FRONTEX

Warsaw, [date]
Reg. No
Ref: <Division>/<Unit>/<Initials of the responsible(4)>/<Registration number>/<Year>
[please insert marking]

[for to change the entire format into new template for MB decisions, mail sent by MBS]

Draft Frontex Management Board Decision

Frontex Implementing Measures for processing operational personal data

Done at Warsaw
00/00/2012

.....
Signature
Name Surname
Position

Formatted: English (United Kingdom)
Formatted: English (United Kingdom)

Frontex - European Border and Coast Guard Agency
www.frontex.europa.eu | Pl. Europejski 6, 00-844 Warsaw, Poland | Tel. +48 22 205 95 00 | Fax +48 22 205 95 01

CHAPTER I

General provisions

Article 1

Subject and scope

1. This decision lays down the specific measures regarding the processing of personal data ~~exchanged by Frontex with the law enforcement authorities of the Member States, Europol or Eurojust in~~ pursuant to Articles 87(1), points (d) and (e), and 90 of the Regulation (EU) 2019/1896 (hereinafter: the Regulation).

Article 2

Definitions

1. For the purpose of this Decision the definitions included in the Data Protection Regulation and in the Regulation apply.

2. For the purpose of this Decision:

   (a) 'Data Controllers' are jointly the Executive Director and Member States;

   (b) 'Operational personal data' means all ~~data~~ personal data processed by Frontex related to persons (data subjects) suspected on reasonable grounds by the competent authorities of Member States, Europol, Eurojust, or the Agency of involvement in cross border crime or terrorism, as well as personal data of victims or witnesses where those personal data supplement the personal data of suspects processed by the Agency.

   (c) [here goes the definition on suspects, per above reference already introduces the concepts of suspect, victim and witness - to be discussed whether we include contacts as per the wide definition of "reasonable grounds of involvement in CBC or terrorism- as involvement may have different degrees - contact/associates - to put as an example companies used to smuggle migrants via land borders - drivers may be a suspect, to be determined whether managerial levels of the company is involved - may not be a suspect per se, but surely a person of interest]

   (d)

   (e) 'Victim' is a person whose fundamental rights, physical integrity, or financial means were affected as a result of cross-border crime or terrorism. - UN definition Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power adopted by General Assembly resolution 40/34 of 29 November 1985: "Victims" means persons who, individually or collectively, have suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that are in violation of criminal laws operative within Member States, including those laws proscribing criminal abuse of power.

   (f) 'Witness' is a person who has the legal status of witness in a judiciary proceeding involving cross-border criminal activities or terrorism, or who expressed his willingness to give testimony regarding such illegal activities and the persons involved.

   ~~(b)~~(g)

   ~~(c)~~(h) 'Deletion" is to be understood as hard deletion by removal of personal identifiers of the data subjects as a result of the review process on the necessity of storage of that personal data~~Anonymised data' is data where data subjects cannotare not likely to be identified, having regard to any methods reasonably likely to be used by the data controller or any other person to identify the data subject. Where data has been anonymised to such an extent that it iswould not be possible to identify an individual in the anonymised data even with the aid of the original data, the anonymised data is not to be considered as personal data~~.

   ~~(d) 'Victim' is a person whose fundamental rights, physical integrity, or financial means were affected as a result of cross-border crime or terrorism.~~

   ~~(e) 'Witness' is a person who has the legal status of witness in a judiciary proceeding involving cross-border criminal activities or terrorism, or who expressed his willingness to give testimony regarding such illegal activities and the persons involved.~~

Commented pe - to just talk about OPD which is the scope - purposes are perhaps to be placed on another article

Commented May want to include that in case of conflict of interpretation, the def from the DPR prevails?

Commented : Not jointly - this needs to be in article about when to have JC or not - decision making: FX data controller - ED or DSAM - RAU (?)

Commented Restricts it to criinal prosecution, which is not within FX mandate - we need to broaden up the concept: a person who sees an event to be considered as a criminal offence committed along or within the proximity of the external border - question: if we restrict this, we may blow up the secondary movements, thus taking away THB within EU

Commented : Cross check with DPR recitals and consider if I need to add pseudoanonymisation
2. also, why to include this in OPD IR?

