



Opinion on the Integrated Data Management Guidelines provisionally adopted by the Management Board of Europol (Case 2017-0469)

The EDPS,

Having regard to Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 (the "**Europol Regulation**")¹ and, in particular, Articles 18(7) and 18(6) thereof,

Having regard to Article 43(2)(d) of Europol Regulation,

Has adopted the following Opinion on the guidelines further specifying the procedures for processing of information (hence, the "**Guidelines**")² which were provisionally adopted by the Management Board of Europol on 1 May 2017, pending the Opinion of the EDPS.

1. Introduction and background

The Europol Regulation, applicable in its integrity from 1 May 2017, under **Article 43** establishes that the EPDS "*shall be responsible for monitoring and ensuring the application of the provisions of this Regulation relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by Europol, and for advising Europol and data subjects on all matters concerning the processing of personal data*".

In particular, pursuant to **Article 43(2)(d)**, the EDPS has the duty of "*advising Europol, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before it draws up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data.*"

Article 18(6) of the Europol Regulation provides that "*Europol may temporarily process data for the purpose of determining whether such data are relevant to its tasks and, if so, for which of the purposes referred to in paragraph 2. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data, in particular with respect to access to and use of the data, as well as time limits for the storage and deletion of the data, which may not exceed six months, having due regard to the principles referred to in Article 28.*" (emphasis added)

Article 18(7) of the Europol Regulation states that: "*The Management Board, after consulting the EDPS, shall, as appropriate, adopt guidelines further specifying procedures for the processing of information for the purposes listed in paragraph 2 in accordance with point (q) of Article 11(1)*" (emphasis added).

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 Europol's reference: EDOC #832397v27.

By letter of 4 May 2017 to the EDPS the Chairperson of the Europol Management Board has submitted to the EDPS for his formal Opinion the Guidelines provisionally adopted by the Europol Management Board at its meeting in Malta on 1 May 2017 in accordance with Article 11(1)(q) of the Europol Regulation, pending the delivery of a formal opinion of the EDPS to be issued after 1 May 2017.

By letter of 18 May 2017, the EDPS replied to the aforesaid letter and announced the Chairperson of the Europol Management Board the issuance of this Opinion, so as to allow the final adoption of the Guidelines by the Europol Management Board.

In this context, the EDPS has also been provided with the document “Integrated Data Management Concept. Specification of the envisaged application. The IDMC as per 1 May 2017”³ (hence, “*FAQ document*”). This document, specifying the envisaged IDMC implementation by presenting a list of *Frequently Asked Questions* and the answers to those, has been taken into account as background information for this assessment of the Guidelines.

For his assessment of the Guidelines, the EDPS has also benefited from the staff level visit made on 15 and 16 May 2017 to Europol.

2. Aim of the Guidelines

The Guidelines, more commonly referred to as IDMC (for “Integrated Data Management Concept”) further specify the procedures for data processing by Europol⁴ and aim at ensuring compliance, among others, of Europol’s activities with data protection principles and rules as laid down in the Europol Regulation⁵.

Integrated Data Management refers to the possibility to use information that Europol receives and collects for several processing purposes. The Europol Regulation allows for a processing environment which moves away from specifically described systems towards purposes of processing operations which can be implemented in a technology-neutral manner⁶.

The Guidelines were adopted to implement both Articles 18(6) and 18(7) of the Europol Regulation⁷.

3. Legal analysis and recommendations

As a **preliminary observation**, we note that the Guidelines have been adopted by the Management Board, admittedly provisionally, without having formally consulted the EDPS, which was required under Article 18(7) of the Europol Regulation. The preamble of Guidelines seems to justify the provisional adoption and the *a posteriori* consultation of the EDPS by the fact that the latter was responsible for the supervision of Europol only on 1 May 2017 when the Europol Regulation became applicable. In this respect, we would like to point out that there was no legal obligation for Europol to have guidelines in place on 1 May 2017, as it derives

³ Europol’s reference: EDOC#888329v2.

