MANAGEMENT BOARD DECISION 69/2021

of 21 December 2021

adopting the rules on processing operational personal data by the Agency

THE MANAGEMENT BOARD

Having regard to the European Border and Coast Guard Regulation[1] ('the Regulation'), in particular Articles 86(2) and 100(2) thereof,

Whereas:

(1) Article 86(1) of the Regulation requires the Agency to apply Regulation (EU) 2018/1725[2] ('the Data Protection Regulation') when processing personal data.

(2) Pursuant to Article 90(1) of the Regulation, where the Agency, in the performance of its tasks under Article 10(1)(q) of the Regulation, processes personal data which it has collected while monitoring migratory flows, carrying out risk analyses or in the course of operations for the purpose of identifying suspects of cross-border crime, it shall process such personal data in accordance with Chapter IX of the Data Protection Regulation. Personal data processed for that purpose, including licence plate numbers, vehicle identification numbers, telephone numbers and ship or aircraft identification numbers which are linked to such persons, shall relate to natural persons whom the competent authorities of the Member States, Europol, Eurojust, or the Agency have reasonable grounds to suspect are involved in cross-border crime. Such personal data may include personal data of victims or witnesses where those personal data supplement the personal data of suspects processed by the Agency in accordance with this Article.

(3) Pursuant to Article 90(2) of the Regulation, operational data processed for the purpose of Article 90(1) of the Regulation should be exchanged only with Europol or Eurojust where they are strictly necessary for the performance of their respective mandates and in accordance with Article 68 of the Regulation, or with the competent law enforcement authorities of the Member States where they are strictly necessary for those authorities for the purposes of preventing, detecting, investigating or prosecuting serious cross-border crime.

(4) Pursuant to Article 91(3) of the Regulation, operational personal data processed for the purposes of Article 90 shall be deleted as soon as the purpose for which they have been collected, namely the identification of a suspect of cross-border crime has been achieved by the Agency. The Agency shall continuously review the necessity of storing such data, in particular the personal data of victims and witnesses. In any case, the Agency shall review the necessity of storing such data no later than three months after the start of initial processing of such data, and every six months thereafter. The Agency shall decide on the continued storage of personal data, in particular the personal data of victims and

[1] *Regulation (EU) 2019/1896 of 13 November 2019 on the European Border and Coast Guard (OJ L 295, 14.11.2019, p. 1).*

[2] *Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 23.10.2018, p. 39).*

witnesses, until the following review, only if such storage is still necessary for the performance of the Agency's tasks under Article 90.

(5) In accordance with Article 86(2) of the Regulation, the Management Board shall adopt internal rules on the application of the Data Protection Regulation by the Agency.

(6) The Agency, as part of the European Border and Coast Guard, together with the border management authorities of the Member States, is responsible for implementing European Integrated Border Management. For the performance of its task the Agency processes personal data that fall under the general part of the Data Protection Regulation. However, the personal data collected while monitoring migratory flows, in the course of operations or carrying out risk analysis may be repurposed to serve the task of the Agency as referred to in Article 10(1)(q) of the Regulation related to the cooperation with Europol and Eurojust and provide support to Member States in particular in prevention, detection, investigation, prosecution of cross-border crime, such as migrant smuggling, trafficking in human beings and terrorism, including the identification of suspects of those crimes. While the Agency carries out these activities it should apply Chapter IX of the Data Protection Regulation.

(7) The Agency in performance of its tasks as referred to in Article 10(1)(q) of the Regulation may conduct activities which entail the processing of personal data of minors, in particular related to cross-border crime. Sufficient procedural safeguards should be introduced to ensure the protection of fundamental rights of children to the fullest possible extent including the requirement of justified reasons of such a processing of personal data for the purposes of Article 90 of the Regulation.

(8) The identification of suspects may require occasionally processing of special categories of personal data, for example, when the witnesses and victims of cross-border crime may provide the Agency information or description of suspects or associates, which may include racial or ethnic origin, health, sexual orientation, or especially regarding terrorism concerning political opinions, religious or philosophical beliefs. Equally those special categories of personal data can be absolutely necessary to link an individual with a committed or attempted cross-border crime or terrorism. This collection may provide vitally important cues for establishing the identity of suspects of cross-border crime, for example, by referring to use of specific medical devices, or a particular health condition of an individual, or linking an individual to a particular religious or ethnic group. Sexual orientation of an individual may be necessary to identify victims and witnesses of trafficking in human beings, or link them with a potential suspect or associate, especially if such a crime is committed or attempted for the purpose of sexual exploitation.

(9) Genetic and biometric data, including photographs, where available, provide necessary elements to establish the identity of an individual.