Formatted: Indent: Left: 1.27 cm, Hanging: 0.63 cm

Commented mandate - we need to broaden up the concept: a person who sees an event to be considered as a criminal offence committed along or within the proximity of the external border - question: if we restrict this, we may blow up the secondary movements, thus taking away THB within EU

~~(f)~~(i) 'Data Collection Plan' ~~is a document, either in the form or an annex to a Joint Operation Plan or as a standalone document used for a Pilot Project, that defines the data required within an Operation or a Pilot Project. The Data Collection plan~~ establishes the data sets that can be collected, the sources of information, the law enforcement bodies that will supply the data, the format how personal data can be supplied, and the desired or exceptional means of transmission of persona data.

~~(g)~~(j) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

~~(h)~~(k) 'Law enforcement authorities of the Member States' means any national authority of the Member States that, according to their national law, are competent for preventing, detecting, investigating or prosecuting cross-border crime ~~and~~ or terrorism.

CHAPTER II
Processing of operational personal data

Article 3

Purposes for processing operational personal data

1. Frontex processes operational personal data:

   (a) in the performance of its task under point (q) of Article 10(1) of the Regulation, for the purpose of facilitating the exchange of information with the law enforcement authorities of the Member States, Europol or Eurojust, in accordance with point (d), paragraph (1) of Article 87 and Article 90 of the Regulation.

   (b) for the purpose of risk analysis, in accordance with Article 29 and point (e), and paragraph (1) of Article 87 of the Regulation.

   ~~(b)~~(2) [BRAINSTORMING not definitive] purpose is identification of suspects - which entails assessment of the data provided for example to distinguish the data category of the DS and further transmission of accurate data - the non-personal data once deletion enters into force can and will be used for risk analysis purposes and threat assessments of CBC - to discuss different interpretations with the EDPS - linked to the development of the concept of risk analysis with PD, both OPD and 88

Article 4

Source and scope of operational personal data

1. The providers of operational personal data to Frontex are the Frontex own staff, including SNE's TAs and the Standing Corps (hereinafter: Frontex' own staff), the law enforcement authorities of the Member States, Europol, and Eurojust.

2. Frontex collects operational personal data while performing the following activities:

   (a) monitoring migratory flows,

   (b) risk analysis, and

   (c) operations for the purpose of identifying persons suspected for involvement in cross-border criminal activities and terrorism.

3. For the purpose mentioned under~~at~~ point 2 of this article, Frontex may process the personal data of the following categories of data subjects:

   (a) Persons suspected on reasonable grounds for involvement in cross-border criminal activities and terrorism, by the competent authorities of the Member States, Europol, Eurojust or Frontex.

   (b) Victims and witnesses where these personal data complement the personal data of the suspects mentioned at point 3(a) of this article.

4. The conditions under which operational personal data are transmitted to Frontex are set out in specific provisions of the:
   (a) Working Arrangements signed with Europol and Eurojust,

Commented ?

Commented The list of authorized LE authorities to receive FX data should be part of the DCP? Or put it in the Annex to the JOs? Or shall we say its up to the NFPOC to distribute it? Because Article 90 refers directly to LE agencies, no NFPOC involvement

Commented Art 90 further defines the purpose, which is the identification of suspects - that should be considered as possible additional suspects beyond the exchange

Commented : ETIAS is out of scope of OPD even if there's a hit with the watchlist...

Commented [?

Formatted: Font color: Text 2

Formatted

Commented What are these activities? BC this is a copy of Art 90, but I still wonder what OPD do we collect while monitoring migration flows not being EUROSUR - Vessels of Interest/ Identification of vessels?

Commented : Same here - unless the output

Commented : We should consider what is meant here by operations, wheter in the sense of JO or operational activities that any can activate without much regard of the Reg requirements

(b) Status Agreements, Operational Plan and Analysis Project Plan if applicable, signed with the Member States.

The Operational Plan and the Analysis Project Plan should contain a Data Collection Plan covering the types of data to be collected, sources and transmission channels.