⁴ Seventh whereas of the Guidelines.

⁵ Second, third and fifth whereas of the Guidelines.

⁶ Second whereas of the Guidelines.

⁷ Eighth whereas of the Guidelines.

from the wording of Article 18(7) of the Europol Regulation ("*The Management Board, after consulting the EDPS, shall, as appropriate, adopt guidelines (...)*").

As regards their content, the EDPS welcomes the attention paid to data protection in the Guidelines. Despite his globally positive appreciation, the EDPS sees significant room for improvement as set out hereunder. This Opinion analyses and highlights the provisions which do not seem to be in conformity with the Europol Regulation and the data protection principles set out in Article 8 of the Charter of Fundamental Rights of the European Union, and makes **recommendations** accordingly.

3.1. Scope of the Guidelines

The Guidelines constitute a *specification* of the procedures for the processing of information by Europol in accordance with the Europol Regulation.

Both the title ("*guidelines further specifying the procedures for processing of information for the European Law Enforcement Agency in accordance with Article 18 of the Europol Regulation*") and the text of the Guidelines (Article 1.1, *Scope*) correctly point out that the aim of the Guidelines is *to specify* the aforesaid procedures.

We recall that both Article 18(6) and (7) refer to the processing of data by Europol *only for the purposes indicated under Article 18(2)*; and that Article 18(1), applicable to all processing of personal data by Europol, lays down that Europol may process information, including personal data, *in so far as necessary for the achievement of the objectives laid down in Article 3*. To 'close the circle', Article 3(1) spells out that "*Europol shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy, as listed in Annex I.*", as well as, pursuant to Article 3(2), the "*related criminal offences*" specified therein.

Against this background, we observe that the Guidelines seem to allow for processing of personal data by Europol more broadly than the scope defined by the aforementioned legal provisions, thus 'opening the door' to a processing of personal data which could go **beyond the scope** indicated both in the title of the Guidelines and under its Article 1(1).

The Guidelines seem to refer to different and unspecified objectives of the processing of personal data by Europol, and to 'possibilities' to process personal data (for Europol as well as for Member States) which are also **unspecified** and **not expressly set out** under the Europol Regulation.

The aforesaid observations by the EDPS are supported by the following examples:

- **Article 19(4)** of the Guidelines refers to "*a procedure for the merging and de-confliction of overlapping data sets*" [our remark: these "data sets" are not specified] to be developed by Europol in consultation with the Member States.

This reference is followed -under the same paragraph 4- by the specification that "*the technical facilitation of data merging shall allow for the retention of all data elements and for the de-coupling when needed without any possible loss of data*". Again, the context to which such "technical facilitation" would apply is unclear.

▪ **Article 19(5)** of the Guidelines states: “*processing by Europol shall take into account the principles of interoperability as well as interconnectivity*” [our remark: interoperability and interconnectivity of and with *unspecified* information systems].

The EDPS understands this as a ‘political statement/commitment’ (in the light of ongoing work at the Council of the European Union), instead of a clarification based on the *currently applicable* legal framework.

The EDPS would like to draw the attention of the Management Board of Europol to the fact that the vague, ‘open’ (so-called ‘future looking’) ‘clauses’ under Article 19(4) and 19(5) of the Guidelines **do not result appropriate to the nature and aim of the Guidelines**, which aim at providing operational guidance (to the “end users”, in particular, to the data analysts), “further specify[ing] the procedures for the processing of information, including personal data, in accordance with Article 18 of the Europol Regulation”⁸. More to the point, such ‘**vague**’ references entail the risk of **blurring the data protection safeguards** contained in the Guidelines which refer to **specific** scenarios for the processing of data by Europol based on (strictly derived from) the legal text of the Europol Regulation as currently in force and applicable⁹.

