constitute the official EU framework for MS' horizontal police/law enforcement information exchange cooperation.

Both Article 39.1 CISA and Articles 1.5 and 1.6 Swedish Framework Decision exclude information obtained by means of coercive measures from the scope of law enforcement cooperation, except – in the case of the Swedish Framework Decision – where it concerns information *previously* obtained by means of coercive measures, leaving no scope for real-time or near real-time sharing of such information [underlining and italics added]:

> CISA | Chapter 1. Police cooperation | Article 39
>
> 1. The Contracting Parties undertake to ensure that their police authorities shall, in compliance with national law and within the scope of their powers, assist each other for the purposes of preventing and detecting criminal offences, in so far as national law does not stipulate that the request has to be made and channelled via the judicial authorities and provided that the request or the implementation thereof does not involve the application of *measures of constraint* by the requested Contracting Party. Where the requested police authorities do not have the power to deal with a request, they shall forward it to the competent authorities.
>
> Swedish Framework Decision | Article 1. Objective and scope
>
> 5. This Framework Decision does not impose any obligation to obtain any information or intelligence by means of coercive measures, defined in accordance with national law, in the Member State receiving the request for information or intelligence.
> 6. Member States shall, where permitted by and in accordance with their national law, provide information or intelligence *previously* obtained by means of coercive measures.

Moreover, both instruments explicitly require *judicial* cooperation-based authorisation to use information exchanged at law enforcement level in case of intended use as evidence before a judicial authority [underlining and italics added]:

---

[12] See a.o.: COUNCIL, 8331/98 CRIMORG 72 PECOS 65, 19 May 1998, 11.

[13] Replaced by Article 12 of the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, with the provisions of the said Framework Decision, in as far as Article 39 (1) relates to exchange of information and intelligence for the purpose of conducting criminal investigations or criminal intelligence operations as provided for by the said Framework Decision.

[14] Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

CISA | Chapter 1. Police cooperation | Article 39

2. Written information provided by the requested Contracting Party under paragraph 1 may not be used by the requesting Contracting Party as evidence of the offence charged other than with the consent of the competent judicial authorities of the requested Contracting Party.

Swedish Framework Decision | Article 1. Objective and scope

4. This Framework Decision does not impose any obligation on the part of the Member States to provide information and intelligence to be used as evidence before a judicial authority nor does it give any right to use such information or intelligence for that purpose. Where a Member State has obtained information or intelligence in accordance with this Framework Decision, and wishes to use it as evidence before a judicial authority, it has to obtain consent of the Member State that provided the information or intelligence, where necessary under the national law of the Member State that provided the information or intelligence, through the use of instruments regarding *judicial* cooperation in force between the Member States. Such consent is not required where the requested Member State has already given its consent for the use of information or intelligence as evidence at the time of transmittal of the information or intelligence.

Linking in with the above historical analysis, there is merit in recapping that the WPMA had examined whether the use of technical devices was permitted in the various MS (also in cases other than controlled deliveries) and whether the MS were able to cooperate successfully in this respect.[15] This revealed that there was (is) no problem *in so far the use of the technical equipment was (is) permitted by national law – which was (still is) actually by no means the case for all EU MS with regard to the instalment of bugging or tracking equipment or beacons* – to request the installation of certain devices in another MS, on the basis of the applicable MLA instruments. *Under the same conditions*, it was (is) also possible to ask whether, if a vehicle or person was (is) to reach the territory of the requested MS, devices which were (are) already installed could (can) be replaced by, or exchanged for equipment installed *in application of the internal law of the requested MS*.[16]

Likely, the position of the WPMA had to be seen also against the background of the then developments in the UN, in the context of the pending negotiations on the UN Transnational Organised Crime (UNTOC) Convention. In particular, it had become clear that the future UNTOC Convention would include an obligation in principle for the parties, by analogy with Art. 11.1 of the Convention against illicit traffic in narcotic drugs and psychotropic substances, and inspired by a draft text drawn up by the United States,[17] *in so far as this is harmonious with their internal law, and in accordance with fundamental human rights*, to take all possible measures to allow *electronic surveillance* to be carried out, as well as undercover operations.[18]

Article 20. Special investigative techniques

1. *If permitted by the basic principles of its domestic legal system*, each State Party shall, *within its possibilities and under the conditions prescribed by its domestic law*, take the necessary measures to allow for the appropriate use of controlled delivery and, where it deems appropriate, for the use of other special investigative techniques, such as *electronic* or other *forms of surveillance* and undercover operations, by its competent

[15] COUNCIL, 5816/97 JUSTPEN 9, 13 February 1997, 5-7.
[16] COUNCIL, 6556/97 JUSTPEN 18, 11 March 1997, 4-5.
[17] Containing that parties should adopt effective measures to work out regulations in the matter of electronic surveillance, *undercover*-operations and controlled delivery, in order to gather evidence against persons involved in offences punishable according to the Treaty, and to take judicial steps against them (Art. 9.1(f), *Draft Convention for the Suppression of Trans-national Organized Crime*).
[18] *Outline of Options for Contents of the United Nations Convention against Organized Transnational Crime*, no. 15.1.

authorities in its territory for the purpose of effectively combating organized crime.
2. For the purpose of investigating the offences covered by this Convention, States Parties are *encouraged to conclude, when necessary, appropriate bilateral or multilateral agreements or arrangements for using such special investigative techniques in the context of cooperation at the international level*. Such agreements or arrangements shall be concluded and implemented in full compliance with the principle of sovereign equality of States and shall be carried out strictly in accordance with the terms of those agreements or arrangements.