5. Frontex does not process personal data that was obtained in violation of ~~the law e.g. the~~ EU Charter of Fundamental Rights, the Data Protection Regulation, the Frontex Regulation or any national data protection rules and regulations.

Article 5a

Collection of operational personal data while performing risk analysis

1. Pursuant to points (a) and (c), paragraph (1) of Article 88 of the Regulation, Frontex processes the personal data of persons who cross the external borders without authorisation, including, licence plate numbers, vehicle identification numbers, telephone data or ship and aircraft identification numbers which are linked to these persons, and which are necessary for analysing routes and methods used for illegal immigration.

2. Frontex will process the personal data mentioned in paragraph (1) of this article when collected by the Member States, by members of the teams, by Frontex own staff or by EASO and transmitted to the Agency in the context of joint operations return operations, return interventions, pilot projects, rapid border interventions, and migration management support team.

3. In order to perform its task stipulated by the paragraph (1) of article 90 of the regulation, Frontex will process the personal data mentioned in paragraphs (1) and (2) as follows:

   (a) Cross-check the collected personal data against the databases of the Member States and the relevant Union agencies, in accordance with point (c), paragraph (1) of Article 87 and point (a), paragraph (2) of Article 88 of the Regulation, with the purpose of identifying persons suspected for involvement is cross-border criminal activities and terrorism. These activities will be further detailed in the operational plans, Working Arrangements, or Status Agreements signed between Frontex and its partners, mentioned by point (c), paragraph (1) of Article 86 of the Regulation, respectively.

   (b) Perform risk analysis, in accordance with Article 29 and point (c), paragraph (2) of Article 88 of the Regulation.

4. The Frontex activities mentioned by point (3) of this Article will be implemented for the purpose of identifying persons suspected for involvement in cross-border criminal activities and terrorism, in accordance with paragraph (1) of Article 90 of the Regulation, without prejudice to other activities that Frontex may implemented, in accordance with points (a) and (c), paragraph (2) of Article 87 of the regulation.

Article 5b

Collection of operational personal data while monitoring migratory flow via Eurosur

1. Pursuant to Article 19 of the Regulation, Eurosur shall be used for border checks at authorised border crossing points and for external land, sea and air border surveillance, including the monitoring, detection, identification, tracking, prevention and interception of unauthorised border crossings for the purpose of detecting, preventing and combating illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants.

2. While monitoring migratory flows, in accordance with Article 90 of the Regulation, Frontex shall collect operational personal data:

   (a) provided in the Eurosur national, European and specific situational pictures, in accordance with Articles 24 and 89 of the Regulation.

   (b) via Eurosur Fusion Services, in accordance with Article 28 of the Regulation.

Commented [?

Commented : Aren't we complicating things? I remember from the discussions with the MSs this was controversial - we need to think how do we demonstrate proportionality and exersice accountability from it. Would it be the DCP enough, plus the annex to the OPLAN on DP requirements? We started considering all extra documents mainly because we were looking into the 2016 Reg that had nothing on JOs

Commented :

Commented Art 91

Article 6

Criteria for assessing the involvement of a person in cross-border criminal activities or terrorism

1. Before transferring ~~to Frontex~~ personal data of persons who are suspected of involvement in cross-border criminal activities or terrorism to Frontex, the Frontex' ~~-~~ own staff, the Member States, Europol, and Eurojust have the obligation to:
   (a) assess whether their suspicion is based on reasonable grounds.
   (b) transmit to Frontex only the personal data of suspects where this criterion is met and indicate the crime(s) each ~~of them~~ person~~s~~ is suspected for.

2. When Frontex ~~own staff who~~ collects personal data of suspects of cross-border crime or terrorism while performing their tasks in joint operations, pilot projects, and migration management teams activities, the Frontex staff will transmit the data to Frontex via the National Contact Points or Intelligence O~~o~~fficers of the host Member State that will implement the activities described in paragraph (1) of this article.

3. When collecting personal data of suspects of cross-border crime or terrorism in other situations stipulated by Article 90(1) of the Regulation, but not mentioned in paragraph (2) of this article, the Frontex staff shall transfer these data directly to Frontex. In this situations, the Frontex staff collecting the data will assess the grounds for suspicion, not a Member State as in paragraph 2 of this article.