The specification under **Article 1(2)** of the Guidelines that these “*do not deviate from*” the Europol Regulation is oddly placed (in the Article about ‘the scope’, rather than as ‘stand-alone’ rule) and insufficient to resolve above concerns.

We also note that:

- **Article 3** of the Guidelines stipulates that “*Europol may process personal data in so far as it is necessary for the achievements of its objectives and in accordance with the provisions of the Regulation and this Decision*” (emphasis added).
- Under **Article 4(3)** of the Guidelines “*searches by the Member States may be individual or systematic, in accordance with the provisions of the Regulation and other applicable legislation*” (emphasis added).
- **Article 6(1)** of the Guidelines, the purpose of operational analysis is “*to support criminal investigations and criminal intelligence operations*” (emphasis added) whereas the definition of operational analysis in the Europol Regulation¹⁰ refers to criminal investigations only.
- **Article 15(5)** refers to “*a single search facility*” to be provided by Europol as soon as feasible. This tool is not foreseen under the Europol Regulation.

In this regard, as already mentioned regarding Article 19(4) and (5), the EDPS points out that the aforesaid provisions [Article 3; Article 4(3); Article 6(1); Article 15(5)] also raise concerns on the scope of application of the Guidelines on the processing of data by Europol. We recall that the Guidelines constitute a further specification of the Europol Regulation (the legal instrument on which basis they are issued) and cannot therefore lay down rules applicable beyond its scope of application, ultimately referring, as legal basis for Europol’s processing activities, to the Guidelines themselves (the Management Board Decision adopting the

⁸ Article 1(1) of the Europol Regulation. See also the seventh and tenth whereas of the Guidelines.

⁹ See, in this regard, the considerations made at Section 3.2.a) of this Opinion on the different rules (relevant data protection standards) applicable on one side to strategic and thematic analysis and on the other to operational analysis, based on the specific purposes as defined by the data owners.

¹⁰ Article 2(c) of the Europol Regulation.

Guidelines) under Article 3; or to other (unspecified) applicable legislation which would allow the data processing (individual or systematic searches) described under Article 4(3).

To avoid contradicting their own Article 1, **the Guidelines must be a ‘picture of the present’** which fixes the procedures to be followed by Europol in its operational activities, and must not contain any reference (which would be at least confusing for the end users/operators) to future scenarios (processing operations, tools, *etc.*) not set out under the Europol Regulation as currently in force and applicable¹¹.

1. Therefore, Europol should:

- a. Delete both Articles 19(4) and (5); and moving Article 1(2) into a specific Article (as new Article 2).
- b. Reword Article 3: for example, “*Europol may process personal data in so far as it is necessary for the achievements of its objectives and in accordance with the provisions of the Regulation, for which this Decision lays down operational guidance*”;
- c. Delete Article 4(3), or specify what is meant by “individual and systematic” searches by Member States and how this is linked to Article 18 of the Europol Regulation;
- d. Either remove “*and criminal intelligence operations*” from Article 6(1) or further explain the meaning of this concept and how it falls within the scope of application of Article 2(c) of the Europol Regulation;
- e. Specify the applicable legal basis for the “single search facility” under Article 15(5) and how this basis is linked to Article 18 of the Europol Regulation.

3.2. Implementation of the purpose limitation principle

The Guidelines raise concerns as regards the implementation of the purpose limitation principle, which is expressly laid down in the Europol Regulation under Article 28(1)(b)¹².

We recall that personal data may be processed by Europol only for the purposes indicated under Article 18(2) of the Europol Regulation and that the aim of the Guidelines is to further implement and ‘explain’ the rules provided in the Europol Regulation.

The EDPS considers that **the purpose limitation principle risks being undermined** by the following provisions of the Guidelines.

- a) Differentiation between the purposes of analysis of strategic or thematic nature and of operational analysis

Regrettably, the Guidelines **do not fulfil the aim of further clarifying** the difference between the purposes listed in Article 18(2)(b) and (c) of the Europol Regulation.