(10) Implementing measures for processing operational personal data as referred to in Article 90 of the Regulation should specify *inter alia* the procedures regarding the data, provide criteria for reasonable grounds to suspect that a person is involved in cross-border crime, and detail roles and responsibilities of persons and entities involved in processing of operational personal data. As Article 90 of the Regulation sets out only certain aspects required by Chapter IX of the Data Protection Regulation, these implementing measures should specify, in a pragmatic way, the implementation of the Data Protection Regulation for that Chapter when the Agency performs its tasks under Article 10(1)(q) of the Regulation concerning activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Treaty on the Functioning of the European Union. While doing so, the Agency should fully apply the principles related to processing operational personal data in accordance with Article 71(1) of the Data Protection Regulation.

HAS DECIDED AS FOLLOWS:

Article 1
Object

The rules on processing operational personal data by the Agency (OPD Rules), as set out in the Annex to this Decision, are hereby adopted.

Article 2
Entry into force

This decision enters into force on the day following the date of its adoption.

Done by written procedure, 21 December 2021.

For the Management Board

[e-signed]

Marko Gašperlin
Chairperson

ANNEX: Rules on processing operational personal data by the Agency (OPD Rules)

ANNEX

Rules on processing operational personal data by the Agency (OPD Rules)

CHAPTER I

General provisions

Article 1

Subject and scope

1. This Annex lays down the Agency's rules on the application of Chapter IX of Regulation (EU) 2018/1725[3] ('the Data Protection Regulation') regarding the processing of operational personal data, in accordance with Article 90 of the European Border and Coast Guard Regulation[4] ('the Regulation'), including specific internal rules on data retention of operational personal data in accordance with Article 91(3) of the Regulation.

2. This Annex defines specific data protection rules for the processing of operational personal data where the Agency, in the performance of its tasks under Article 10(1)(q) of the Regulation, processes personal data which it has collected while monitoring migratory flows, carrying out risk analyses or in the course of operations for the purpose of identifying suspects of cross-border crime. These rules need to be applied without prejudice to the general data protection rules applicable to the Agency.

Article 2

Definitions

For the purpose of this Annex, the following definitions apply:

(a) 'personal data' means personal data as defined in point (1) of Article 3 of the Data Protection Regulation;

(b) 'operational personal data' takes the meaning of point (2) of Article 3 of the Data Protection Regulation where the Agency processes personal data in the performance of its task referred to in Article 10(1)(q) of the Regulation;

(c) 'processing' means processing as defined in point (3) of Article 3 of the Data Protection Regulation;

(d) 'data controller' means controller as defined in point (8) of Article 3 of the Data Protection Regulation;

(e) 'cross-border crime' means cross-border crime as defined in point (12) of Article 2 of the Regulation; This definition includes terrorism in line with Article 10(1)(q) of the Regulation;

(f) 'suspect' means a natural person who the competent authorities of the Member State(s)[5], Europol, Eurojust, or the Agency have reasonable grounds to suspect is involved in cross-border crime;

(g) 'associate' means a natural person who the competent authorities of the Member State(s), Europol, Eurojust or the Agency have reasonable grounds to suspect is cooperating with a suspect in the commission of a cross-border crime, in particular by aiding and abetting or inciting an offence;

---

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 38).

[4] Regulation (EU) 2019/1896 of 13 November 2019 on the European Border and Coast Guard (OJ L 295, 14.11.2019, p. 1).

[5] For the purpose of this Annex, the term 'Member States' includes also the States participating in the relevant development of the Schengen acquis within the meaning of the Treaty on the Functioning of the European Union and its Protocol (No 19) on the Schengen acquis integrated into the framework of the European Union.

(h) ‘victim’ means a natural person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a cross-border crime, or with regard to whom certain facts give reason to believe that they could be the victims of such a cross-border crime;

(i) ‘witness’ means a natural person who provides information on a cross-border crime;

(j) ‘data subject’ means an identified or identifiable natural person who is either a suspect, associate, victim or witness, and whose personal data are being processed;

(k) ‘deletion’ means the irreversible deletion of operational personal data;

(l) ‘anonymisation’ means the process of irreversible removal of personal identifiers and any other information in such a manner that the data subject is not or no longer identifiable;

(m) ‘data collection plan’ means a document that establishes the data sets that can be collected, the agreed providers of information including the Agency’s own staff, the competent law enforcement authorities of Member States, Europol or Eurojust that will supply and receive the data, the format in which operational personal data can be supplied, the types of data subjects, and the desired or exceptional means of exchange of operational personal data, and, if necessary, the specific modalities agreed in relation to answering requests;

(n) ‘competent law enforcement authority of the Member States’ means any national authority of the Member States listed in the data collection plan, which according to the respective national legislation is competent for preventing, detecting, investigating or prosecuting cross-border crime.

CHAPTER II
Roles and responsibilities

Article 3
Data protection responsibilities of the Agency

1. The Agency, as the controller, is represented by the Executive Director. The Executive Director may delegate the implementation of appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Chapter IX of the Data Protection Regulation and this Annex.