4. In the situations mentioned in paragraph 3 of this article, the Frontex staff has reasonable grounds to suspect one person of involvement in cross-border crime or terrorism when the staff has:
   (a) evidence or facts ~~indicate~~ clearly indicating the involvement of the data subject in cross-border crime and terrorism. ~~e it.~~
   (b) information collected from at least two different official sources can be corroborated to support the suspicion. ~~indicate it.~~
   (c) ???

Article 7

Channels for exchanging personal data

1. Frontex shall exchange personal data with its partners mentioned at points (c) and (d), of Article 87(1) of the Regulation, only via the:
   (a) Frontex Joint Operations Reporting Application (JORA),
   (b) European Border Surveillance System (EUROSUR)
   (c) Communication Network mentioned by Article 14 of the Regulation,
   (d) information exchange systems and applications developed and managed by Frontex, in accordance with Article 15 of the Regulation,
   (e) Secure Information Exchange Network Application (SIENA),
   (f) Other secure information exchange systems or applications agreed with its partners, and stipulated in the operational plans, Status Agreements, or Working arrangements, where applicable.

2. Frontex and its partners mentioned at points at points (c) and (d), of Article 87(1) of the Regulation may use other channels for exchanging personal data, only under exceptional circumstances, when the information exchange systems and applications mentioned at paragraph (1) of this article are not available, and the parties exchanging the information reach a prior agreement and the channel is secure.

3. In situations when the Frontex staff needs to exchange on spot personal data related to persons suspected of involvement in cross-border criminal activities or terrorism with staff of the national authorities of the Member States, Europol, or Eurojust, the Frontex staff should:

   (a) In case of collection: report the collected information and personal data to Frontex via the dedicated information exchange systems and applications mentioned by paragraph (1) and (2) of this article indicating by the handling codes the source and reliability of the information, and~~, via the handling codes,~~ the purposes for which the information may be used further.

   (b) In case of transmission: share the personal data and record the transmission in register that will be created at Frontex for this purpose, where it will indicate: the source of the data, the date and purpose of the transmission, the name and institution of the recipient. This register should be accessible to and regularly verified by the Frontex Controller and DPO.

4. In the event operational personal data are sent to Frontex via a channel other than those mentioned in paragraphs (1), (2), and (3) of this article, Frontex ~~proceeds to~~ deletes the received personal data, and the transmission will be logged for monitoring and evaluation purposes.

5. Access to the information exchange systems and applications described in paragraph (1) of this article is granted only to duly authorized staff of Frontex, ~~national~~law enforcement authorities of the Member States, Europol, and Eurojust~~uts~~, and in accordance with the Operational Plans, Working Arrangements, or other procedures agreed by Frontex with its partners.

6. Frontex exchanges personal data with the Member States via the National Contact Points established in accordance with Article 13 of the Regulation or the Intelligence Officers nominated by the Member States.

7. The National Contact Points and the Intelligence Officer are responsible for disseminating the personal data transmitted by Frontex to the law enforcement~~competent~~ authorities of their Member States.

8. When transmitting operational personal data to Frontex, the National Contact Points or the Intelligence Officer shall indicate the crime for which the person is suspected, the reliability of the information, and the purposes for which Frontex may use the information via handling codes.

9. When, in the context of a joint operation or a pilot project, Frontex own staff collects and transmits operational personal data to Frontex, these data must be transmitted only via the National Contact Point or the Intelligence Officers of the host Member State. In this case, the National Contact Point or the Intelligence Officers need to confirm or reject whether the suspicion of involvement in cross-border criminal activities or terrorism is based on reasonable grounds. This decision needs to be made within a specific timeframe, agreed in the Operational Plan. In the absence of action by the Member State Intelligence Officer within the specific timeframe, the suspicion is confirmed via positive silence.

Article 8

Verification and acceptance process

1. Frontex reserves the right to accept or reject operational personal data transmitted by Member States, Europol, Eurojust, and via Frontex staff, ~~including the Standing Corps~~ and the decision~~s~~ made by Frontex in this regard is justified~~are underpinned~~ by the~~a~~ verification process.