¹¹ It has to be noted that the “FAQ document” (No. 7) specifies that “*The Management Board Guidelines can be amended whenever the Management Board sees a need for adjusting it. This process is much faster and flexible than requiring a change in the legal text of the Europol Regulation. As such it contributes to a more flexible maintenance of the set of rules governing the data processing.*”

¹² Personal data shall be “*collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes*”.

Even if this is defined from a practical point of view (and clarified by the “FAQ document”¹³), the Guidelines **do not set out a clear distinction between the concepts of (processing for the purposes of) analysis of "strategic" and "thematic nature", on the one side, and of “operational analysis”, on the other side.**

As an example of the above we point to the broad wording (definition) of an operational analysis project under **Article 6(2)** of the Guidelines as “*a platform in which operational analysis can be conducted to support international criminal investigations and criminal intelligence operations against specific targets. (...)*” (emphasis added). This definition contains wording [“*The scope of such a platform can in particular be a crime area covering one or more types of crime, it can relate to a geographical dimension, or it can focus on particular crime structures, phenomena or incidents (...)*”] which is similar to the one referred to under Article 5(3) of the Guidelines in relation to analysis of a strategic or thematic nature [“*specific areas such as crime phenomena, modi operandi and geographical dimensions, for the target collection of information (...)*”].

A clearer demarcation between the two is crucial as different rules apply to the processing for each purpose. For instance:

- Article 20 of the Europol Regulation differentiates between access by Member States to information provided for the purposes of cross-checking and analyses of a strategic and thematic nature [Article 20(1)], on the one hand; and access (on the basis of a hit/no hit system) to information provided for the purpose of operational analyses [Article 20(2)];
- Article 18(5) of the Europol Regulation makes a *renvoi* to Annex II to the Europol Regulation for the specification of the categories of personal data and of the categories of data subjects whose data may be collected and processed by Europol for *each* purpose listed in Article 18 of the Europol Regulation.

Due to the **key role this differentiation between the two different purposes** of data processing by Europol **plays** for the applicable data protection safeguards, the EDPS considers that the Guidelines should more clearly differentiate between strategic and thematic analysis on one side and operational analyses on the other side.

2. In view of the above, Europol should **further specify** in the Guidelines the differentiation between processing performed for the purposes of analysis of "strategic" or "thematic nature", on the one side, and for “operational analysis”, on the other side.

b) Specification of the purpose(s) by the data provider and/or by Europol in the absence of specification by the data provider

Article 19(1) of the Europol Regulation reads: “*A Member State, a Union body, a third country or an international organisation providing information to Europol shall determine the purpose or purposes for which it is to be processed, as referred to in Article 18. If it has not done so, Europol, in agreement with the provider of the information concerned, shall process the information in order to determine the relevance of such information as well as the purpose or purposes for which it is to be further processed. Europol may process information for a purpose different from that for which information has been provided only if authorised to do so by the provider of the information.*” (emphasis added).

¹³ In particular, FAQ Nos .20-27.

Nonetheless, the Guidelines provide for mere **assumptions** that data submitted for one specific purpose can be processed for other purposes **unless explicitly stated otherwise by the provider** (emphasis added):

- **Article 6(13)(c)** (processing for the purpose of operational analysis) : "(...) *unless explicitly stated otherwise, all contributions to a specific operational analysis project shall be deemed to be submitted for the purpose of operational analysis as well as for the purpose of strategic and thematic analysis*". (emphasis added).

The EDPS recalls the importance of the purpose limitation principle (Article 28(1)(b) the Europol Regulation). Given the broad interpretation of Article 19 of the Europol Regulation enshrined in this provision, the EDPS considers that data providers should be **specifically informed** by Europol of the "by default" dual purposes in due time to decide whether or not they wish to object to the dual purposes. The EDPS recommends implementing measures to ensure specific information at the moment of the transmission of the data to Europol.