2. While processing operational personal data the data controller is responsible for ensuring that:

   (a) Technical and organisational measures are implemented to ensure compliance with the Regulation and this Annex, taking into account the state of the art, the cost of implementation as well as the risks for the rights and freedoms of the data subjects;

   (b) The Data Protection Officer (‘DPO’) shall be involved, in a properly and timely manner, in all issues related to data protection;

   (c) A data protection impact assessment is conducted prior to processing where significant modifications are introduced in the systems; or 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.

3. In accordance with Article 15(2) of the Regulation, the Agency is responsible for developing, deploying and operating an information system that is able to exchange operational personal data. The Agency shall ensure that the competent law enforcement authorities of the Member States are provided with access to systems in Article 11(4) of this Annex for transmitting operational personal data to the Agency.

   The Agency shall implement in the systems under its responsibility the necessary technical security controls referred to in Article 91 of the Data Protection Regulation in order to prevent unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration of personal data, as well as all other unlawful forms of processing. By adopting such security measures, the Agency shall in particular:

(a) Ensure that all actions by the Agency's IT administrators to operational personal data are logged and that safeguards are set-up to ensure the integrity of the logs;

(b) Adopt measures concerning audit logs and access through a decision of the Director of Financial, Digital and Security Division.

4. The competent law enforcement authorities of the Member States shall designate a point of contact for the exercise of data protection responsibilities. The point of contact will be included in the data collection plan.

Article 4
Joint controllership

1. Where the Agency and the competent law enforcement authorities of the Member States[6], Europol or Eurojust are joint controllers in accordance with Article 86 of the Data Protection Regulation, the data collection plan shall cover the necessary elements of the arrangement referred to therein.

2. For the purpose of paragraph 1 of this Article the following shall apply:

(a) Where operational personal data has not been collected by the Agency and pending the successful validation process, the Agency shall be responsible for the data security of the information system on which operational personal data is transmitted, in particular for the confidentiality, availability and the integrity of the operational personal data whilst that data is transmitted. If the system is not administrated by the Agency, the Agency shall seek assurance from the owner that it complies with the highest standards;

(b) Where operational personal data has not been collected by the Agency and pending the verification process referred to in Article 12 of this Annex is completed, the content of the uploaded operational personal data remains the joint responsibility of the Agency and the competent law enforcement authorities of the Member State, if applicable. After that verification process, the Agency is solely responsible for the operational personal data until it is further transmitted or deleted;

(c) The Agency shall ensure that information related to the processing of operational personal data and the exercise of data subject rights is clearly communicated on its website.

CHAPTER III
Processing of operational personal data

Article 5
Purpose for processing operational personal data

The Agency may process operational personal data only for the purpose of identifying suspects of cross-border crime while performing its task under Article 10(1)(q) of the Regulation.

Article 6
Source and scope of operational personal data

1. Operational personal data may be collected while the Agency performs the following activities:

(a) Monitoring migratory flows;

(b) Carrying out risk analysis;

(c) In the course of operations.

[6] *For example in situations within the scope of Article 88 of the Regulation.*

2. The Agency may process the operational personal data of the following categories of data subjects:

   (a) Persons involved in cross-border crime, namely suspects and associates;

   (b) Victims;

   (c) Witnesses.

   Personal data of the data subjects referred to in points (b) and (c) may only be processed as supplement to data processed under point (a).

3. The sources of operational personal data and the Agency's activities for collecting operational personal data are further defined in Articles 7, 8Article 9 of this Annex. For the purposes of this Annex, that data may not be processed further until the conditions in Article 10 and other conditions set out in this Annex are met.

4. For the purpose of this Annex, the Executive Director may decide, in consultation with the Member State concerned where relevant for the processing referred to in Article 88 of the Regulation, to further regulate in operational plan or in data collection plan whether dedicated Agency's staff, including Category 1 of the European Border and Coast Guard standing corps and specialised staff in the Agency's Headquarters, seconded national experts (SNEs) and Categories 2-4 of the European Border and Coast Guard standing corps ('the Agency's own staff') are allowed to process operational personal data in accordance with this Annex.

Article 7

Collection of operational personal data while monitoring migratory flows

1. While monitoring migratory flows, the Agency may use the EUROSUR framework as a collection point of information in accordance with Article 89 of the Regulation. Any further processing of such information that entails the processing of operational personal data shall be processed under this Annex.

2. Where the Agency activates the EUROSUR Fusion Services on behalf of a Member State, any processing of personal data other than ship and aircraft identification numbers shall fall under the scope of Article 90 of the Regulation and be marked under the ownership of the Member State which requested the EUROSUR Fusion Services.

3. Where the Agency uses the EUROSUR Fusion Services on its own initiative, it shall do so in accordance with Article 89 of the Regulation, under the ownership of the Agency.