2. During the verification process, operational personal data are stored in a restricted database~~location~~ separated~~distinct~~ from others analytical systems.

3. The verification process involves the following stages:

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

      (i) National Contact Points as stipulated by Article 13 of the Regulation or Intelligence Officers appointed by Member States for data collected by Member States, Standing Corps, and Frontex own staff, in accordance with the Data Collection Plan.

(ii) Europol or Eurojust via SIENA, in accordance with Working Arrangements agreed between Frontex and these agencies.

(b) Channels for transmission: Operational personal data are accepted only when they are transmitted via the ~~Frontex~~ information system channels described in the points (1) and (2) of Article ~~7~~6 of this Decision.

(c) Scope: Operational personal data as ~~can only be processed when falling under the typology of data subjects as~~ described in Article 90 (1) of the Frontex Regulation ~~and as defined in Article 4 of this Decision.~~

(d) Data quality: Frontex only accepts operational personal data collected in a way consistent with the principles referred to in Articles 10, 11, 16 and 17 of this Decision.

(e) Data Management: Frontex accepts operational personal data only when marked with handling codes and reliability codes.

(f) Legality: Frontex accepts operational personal data related to suspects of involvement in cross-border crime and terrorism only when a suspicion on reasonable grounds is indicated or confirmed by the law enforcement~~competent~~ authorities of the Member States or by Frontex' staff.

(g) 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 validation process and will be deleted from the systems for processing operational personal data.

(h) Where it is not possible to fully complete the verification process, Frontex may reject the report containing personal data and contact the data provider to request for additional information to support ~~material that may further inform~~ the verification process. This provision of information is documented by Frontex staff.

(i) If a transmission fails any component of the verification process, Frontex contacts the data provider and informs about the failure and the reason for the Decision. This provision of information is documented by Frontex staff.

(j) In the circumstances referred to in the previous paragraphs, the data provider will have 7 days to supply additional information~~material~~.

(k) Upon receipt of additional information the verification process will ~~be~~ continue~~re-launched~~.

(l) After 7 days if no additional material has been disclosed by the data provider, the operational personal data will fail the authentication process and will be deleted from the temporary location described in paragraph 3 of this article.

Article 9

Access to personal data

1. Access to personal data in Frontex is limited to the minimum necessary for the purposes listed in Article 3 of this Decision.

2. Personal data are only accessible to the Data Controller and duly authorized Frontex staff who will process personal data on behalf of the Data Controller. Roles and responsibilities for access are further defined on the Access Management Policy to operational personal data systems.

3. For the purpose of analysis and transmission of personal data to authorities of relevant Member States or the Union Agencies stipulated in the points (c) and (d), paragraph (1), Article 87 of the Regulation, Frontex nominated analysts have read/write/delete access to operational personal data.

4. Frontex own staff nominated to collect and transmit operational personal data to Frontex have read/write /delete access to the personal data collected by themselves and, read access to other personal data processed by the Agency to the extent necessary for the performance of their tasks.

5. A list of users provided with access to operational personal data processing systems is made available to the Frontex Data Protection Officer on request by the Data Controller.

6. The Frontex Data Protection Officer has access to all operational personal data contained in the systems used for transmission and exchange of operational personal data as well as to the systems used for risk analysis.

Article 10

Analysis Projects

1. Frontex may establish Analysis Projects to facilitate the analysis of operational personal data, in order to perform its tasks stipulated by Article 10(1)(q) and 90(2) of the Regulation.

2. The Analysis Projects are coordinated by the Frontex Risk Analysis Unit and they may have different focuses, such as specific cross-border crimes or terrorism, geographical areas of interest, emerging modi operandi, risks to the internal security of the EU/SAC area or its external borders, joint operations or pilot projects.

3. Analysis Projects are opened and closed with the approval of the Frontex Executive Director, based on the proposals of the relevant Frontex units or the requests from the Member States, Europol, or Eurojust, and the recommendations of the Head of the Frontex Risk Analysis Unit and the Frontex Data Protection Officer.