- **Article 10(7)**: "*until technical solution is in place to accommodate for a more specified differentiation by the data owner, data submitted to Europol for the purpose of cross-checking [under Article 18(2)(a) of the Europol Regulation] shall be deemed to also have been submitted for strategic and thematic analysis*". (emphasis added).

The EDPS considers that this provision could 'dis-incentivise' the finding of such a technical solution by Europol (as the absence of such a solution actually increases Europol's margin of manoeuvre). The EDPS therefore considers that this provision should be deleted. As a general point, the EDPS also asks Europol to clarify why reference is made to 'data owner' rather than (as under other Articles of the Guidelines) to 'data provider'; how 'data owner' and 'data provider' are defined, in which cases reference should be made to the first or to the other term, and to ensure a consistent use of these terms.

Moreover, the wording of the Guidelines seems rather weak as to the requisite for the Member States to indicate **the operational analysis project** for which they submit data to Europol:

- **Article 6(13)(a)**: "*where possible*" contributions shall indicate for which operational analysis project or projects the information is intended; and
- **Article 10(3)** "*where feasible*", Member States, Union bodies, third countries or international organisations shall indicate at the point of transmission, if submitting for the purpose of operational analysis, which operational analysis project(s) the information shall be submitted to].

Given the importance of the purpose limitation principle (Article 28(1)(b) the Europol Regulation), the EDPS recommends **deleting** the wording "*where possible*" and "*where feasible*". The EDPS recommends replacing it with specific wording closer to the Europol Regulation, that is: "*...the contributor shall indicate for which operational analysis project or projects the information is intended. If it has not done so, Europol, in agreement with the provider of the information concerned, shall process the information for an operational analysis project identified by Europol. In such case, Europol shall request the data owner to grant permission for processing the data for the applicable operational analysis project.*"¹⁴ (emphasis added).

¹⁴ To further explain this recommendation, we add -on the practical side of the implementation of the purpose limitation principle- that the EDPS considers that the provider should be given by Europol actual means for

3. Hence Europol should:
 - a. Add at the end of Article 6(13)(a) of the Guidelines that data providers should be **specifically informed** of the “by default” dual purposes at the moment of the transmission of the data to Europol.
 - b. **Delete** Article 10(7) of the Guidelines;
 - c. **Delete the wording “where possible” and “where feasible”** in Article 6(13)(a) and in Article 10(3) of the Guidelines, and adding the wording: “...*the contributor shall indicate for which operational analysis project or projects the information is intended. If it has not done so, Europol, in agreement with the provider of the information concerned, shall process the information for an operational analysis project identified by Europol. In such case, Europol shall request the data owner to grant permission for processing the data for the applicable operational analysis project.*”
 - e. **Clarify** why reference is made to ‘**data owner**’ rather than (as under other Articles of the Guidelines) to ‘**data provider**’; how ‘data owner’ and ‘data provider’ are defined, in which case/Article of the Guidelines reference should be made to the first or to the other term, and ensure a consistent use of these terms in the Guidelines.

3.3. Processing for the purpose of facilitation of information exchange (Article 7 of the Guidelines)

Article 7 of the Guidelines provides that “*Europol may enable the use of its infrastructure for the exchange of information between Member States, third countries, international organisations, Europol and other Union bodies.*”

According to Article 38(7) of the Europol Regulation, “*Europol shall be responsible for all data processing carried out by it, with the exception of the bilateral exchange of data using Europol’s infrastructure between Member States, Union bodies, third countries and international organizations to which Europol has no access. Such bilateral exchanges shall take place under the responsibility of the entities concerned and in accordance with their law.*” (emphasis added). *Nonetheless, the same Article states at the end that “The security of such exchanges shall be ensured in accordance with Article 32”* (emphasis added). According to Article 32(1) of the Europol Regulation “*Europol shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss or unauthorised disclosure, alteration and access or any other unauthorised form of processing.*”

Europol’s **obligation to ensure security**, which is enshrined in Article 32 of the Europol Regulation, is therefore also applicable to the scenario referred to under Article 7 of the Guidelines and should be reflected therein.