Article 8

Collection of operational personal data in the course of operations

The Agency may collect operational personal data in the course of operations while conducting its tasks, in particular while performing actions at the external borders under an operational plan, with the purpose defined in Article 5 of this Annex, including but not limited to:

(a) When performing border checks of persons including their means of transportation and the objects in their possession;

(b) When performing border surveillance at land, air and sea including detection, identification, tracking and interception of illegal border crossing, the prevention, detection and fight against cross-border crime and checks on the identity of unknown persons in the surveillance areas;

(c) When performing migration management support activities including interviewing or debriefing of migrants or examining travel and other documents, and/or any objects in their possession;

(d) When executing the EUROSUR Fusion Services in the course of operations in accordance with Article 7 of this Annex in order to collect information on the external borders and the pre-frontier area;

(e) When performing specific activities such as media monitoring through open sources as a part of an operational activity;

(f) When conducting any other processing activities in the course of operations as agreed within the operational plan.

Article 9

Collection of operational personal data while carrying out risk analysis

1. The Agency may collect operational personal data including in the context of activities mentioned under Articles 7 and 8 of this Annex and may process operational personal data while carrying out risk analysis for the purpose of identifying suspects of cross-border crime.

2. While carrying out risk analysis in cases for which Article 88 of the Regulation applies, this Annex shall take precedence if due to that analysis there are reasonable grounds to suspect that persons who crossed the border without authorisation are involved in cross-border crime.

3. Operational personal data may be collected while carrying out risk analysis based on personal data, including but not limited to, personal data collected from open sources, social media monitoring and commercially available databases, the EUROSUR Fusion Services or within cooperation with competent law enforcement authorities of the Member States, Europol and/or Eurojust, if due to that analysis there are reasonable grounds to suspect that a natural person is involved in cross-border crime.

Article 10

Criteria for assessing the involvement of a person in cross-border crime

1. When processing operational personal data the controller shall:

   (a) Assess whether there are reasonable grounds to suspect that the natural person concerned is involved in cross-border crime; and

   (b) Indicate the cross-border crime each person is suspected of.

   If the criteria of reasonable grounds to suspect is not met, processing of operational personal data is not possible under this Annex.

2. If the Agency's own staff performs the assessment in paragraph 1 of this Article, the following points are to be considered:

   (a) Evidence, facts or information indicating the possible involvement of the data subject in cross-border crime; or

   (b) Information collected from at least two different sources which can be corroborated to support the suspicion. The cooperation by the Agency in this regard with Europol, Eurojust and Member States is encouraged.

3. The assessment of the reasonable grounds to suspect, either by the Agency's own staff, or the Member State competent authorities, Europol or Eurojust when received by the Agency, is subject to the verification process defined in Article 12 of this Annex.

4. Where information related to a suspect or associate of a cross-border crime is accepted by the Agency from any of the data providers mentioned in paragraph 3 of this Article, a sufficient justification related to the assessment on reasonable grounds shall be given whether those are based on evidence, facts or information, or on a personal assessment of the data provider. This includes the compliance with Article

7 of the Law Enforcement Directive[7] when the data provider is a competent law enforcement authority of a Member State.

Article 11

General conditions and channels for exchanging operational personal data

1. A data collection plan shall be drawn up by the Agency prior to the processing of operational personal data. In the course of operations as referred to in Article 8 of this Annex, that data collection plan shall be part of the operational plan in line with Article 38(3)(d) of the Regulation.

2. The template of the data collection plan may be established by a decision of the Executive Director.

3. Without prejudice to this Annex, further conditions under which operational personal data are exchanged may be set out in specific provisions of:

   (a) Working arrangements between the Agency, Europol and Eurojust, respectively, and in accordance with Article 68 of the Regulation; or

   (b) Executive Director's decisions as regards the roles and responsibilities of the Agency's own staff.

4. When the Agency exchanges operational personal data with the competent law enforcement authorities of the Member States and with Europol and Eurojust it shall use SIENA[8] and/or JORA[9]. Other channels may be established by the Executive Director, subject to the conditions set out in particular in Articles 85, 89, 90 and 91 of the Data Protection Regulation. The competent law enforcement authorities of the Member States may submit their preference for the channel for exchanging operational personal data in the data collection plan.

5. Where a competent law enforcement authority of a Member State, Europol or Eurojust transmits personal data to the Agency it shall indicate for what purpose that data needs to be processed in accordance with Article 87(1) of the Regulation. The channels referred to in paragraph 4 of this Article shall ensure that such a purpose is always determined, in accordance with Article 87(2) of the Regulation. The Agency may repurpose the initially provided data under the condition that it performs a written compatibility assessment seeking written approval prior to the repurposing of the data from the provider, following the applicable European Data Protection Supervisor ('EDPS') guidelines.

6. In the event operational personal data are sent to the Agency via a channel other than those referred to in paragraph 4 of this Article, the Agency deletes the received personal data.