4. The duration and scope of the Analysis Projects will be established based on the purpose~~.~~ to be served~~they need to serve~~, in accordance with Article 10(1)(q) and 90(2) of the Regulation. The duration and the scope of the Analysis Project may be reduced or extended only with the approval of the Frontex Executive Director.

5. For each Analysis Project, the Frontex Risk Analysis Unit will prepare in cooperation with its partners for the project an Analysis Project Plan that includes Data Collection Plan. Both plans need to be reviewed by the Frontex Data Protection Officer and approved by the Frontex Executive Director together with request for initiating the Analysis Project.

6. The Frontex Risk Analysis Unit in cooperation with the Data Protection O~~o~~fficer, other relevant Frontex units, and external partners shall evaluate the Analysis Projects after their closure and periodically during their lifecycle, to ensure their efficacy and effectiveness in achieving the planned objectives, as well as compliance with data protection rules and Article 91 of the Regulation.

7. In the framework of Analytical Projects, Frontex Risk Analysis Unit should prepare intelligence and analytical outputs containing operational personal data only for the purposes established by Article 90(2) of the Regulation.

8. Whenever possible, Frontex shall coordinate its activities implemented in the framework of Analysis Projects with the law enforcement authorities of the Member States, Europol, or Eurojust and this may include the preparation of joint reports containing operational personal data.

9. Frontex may use the operational personal data processed and stored in the framework of Analytical Projects for risk analysis purposes. The results of the risk analysis shall be anonymised.

Article 11

Data Structure

1. Operational personal data must be collected, reported and processed based on a data model that is compatible with most current version of the Universal Messaging Format.

2. Whenever possible, Frontex data structure comprises:

   (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

~~(j)~~

3. Frontex may change this data structure depending on the analytical and operational needs.

Article 12

Categories of data

1. Whenever possible, operational personal data must include categories consistent with the data model of the Universal Messaging Format. Examples of data categories are:

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

(b) Nick name or alias;

(c) Nationality/-ies;

(d) Gender;

(e) Age

(f) Description

(g) DNA

Fingerprint

~~(d)~~(h) ~~Photo~~

(i) Name of accomplices;

(j) Nick name or alias

(k) Nationality/ies

(l) Gender

(m) Age

~~(e)~~(n) Description

(o) Biometric data

(p) DNA

Fingerprint

~~(f)~~(q) ~~Photo~~

~~(g)~~(r) Organized crime group;

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

~~(i)~~(t) Personal address and/or coordinates;

~~(j)~~(u) Safe house address and/or coordinates;

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

~~(l)~~(w) Means of transportation (vehicle registration, boat name, license plate, chassis number, flight tickets, etc.).

(x) Weapon(s);

~~(m)~~(y) Illegal goods

~~(n)~~(z) Photograph(s)

~~(o)~~(aa) Personal characteristics;

~~(p)~~(bb) Offence event (description of criminal offence);

~~(q)~~(cc) Non-offence event (meeting or communication or any other event linked to the criminal offences that fall under the scope of the present Decision).

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

Article 13

Transfer of personal data to the law enforcement authorities of the Member States

1. Frontex will transfer operational personal data to the ~~competent~~ law enforcement authorities of the Member States only where they are strictly necessary for those authorities for the purposes of preventing, detecting, investigating or prosecuting serious cross-border crime.

2. Frontex will transfer these data only to the National Contact Point of the Member States via the information exchange systems and applications mentioned in Article 7~~6~~ of this Decision. The National Contact Points will disseminate further the information, including the operational personal data, to the law enforcement authorities of their Member State that is competent to use them in accordance with Article 90(2)(b), of the Regulation.

3. Frontex will decide to which Member States to transfer 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 a suspect or a related entity, and a Member State;
      (ii) likelihood that the security of the Member State is affected by the criminal activities of a suspect or the organized crime group the suspect belongs to;
      (iii) submission of a justified request for information by a Member State to Frontex, in accordance with Article 90 of the Regulation.

   (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 Frontex.