As proper information security can only be achieved by looking at the exchange of information as a whole, it is necessary to protect the information throughout its lifecycle (creation, distribution, destruction, archiving...). This means that information security should not only be ensured by Europol within the remit of its responsibilities but also by Member States, Union bodies, third countries and international organisations working with Europol.

identifying purpose(s), such as *check boxes* in SIENA, with a list of the different purposes, and, in case of operational analysis, of the different Operational Analysis Projects.

4. The EDPS hence recommends adding **specific references** to the need for **information security**, the **responsibilities of all parties** (Europol, Member States, Union bodies, third countries and international organisations) and the **means to enforce security** in Article 7 of the Guidelines.

3.4. Chapter IV of the Guidelines: title, data protection by design, auditing

a) Title of Chapter IV

The reference to ‘Data Protection’ in the title of Chapter IV is misleading since various other provisions of the Guidelines refer to data protection principles and a general reference to data protection requirements is also made in Article 1(2) of the Guidelines (“*This Decision does not deviate from the applicable provisions of the Regulation in any manner and specifically not as regards the data protection requirements and conditions*”).

5. As the Guidelines do not further describe how to implement the data protection safeguards laid down in Chapter VI of the Europol Regulation, the EDPS recommends **replacing the title** of Chapter IV “Data Protection” of the Guidelines with a less misleading one, for instance: “*Data protection by design, auditing of data processing and data review*”.

b) Data protection by design (Article 19 of the Guidelines)

A key item of data protection is the need to secure personal data using a risk-based approach. This means that a thorough analysis of the information security risks needs to be performed to ensure that risks are properly handled¹⁵.

If implemented correctly, **anonymisation/pseudonymisation** (referred to under Article 19(3) of the Guidelines) can be useful in protecting personal data. Unfortunately properly applying techniques for anonymisation/pseudonymisation is difficult to achieve. Due care should be taken when implementing those techniques as failure could mean the occurrence of data breaches.

6. Europol should clearly indicate in Article 19 of the Guidelines that an **independent responsible party** needs to ensure that the **anonymisation/pseudonymisation techniques are appropriate and correctly implemented**.

c) Auditing of data processing (Article 20 of the Guidelines)

As laid out in this article proper **logging of the processing of personal data** is important to ensure that activities can be traced, purposes of processing checked and responsibilities and ownership assigned for each part of the collective delivery process in the context of strategic and thematic and operational analysis. The objectives of logging can only be achieved if **suitable tools for auditing** are designed and implemented. The amount of logs produced in Europol’s environment would otherwise make any auditing impossible. This would help auditors perform their duties in an effective and efficient manner.

¹⁵ See the EDPS’ Guidance on Security Measures for Personal Data Processing Article 22 of Regulation 45/2001. Article 32 of the Europol Regulation is similar to Article 22 of Regulation 45/2001.

7. The EDPS recommends including in Article 20 of the Guidelines a **clear statement that proper auditing tools will be implemented.**

3.5. Other specific recommendations

▪ **Article 6(8)** of the Guidelines deals with further use of data provided for an operational analysis project in the context for another operational analysis project “*where it becomes apparent*” that these personal data “*may be relevant*” for this other project. The Guidelines should expressly provide that the analysis made in this context shall be duly documented.

8. In Article 6(8) of the Guidelines, Europol should indicate that the analysis made to assess the **relevance of personal data collected for an operational analysis project for another operational analysis project shall be duly documented.**

▪ **Article 6(13)(e)** of the Guidelines stipulates that “*if Europol believes, after appraisal, that personal data provided by Member States, Union bodies, third countries and international organisations for an operational analysis project is incorrect, inaccurate, no longer up to date or should not have been transmitted, it shall without undue delay inform the data provider, which shall provide its position on the matter, and take appropriate action*”.