7. Access to the information exchange systems and applications referred to in paragraph 4 of this Article shall be granted only to duly authorised staff of the Agency, the competent law enforcement authorities of the Member States, Europol, and Eurojust in accordance with the Operational Plans, working arrangements, or other procedures agreed by the Agency with its partners.

8. The Agency exchanges personal data directly with the Member States' competent law enforcement authorities.

9. When exchanging operational personal data with the Agency, the competent law enforcement authorities of the Member States, Europol or Eurojust, or the Agency's own staff shall indicate the reliability of the information, and the purposes for which the Agency may use the information via handling codes as described in Article 23 of this Annex.

---

[7] 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).

[8] Secure Information Exchange Network Application.

[9] Joint Operations Reporting Application.

10. The channels for exchange of operational personal data referred to in this Article shall ensure that the conditions set out in Article 91 of the Data Protection Regulation are always met.

Article 12

Verification and acceptance process

1. The Agency shall verify and accept operational personal data transmitted by Member States, Europol, Eurojust and the Agency's own staff ('verification process').

2. During the verification process, operational personal data shall be separately stored from other data sets.

3. The verification process involves the following steps:

   (a) Confirmation of the source of transmission. Operational personal data are accepted only when transmitted by:

      (i) Member States and, in the course of operations, their appointed officers in accordance with the data collection plan;

      (ii) The Agency's own staff, in accordance with the data collection plan;

      (iii) Europol or Eurojust, in accordance with working arrangements agreed between the Agency and these agencies and its own respective mandates.

   (b) Channels for transmission: operational personal data are accepted only when they are transmitted via the information system channels described in Article 11(4) of this Annex;

   (c) Personal data processed is operational personal data as defined in this Annex and it is relevant, accurate and not excessive in relation to the purpose in Article 5 of this Annex;

   (d) Data quality: the Agency only accepts operational personal data collected in a way consistent with the provisions of Articles Article *14* Article 15 of this Annex;

   (e) Data management: the Agency accepts operational personal data only when marked with handling codes and reliability codes;

   (f) Lawfulness: the Agency accepts operational personal data related to persons' involvement in cross-border crime only when reasonable grounds to suspect are provided by the competent law enforcement authorities of the Member States, Europol, Eurojust or by the Agency's own staff.

4. Operational personal data items that clearly do not comply with the criteria foreseen in paragraph 3 of this Article are deemed to have failed the verification process and will be deleted from the systems for processing operational personal data.

5. Where it is not possible to fully complete the verification process, or any other component of the verification process fails to be met, the Agency shall reject the operational personal data and contact the data provider in paragraph 3(a) of this Article to request for additional information to support the verification process. This provision of information is documented by the Agency's staff.

6. In case referred to in paragraph 5 of this Article, the data provider shall provide additional information in 7 calendar days when requested. Upon receipt of additional information by the Agency, the verification process will continue. After 7 calendar days, if no additional material has been disclosed by the data provider, the operational personal data will fail the verification process and will be deleted.

7. Verification process in paragraph 3 of this Article should not take longer than 7 business days.

8. Once operational personal data which has been collected in the course of operations has been verified, the Agency shall inform the host Member State, as well as further transmission when applicable.

Article 13

Access to operational personal data by the Agency

1. Access to operational personal data in the Agency is limited to the minimum necessary for the purpose in Article 5 of this Annex.

2. Operational personal data shall only be accessible to the Agency's duly authorised staff who will process personal data to the extent necessary for the fulfilment of their duties. Roles and responsibilities for access may be further defined by the Executive Director on the Access Management Policy to operational personal data systems.

3. The Agency's own staff collecting and transmitting operational personal data to operational personal data systems of the Agency or transmitting such data to the competent law enforcement authorities of the Member States, Europol or Eurojust, have read/write/delete access, or combination of those, based on their roles and responsibilities defined by the Executive Director on the Access Management Policy, to the extent necessary for the performance of their tasks.

4. A list of users provided with access to operational personal data processing systems is made available to the Agency's DPO.

5. The DPO shall have access to all operational personal data processed by the Agency.

Article 14

Data model

1. Operational personal data must be collected and processed based on a data model that is compatible with most current version of the Universal Message Format[10].

2. Whenever possible, the Agency's data structure comprises the following entities:

   (a) Person;

   (b) Organisation;

   (c) Location;

   (d) Item;

   (e) Connections;

   (f) Event;

   (g) Means of communication;

   (h) Means of transportation;

   (i) Financial means;

   (j) Identification documents;

   (k) Photo.