4. In cases when Frontex identify Member States that have the *need to know* specific operational personal data, but cannot share them due to restrictions imposed via the handling codes, Frontex may request the data owner to lift the handling code. Frontex 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 14

Transfer of personal data to Europol and Eurojust

1. Transmissions of personal data to Europol and Eurojust as foreseen in Article 90(2)(a) of the Regulation must:
   (a) Be performed only if the data are necessary for use in accordance with their respective mandates;
   (b) Be subject to specific working arrangements;
   (c) Be subject to prior approval by the EDPS;

(d) Respect the principles of necessity and proportionality. Frontex will only process personal that are adequate and in their extent proportionate in relation to the purposes defined in Article 3 of this Decision.

2. Both Frontex and the recipient Agency bear the responsibility for the legitimacy of the transfer.

3. The Data Controller is required to:

(a) Verify the competence and mandate of the recipient Agency;

(b) Verify ~~Make a provisional evaluation of~~ the necessity of the transfer of personal data;

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

4. To contribute to the evaluation, the recipient Agency must supply in advance and for inclusion in specific operational plans:

(a) Categories of data that are required from the operational area;

(b) Nationalities that are of current interest from the operational area;

(c) Areas of crime that are of current interest in the operational area;

(d) Geographical locations (e.g. countries of origin, transit, departure) which are of current interest.

~~5.~~ Personal data that match one or more of the criteria listed in paragraph 4 pass the evaluation of the necessity for the recipient Agency and can ~~.~~

~~6.~~5. ~~Only the personal data that pass the evaluation may~~ be transferred to the recipient agency.

~~7.~~6. Frontex may transfer to recipient Agencies processed personal data or analytical products containing operational personal data resulting from the analytical processes.

~~8.~~7. For monitoring purposes, recipient agencies are requested to provide regular feedback regarding the utility of the personal data transmitted by Frontex. The format and periodicity of the feedback are detailed on the specific arrangements.

Article 15

Processing of operational personal data for risk analysis

1. Frontex nominated risk analysts have read-only access to personal data in order to support the risk analysis processes.

2. The risk analysis results should be anonymised.

3. The anonymised results of risk analysis are not to be subject to prior checking by the EDPS.

Article 16

Processing of special categories of operational personal data

1. Frontex processes special categories of data following Article 76 of the Data Protection Regulation.

2. In particular, Frontex processes the following special categories related to operational personal data for the purposes of transmission to Member States, Europol, and Eurojust, as well as when necessary for the preparation of risk analyses, only if strictly necessary:

(a) Racial or ethnic origin,

(b) Political opinions, religious or philosophical beliefs;

(c) Genetic data and/or biometric data for the purpose of uniquely identifying a natural person;

(d) Health;

(e) Sexual orientation.

3. Processing of operational personal data based solely on these categories is prohibited. Profiling that results in discrimination against natural persons on the basis of special categories of personal data shall be prohibited. Processing of special categories of data related to persons who cross the external border without authorisation under Article 88(1)(a) shall be done only under having obtained the consent of the data subject. This consent will be informed, explicitly given and documented by the data controller.

4. Transmission of special categories of data related to migrants under Article 88(1)(a) of the Regulation to the competent authorities of the Member States and Union Agencies in accordance with Article 88(2)(a) of the Regulation will be done only when strictly necessary for the completion of the mandate of those national authorities or Union agencies.

5. When the processing of operational data 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 of~~f~~ cross border crime or terrorism.

   (b) If the data subject is a minor between and 15 and 18 years old, the providing Member State 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 or terrorism.

   (c) After transmission, personal data related to a child will immediately be deleted.

Article 17

Data storage and deletion

1. Operational personal data expires in Frontex 90 days after verification and successful acceptance performed by the dedicated Frontex staff.

2. Expiry dates will be calculated from the moment of acceptance of the personal data into systems used by Frontex for the analysis or further transmission.

3. Operational personal data shall be deleted or anonymised from the Frontex operational systems on or before the day of its expiry.

4. Frontex may store personal data longer than 90 days only when these data are necessary in an Analytical Project mentioned in Article 10~~9~~ of this Decision. These operational personal data shall be:

   (a) linked with an Analysis Project only if they were collected in the framework of the project or they fall under the scope of the project, as mentioned in Article 9(2) of this Decision.