In such situations, there are serious grounds for considering that the personal data provided do not satisfy the necessary data quality requirement. This is a situation which can pose significant risks to the fundamental rights and freedoms of the data subject concerned. Therefore, the EDPS welcomes the precision that Europol shall “take appropriate action”. However, this action should be further specified.

9. The EDPS recommends **further describing such appropriate action vis-à-vis the data provider**, by adding for instance “*including restricting the processing of the personal data deemed incorrect, inaccurate or no longer up to date ensuring that they can no longer be processed with the exception of storage*”.

▪ The **procedure** - foreseen under **Article 6(13)** of the Guidelines¹⁶ - can be considered as a ‘third layer’ of procedure (the first layer being the Europol Regulation itself, on which basis the Guidelines are adopted; the second layer the Guidelines, mandating the development of the procedure in question), which further details **the rules for the transmission and acceptance of information in operational analysis projects**, specifying the aspects covered under letters a. to e.

These letters clearly cover aspects which are **crucial** for the processing of personal data by Europol. We list them hereunder for ease of reference:

- “*a. that contributions, where possible, shall indicate for which operational analysis project or projects the information is intended.*
- b. that contributions shall be in accordance with the categories of personal data and data subjects as specified in the decision opening the operational analysis project.*
- c. that, unless explicitly stated otherwise, all contributions to a specific operational analysis project shall be deemed to be submitted for the purpose of operational analysis as well as for the purpose of strategic and thematic analysis, whilst the access for Member States*

¹⁶ According to Article 6(13) of the Guidelines “*Europol shall develop and implement, in close collaboration with the Management Board and the HENUs, a procedure for the transmission and acceptance of information in operational analyses projects.*”

to that data shall, without prejudice to Article 5(3) of this Decision, follow the regime applicable to data provided for the purpose of operational analysis, i.e. not exceed the possibilities for access under Article 20(2) of the Regulation.

- d. that if Europol rejects the information for the specific operational analysis project that the data provider had indicated, it may request the data provider to submit the information for one or more other processing purposes, or for other operational analysis project(s).*
- e. that if Europol believes, after appraisal, that personal data provided by Member States, Union bodies, third countries and international organisations for an operational analysis project is incorrect, inaccurate, no longer up to date or should not have been transmitted, it shall without undue delay inform the data provider, which shall provide its position on the matter, and take appropriate action.”*

10. Since the requirements under aforesaid letters a. to e. of **paragraph 13 of Article 6** of the Guidelines represent **key aspects** of the operational analysis projects, Europol should **lay down this procedure and have it implemented** at the same date of first implementation of the Guidelines. The EDPS also asks to be **promptly informed** about the aforesaid procedure.

- The EDPS notes that **Article 8(7)** of the Guidelines differentiates between ‘deletion’ and ‘destruction’ (the latter word not being used in the Europol Regulation). The reason is not clear and the wording of Article 8(7) of the Guidelines does not define when or to which cases ‘deletion’ or ‘destruction’ applies.

11. Europol should further **specify the meaning and the implications of the terms ‘deletion’ and ‘destruction’** under Article 8(7) of the Guidelines and when (to which cases) each applies.

3.6. Role of the EDPS

- **Article 6(3)** of the Guidelines states that decisions opening an operational analysis project shall be ‘forwarded’ to the EDPS. Article 6(5) makes use of the same terminology for decisions amending or closing operational analysis projects. In this regard, the Europol Regulation¹⁷ refers instead to the obligation “to inform” the EDPS.