Article 15

Types of operational personal data including special categories

1. Whenever possible, operational personal data must include categories consistent with the data model of the Universal Message Format. A non-exhaustive list of data categories is set out in points (a) to (r)

[10] *Universal Message Format (UMF) is an agreement that ensures standardised data exchange between law enforcement authorities of the Member States across national borders, and with Union agencies.*

below, however, the data collection plan may further specify which of the categories below are collected:

(a) Name(s) of the data subject;

(b) Nick name or alias;

(c) Nationality/-ies;

(d) Gender;

(e) Age;

(f) Description (physical characteristics which are not likely to change e.g. height, scars, body deformations, tattoos etc.);

(g) Membership of organised crime group;

(h) Registered business (name, address, coordinates, contact details);

(i) Personal address and/or coordinates;

(j) Safe house address and/or coordinates;

(k) Means of communication (telephone, social media, IP addresses, etc.);

(l) Means of transportation (vehicle registration, vessel and aircraft identification numbers, license plate, chassis number, flight tickets, etc.);

(m) Weapon(s);

(n) Illegal goods;

(o) Photograph(s)[11];

(p) Criminal offence event (description of criminal offence);

(q) Non-criminal offence event (meeting or communication or any other event linked to the criminal offences that fall under the scope of this Annex);

(r) Specific location linked to a person, event or crime (crime scene).

2. The Agency may process special categories related to operational personal data only if strictly necessary to achieve the purpose of Article 5 of this Annex. For the purpose of this Annex special categories of operational personal data are:

(a) Racial or ethnic origin;

(b) Political opinions, religious or philosophical beliefs;

(c) Genetic data and/or biometric data such as DNA, fingerprints or photographs for the purpose of uniquely identifying a natural person;

(d) Health;

(e) Sexual orientation.

Article 16

Processing of operational personal data within the Agency for the purpose of identifying suspects of cross-border crime

The Agency for the purpose of identifying suspects of cross-border crime may further:

[11] *Unless it falls under the specific category of point (c) of paragraph 2 of this Article.*

(a) Collate and assess operational personal data collected from different sources as described in Articles 7, 8 and 9 of this Annex;

(b) Cross-check operational personal data against the Agency's databases and open sources[12] and prepare assessments aiming at identifying suspects of cross-border crime. However, such action exclusively based on special categories of operational personal data as referred to in Article 15(2) of this Annex is forbidden;

(c) Prepare data and information packages containing the results of the cross-checks and assessments to be disseminated to the competent law enforcement authorities of the Member States, Europol and Eurojust.

Article 17

Identification of a suspect by the Agency

1. For the purpose of identifying a potential suspect, the Agency considers that a person is identified when:

   (a) the Agency has established the following data categories of the potential suspect:

      (i) name and surname;
      (ii) place and date of birth;
      (iii) names of parents.

   (b) the data evaluation code concerning this potential suspect has been marked as 'A1' in accordance with the 4x4 evaluation system referred to in Article 24 of this Annex.

2. The suspect referred to in paragraph 1 of this Article is identified as a suspect of a cross-border crime, when the Agency has reasonable grounds to establish a correlation between that person and his or her involvement in a cross-border crime.

Article 18

The Agency's transfer of operational personal data to the competent law enforcement authorities of the Member States

1. The Agency transfers operational personal data to the competent law enforcement authorities of the Member States only where this is strictly necessary for those authorities for the purposes of preventing, detecting, investigating or prosecuting cross-border crime.

2. The Agency transfers this data only via the information exchange systems and applications referred to in Article 11 of this Annex.

3. The Agency decides to which Member States it transfers operational personal data based on their:

   (a) *Need to know* that will be established on a case-by-case basis and will require to fulfil at least one of the following criteria:

      (i) direct or indirect links between the activity of a suspect or a related entity and the Member State;
      (ii) likelihood that the national and/or public security of the Member State is affected by the criminal activities of a suspect or the organised crime group to which the suspect belongs;
      (iii) submission of a justified written request for information by a Member State, Europol or Eurojust to the Agency, referring to Article 90(2) of the Regulation.

[12] *In line with Management Board Decision 50/2021 of 21 September 2021 on Common Integrated Risk Analysis Model.*

(b) *Right to know* that will be established on the basis of the handling codes used by the entity (i.e. data owner) that had provided the operational personal data to the Agency.

4. In cases where the Agency identifies Member States that have the *need to know* as regards specific operational personal data, but it cannot share them due to restrictions imposed via the handling codes, the Agency may request the data owner to lift the restriction. The Agency will share the operational personal data with the Member State that has the *need to know* only if the data owner will allow it.

Article 19

The Agency's transfer of operational personal data to Europol and Eurojust

1. Transmissions of personal data to Europol and Eurojust shall:

   (a) Be performed only if the data are necessary for use in accordance with their respective mandates;

   (b) Be subject to specific working arrangements as stated in the second subparagraph of Article 68(5) of the Regulation;

   (c) Follow the *need to know* and *right to know* principles as stated in Article 18(3) of this Annex;

   (d) Respect the principles of necessity and proportionality, the Agency will only process personal data that are adequate and in their extent proportionate in relation to the purpose defined in Article 5 of this Annex.