It was (is) clear therefore that, as regards the *cross-border use of technical equipment (transmitters, beacons, cameras, microphones …)*, e.g. for the interception of private communications in vehicles, monitoring vehicles or objects or for the observation of persons, there is a complete legal vacuum at the level of EU or international law. No EU or international rules have been drawn up to provide an answer (let alone a satisfactory or clear one) to the question whether a neighbouring State can or should authorise the (continued) use of this equipment, and under what conditions.[19]

Hence, reference needs to be made entirely to participating states' domestic laws – if any – i.e. the laws of *both* the requesting/issuing state and the requested/executing state.

Consequently, in addition to the procedural safeguards already in place, and in line with the principle of privacy by design, the ECB recommends Europol to adapt ETS' design by requiring:

- **the so called data owner, i.e. the MS (or TP) that has placed a beacon for tracking on its territory and/or onto another State's territory to ascertain/certify on a case-by-case basis that such tracking is in accordance with its domestic law and the necessity and proportionality conditions embedded therein, including in terms of the offence range or threshold for which tracking is allowed, and**

- **any recipient MS (or TP) to ascertain/certify on a case-by-case basis that geo-location tracking and therefore access through ETS to (foreign) geo-location tracking data is in accordance with its domestic law and the necessity and proportionality conditions embedded therein, including in terms of the offence range or threshold for which tracking is allowed.**

  This will allow national authorities to minimise the risks of unlawful cross-border exchange of geo-location data when making use of ETS. Compliance with the latter condition cannot be guaranteed by the current data owner principle, as underlying the ETS system. If law enforcement authorities of the other MS (or TP) may easily access (near) real time tracking data through ETS *without having to expressly ascertain/certify on a case-by-case basis* that geo-location tracking would be permitted and proportionate according to their own law and that consequently, access through ETS to (foreign) geo-location tracking data (resulting from a cross-border or foreign geo-location tracking measure) would be permitted and proportionate according to their own law, there is no guarantee whatsoever that fundamental rights, including the right to data protection, are effectively respected according to the laws of all MS (or TP) concerned, which, in the absence of an EU (or international) level framework, is the default backbone for procedural and fundamental rights compliance.

b. No legal basis for blanket inclusion of "blue force" tracking data in the EAS

As far as ETS' secondary purpose is concerned, i.e. the further processing of geo-location data for purposes of criminal analysis (strategic/thematic and operational) by Europol, it is recalled that the

[19] As also noticed by the German delegation (COUNCIL, 6416/96 JUSTPEN 47, 10 April 1996, 8-9).

possible sharing of ETS data with the Europol Analysis System (EAS) for purposes of *operational* analyses (in the sense of Article 18(2)(c) ER) requires compliance with the applicable rules of Annex II.B ER, as referred to in Article 18.5 ER ("Categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in paragraph 2 are listed in Annex II").

Hence, it must be assessed to which extent ETS location data, i.e. data on persons' *movements*, or on the *places* they have *frequented*, in the sense of paragraph 2 (f), under (ii) and (iii), of Annex II.B ER, may be included in the EAS for the purpose of operational analysis projects. For so called "red force" operations ("suspects, associates or potential future criminals") such assessment is positive. However, for so called "blue force" operations ("victims, witnesses and covert police officers"), the collection and processing of data types listed under paragraph 2 of Annex II.B is in principle not possible. For covert police officers (as the 3rd category of persons whose tracking is targeted under "blue force" operations), the EDPS opinion already rightly pointed to the lack of legal basis to process data in the EAS. For both victims and witnesses, however, the collection and processing of paragraph 2 data types is also limited to only the data referred to in point (a) to point (c)(iii), therefore excluding data relating to movements or places frequented (which fall under point (f), under (ii) and (iii)). The only exemption for victims and witnesses to store other paragraph 2 data (possibly including data on movements or places frequented) is where this is "necessary, provided there is reason to assume that they are required for the analysis of such persons' role as (potential)victim or witness" (see paragraphs 4 respectively 5 of Annex II.B, last but one sub-paragraph).

It is therefore recalled that any decision to include ETS data in the EAS must be ad hoc, case-by-case, necessity-based and well-motivated – therefore excluding the blanket inclusion in the EAS of "blue force" tracking data of victims or witnesses.

Brussels, 20 February 2019