12. The EDPS recommends referring to the **terminology** of Article 18(3)(a) of the **Europol Regulation** in Articles 6(3) and 6(5) of the Guidelines, using the wording “*the EDPS shall be fully informed of (...)*”

- **Article 6(7)** of the Guidelines provides that the EDPS ‘*may address any comment on the opening, closure or amendment of an operational analysis project it deems necessary to Europol as controller of the data processing*’ and that Europol ‘*shall promptly inform the Management Board of any such comments received from the EDPS*’. The EDPS draws the attention of the Management Board of Europol to the obligation for Europol to fully implement the EDPS recommendations¹⁸. The requirement for Europol to provide prompt and complete follow up to the EDPS recommendations should be reflected in the Guidelines.

¹⁷ Article 18(3)(a).

¹⁸ See powers of the EDPS under Article 43(3) of the Europol Regulation.

13. Article 6(7) of the Guidelines should state that Europol shall **implement** without undue delay any **recommendations** made by the EDPS in relation to the opening, closure or amendment of an operational analysis project.

▪ The obligation for Europol to submit a request for prior consultation to the EDPS pursuant to **Article 39 of the Europol Regulation** is not referred to in the Guidelines. The **prior consultation** should allow the EDPS to assess in particular whether new technologies, mechanisms or procedures that Europol intends to use are compliant with data protection principles, taking into account the risks for the fundamental rights and freedoms of data subjects. Hence, any new “methods and techniques” (as referred to for instance in Articles 5(1) and 6(1) of the Guidelines) could be submitted to the EDPS for prior consultation.

14. The Guidelines should mention the **requirement for prior consultation** under Article 39 of the Europol Regulation, for example in Article 19 on data protection by design.

▪ **Article 25(6)** of the Europol Regulation provides that “the Management Board of Europol may, in agreement with the EDPS, authorise for a period not exceeding one year, which shall be renewable, a set of transfers in accordance with points (a) to (e) of paragraph 5”. The requirement for Europol to obtain the **prior authorisation** of the EDPS in case of application of Article 25(6) of the Europol Regulation (i.e. set of transfers of personal data to third countries or international organizations) should also be reflected in the Guidelines.

▪ Article **25(7)** of the Europol Regulation provides that “the Executive Director shall as soon as possible inform the Management Board and the EDPS of the cases in which paragraph 5 [of Article 27] has been applied”. The requirement for Europol to **inform** the EDPS in case of application of Article 25(5) of the Europol Regulation (i.e. transfers of personal data to third countries or international organization on a case by case basis) should be reflected in the Guidelines.

15. The Guidelines should mention the **requirements for Europol to inform or ask the prior authorisation** of the EDPS according, respectively, to Article 25(6) and (7) of the Europol Regulation.

▪ Article **30(6)** of the Europol Regulation provides that “every year Europol shall provide to the EDPS a statistical overview of all personal data as referred to in paragraph 2 [¹⁹] which it has processed”. The requirement for Europol to **inform** the EDPS in case of application of Article 30(6) of the Europol Regulation should be reflected in the Guidelines.

Article **31(3)** of the Europol Regulation states that “if personal data as referred to in Article 30(1) and (2) [²⁰] are stored for a period exceeding five years”, the EDPS shall be informed accordingly”. The requirement for Europol to **inform** the EDPS in case of application of Article 30(6) of the Europol Regulation should also be reflected in the Guidelines.

¹⁹ Article 30(2): personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data or data concerning a person's health or sex life.

²⁰ Article 30(1): personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences, or in respect of persons under the age of 18.

Article 30(2): personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data or data concerning a person's health or sex life.

16. The Guidelines should mention the **requirements for Europol to inform the EDPS** according, respectively, to Article 30(6) and 31(3) of the Europol Regulation.

4. Conclusion

The EDPS invites Europol Management Board to inform the EDPS about the implementation of the recommendations made above within six months from the date of receipt of this Opinion. These recommendations should be taken into the utmost account for the revised -and final- Decision of Europol Management Board adopting the Guidelines in accordance with Articles 18(7) and 18(6) of the Europol Regulation.

Done in Brussels,

Giovanni BUTTARELLI