   The specific working arrangements referred to in point (b) above will provide further details on the exchange of operational personal data between the Agency and Europol and Eurojust.

2. Both the Agency and the recipient agency/agencies bear the responsibility for the legitimacy of the transfer.

3. The Agency is required to:

   (a) Verify the competence and mandate of the recipient agency/agencies;

   (b) Verify the necessity of the transfer of personal data;

   (c) Request more information from the recipient agency/agencies if doubts arise as to the necessity of the transfer of personal data.

4. Onward transmission of operational personal data by Europol and Eurojust shall be regulated by the specific working arrangements referred to in point (b) of paragraph 1 of this Article respectively, and shall be performed in full compliance with fundamental rights including relevant data protection safeguards.

Article 20

Processing of operational personal data of natural persons under the age of 18

1. When the processing of operational personal data which falls within the category of Article 6(2)(a) of this Annex relates to persons under 18 years old, specific considerations are taken:

   (a) If the data subject is a minor below 15 years old, his or her personal data shall never be processed as a suspect or associate of cross-border crime;

   (b) If the data subject is a minor between 15 and 18 years old, the providing Member State, Europol or Eurojust will accompany the transmission of his or her data with detailed information as for the reasons why this minor is a suspect of cross-border crime. If the operational personal data is collected by the Agency's staff, the above requirement for justification also applies.

2. When the processing of operational personal data which falls within the categories of Article 6(2)(b) and (c) of this Annex relates to a minor below 15 years old, his or her personal data shall never be

processed as a victim or witness of a cross-border crime, unless the processing of personal data of a victim is exceptionally necessary to identify a suspect of cross-border crime.

3. Personal data of victims exceptionally processed pursuant to paragraph 2 of this Article shall in any circumstances be deleted the latest after three years following its collection.

CHAPTER IV
Data retention

Article 21

Storage, review and deletion

1. The Agency shall store the data in a way that allows establishing the ownership of the data. This includes that the stored data shall be linked to the provider of the data i.e. a competent law enforcement authority of a Member State, Europol, Eurojust or the Agency where the data collected is the result of an activity of the Agency's staff.

2. After verification and successful acceptance performed by the Agency's staff, operational personal data will be stored until its purpose is achieved, or where identification of suspect of cross-border crime has not been successful, until the data expiry. The stored data sets are subject to periodical reviews on necessity by the Agency as mentioned below.

3. In accordance with Article 91(3) of the Regulation, data shall be deleted as soon as the purpose for which they had been collected have been achieved. Where identification of suspect of cross-border crime has not been successful, the Agency's business units review the necessity of storing such data no later than three months after the start of initial processing of such data, and every six months thereafter.

4. Without prejudice to paragraph 3 of this Article, the Agency shall delete or anonymise the personal data of a potential suspect not identified as a suspect of a cross-border crime according to Article 17 of this Annex, if no additional relevant information related to the potential suspect has been collected in the last 24 months since his or her personal data were verified pursuant to Article 12 of this Annex.

5. The Agency's business units shall decide on the continued storage of personal data, in particular the personal data of victims and witnesses, until the following review, only if such storage is still necessary for the performance of the Agency's tasks under Article 90 of the Regulation. That assessment must take into account that new data may render existing data on victims and witnesses no longer necessary.

6. However, if after three years no new data has been received from an individual, the data expires and shall be deleted.

7. In case anonymisation of operational personal data cannot be ensured, the Agency shall delete the operational personal data.

8. Deletion or anonymisation of expired data applies to:

   (a) Operational personal data in its original form as collected from the Agency's own staff, the Member States, Europol, and Eurojust;

   (b) Any other files or documents within the Agency that contain expired data;

   (c) Any on or offsite backups containing expired data;

   (d) Any system used to exchange operational personal data.

9. An automated system will flag data for review and create an entry for compliance checks. Deletion or anonymisation of the personal data stored in the Agency's systems shall be as automated as possible. The Executive Director may decide the details of these processes.

10. Regular checks shall be performed to ensure that no expired personal data remain on the Agency's operational systems.

11. Anonymised data relating to thereafter unidentifiable persons may persist indefinitely in the Agency.

Article 22

Logging

1. The Agency shall keep logs for any of the processing operations within the information exchange systems and applications used for identification of the suspects and exchanging operational personal data and administrated by the Agency in accordance with Article 88 of the Data Protection Regulation. The Agency shall also keep logs of activities of IT administrators as referred to in Article 3(3)(a) of this Annex and of any exchange by using insufficient channels as referred to in Article 11(6) of this Annex, for the purposes of data protection compliance monitoring. The logs may be centralised. The specific information that needs to be logged shall be developed by means of a decision of the Executive Director.

2. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the operational personal data, for criminal proceedings and where necessary for internal investigations conducted by competent authorities of the Member States. Such logs shall be deleted after three years, unless they are required for the internal investigations of the Agency. In these cases, the logs will be immediately deleted once the actions required for internal control are finalised.

3. The DPO has dedicated access to the logs at all times for the assurance of compliance with data protection obligations.

4. The DPO shall make the logs available to the EDPS on request.

Article 23

Handling codes

For the purposes of this Annex, the Member States, Europol and Eurojust shall indicate to the Agency the purposes for which the transmitted operational personal data may be used. The Agency's own staff shall also follow the handling codes.

(a) **Handling Code H0 - This information can only be used for the prevention, detection, investigation or prosecution of cross-border crime, in accordance with Article 90 of the Regulation.**

The Handling Code H0 allows the recipient of the information, to share and use that information as evidence in judicial proceedings, without any prior approval from the owner of the information.

(b) **Handling Code H1 - This information shall not to be used in judicial proceedings without prior consent of the owner of the information.**

The Handling Code H1 regulates the use of the information for police investigation only and its use in judicial proceedings is prohibited unless prior approval from the owner of the information is obtained. The consequence of applying this handling code is that the received information can be further disseminated without any additional authorisation from the owner of the information. Nevertheless, a formal and specific authorisation must be requested to the owner of the information if it is to be used as evidence in judicial proceedings.

(c) **Handling Code H2 – This information shall not to be disseminated without prior consent of the owner of the information.**

Whenever the data provider identifies the need to further protect the source of information, the Handling Code H2 can be applied in order further information sharing, unless prior written consent to its dissemination is obtained from the owner of the information.

(d) **Handling Code H3 - This information includes other restrictions, rights or aims of the transmission.**

The Handling Code H3 can be assigned to describe all other possible restrictions, permissions or purposes of transmission. In case this handling code is applied, additional caveats may be included to specify the nature of restriction/permission/purpose.

Article 24

Evaluation codes

When providing operational personal data to the Agency, the Member States, Europol, and Eurojust shall indicate the accuracy of the information and the reliability of sources from where it was collected by using the 4x4 system, as follows:

(a) Source codes:

'A' - where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be reliable in all instances;

'B' - source from whom information received has in most instances proved to be reliable;

'C' - source from whom information received has in most instances proved to be unreliable;

'D/X' - the reliability of the source cannot be assessed.

(b) Information codes:

'1' - information whose accuracy is not in doubt;

'2' - information known personally to the source but not known personally to the official passing it on;

'3' - information not known personally to the source but corroborated by other information already recorded;

'4' - information which is not known personally to the source and cannot be corroborated.

CHAPTER V
Data subject rights

Article 25

Data subject rights

1. Article 12 of Management Board Decision 56/2021[13] shall apply *mutatis mutandis* to the rights of data subjects, subject to paragraphs 2 to 7 of this Article.

2. Individuals will be informed by the Agency on the processing of operational personal data via a privacy statement available in a dedicated page of the Agency's website. This privacy statement is made in compliance with Article 79 of the Data Protection Regulation.

3. This privacy statement shall contain all provisions referred to in Articles 79(1) and 79(2) of the Data Protection Regulation.

4. Additionally, this Annex and any other policy or procedure of the Agency regulating the exercise of data subject rights shall be made available on the dedicated page of the Agency's website referred to in paragraph 1 of this Article.

[13] *Management Board Decision 56/2021 of 15 October 2021 adopting implementing rules on the application of Regulation (EU) 2018/1725 concerning the tasks, duties and powers of the Data Protection Officer as well as rules concerning Designated Controllers in Frontex.*

5. The Agency has the obligation to respond to all requests, except when found manifestly excessive and unfounded. In such a case, the Agency following a consultation with its DPO shall justify and document the reasons for rejection.

6. All requests shall be responded in writing and its receipt shall be documented by the Agency.

7. The Agency shall ask for proof of identity from the requestor before the request is being processed. In case of doubts in relation to the identity of the data subject, the Agency may request assistance from the competent Member State law enforcement authority for his or her identification.

Article 26

Procedural aspects for restrictions of data subject rights

1. Restrictions applied to the data subject rights will be exercised on a case-by-case basis. They shall be documented and kept on a register available to the EDPS upon request. The register of documented restrictions is kept by the DPO.

2. Prior to responding to the request from a data subject referred to in this Article, the Agency shall coordinate and closely consult its response with the data provider, i.e. competent law enforcement authority(ies) of the Member State(s), Europol and/or Eurojust, if applicable, to ensure:

   (a) That there is no obstruction of official or legal inquiries, investigations or procedures;

   (b) That there is no prejudicing of the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

   (c) The protection of the Member States' public security;

   (d) The protection of the Member States' national security;

   (e) The protection of the rights and freedoms of others, such as victims and witnesses.

3. On the cases referred to in this Article, the Agency shall document the responses of the data provider.