   (b) stored only during the lifecycle of the Analytical project in which they are used and will be anonymised immediately after the closure of the project. Operational personal data that are being used in more than one Analysis Project will anonymised only after the closure of the last project where they are used.

   (c) reviewed no longer than 90 days after the successful acceptance of these data by Frontex staff and after that periodically, but no longer than every 180 days, to verify the necessity of storing these data longer.

5. Pseudo-anonymisation cannot be treated as equivalent to deletion or anonymization referred to in paragraph (3) of this article. Pseudo-anonymised data is still personal data.

6. In case irreversible anonymisation of operational personal data cannot be ensured, Frontex shall delete the operational personal data. The anonymization of personal data should be considered irreversible if data subjects can no longer be identified, having regard to all methods reasonably likely to be used by Frontex to identify the data subject.

7. Deletion or anonymization of expired data applies to:

a. Personal data in its original form as collected from the Frontex own staff, the Member States, Europol, and Eurojust;

b. Any other files or documents within Frontex that contain expired data;

c. Any on or offsite backups containing expired data.

8. Deletion or anonymisation of the personal data stored in the Frontex systems used for collection, analysis, and transmission shall be automated wherever possible.

9. In the event that deletion or anonymization is performed manually, a staff-allocation schedule is to be produced to maintain business continuity.

10. Regular checks shall be performed to ensure that no expired personal data remain on Frontex operational systems.

11. A logbook will be maintained by Frontex authorized staff when manual deletion occurs and when checks are performed. The results of these checks will be provided to Frontex Data Protection Officer.

12. Anonymized data relating to thereafter unidentifiable persons may persist indefinitely in Frontex.

Article 18

Logging

1. Frontex shall keep logs for any of the following processing operations within the information exchange systems and applications used for exchanging personal data and administrated by the Agency: the collection, alteration, access, consultation, disclosure, including transfers, combination and erasure of operational personal data. The logs of consultation and disclosure shall make it possible to establish the justification for, and the date and time of, such operations, the identification of the person who consulted or disclosed operational personal data, and, as far as possible, the identity of the recipients of such operational personal data.

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, and for criminal proceedings. Such logs shall be deleted after three years, unless they are required for on-going control. In case the logs display operational personal data, the operational personal data is deleted in accordance with Article 15 of this Decision.

3. The Data Protection Officer has access to the logs at all times for control purposes.

4. The controller shall make the logs available to the European Data Protection Supervisor when requested.

Article 19

Handling Codes

1. For the purposes established by Article 87(2), the Member States and Union and Union bodies, offices and agencies and international organisations referred to in points (c) and (d), Article 87(1) of the Regulation will use the following handling codes to indicate to Frontex the purposes for which the transmitted personal data may be used.

   (a) Handling Code H0: This information can only be used for the prevention, detection, investigation or prosecution of cross-border crimes and terrorism, in accordance with Articles 87 (c) and 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 consent 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 authorization 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 a 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 20

Evaluation Codes

1. When providing operational personal data to Frontex, the Frontex own staff, 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 III
Roles and responsibilities

Article 21

Data Protection Responsibilities of the host Member State

1. Member States are responsible for collecting personal data during Frontex coordinated Joint Operations, Pilot Projects, and Rapid Border interventions. Member States are also responsible for the collection of operational personal data conducted by migration management support teams.
2. When collecting personal data of persons who cross the external borders without authorizations, Member States will be responsible for the collection done by the European Border and Coast Guard Teams. The data protection responsibility extends until the moment of transmission to Frontex.
3. Member States are responsible for the security and data protection during all processing of personal data, until the moment of transmission to Frontex.
4. The providing Member State shall distinguish, as far as possible, operational personal data based on facts from operational personal data based on personal assessments by using mechanisms for the reliability of the data source.
5. The providing Member State under its responsibility shall take all reasonable steps to ensure that operational personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, the providing Member State shall, as far as practicable and where relevant, verify, for example by consulting with other competent authorities the data originates from, the quality of operational personal data before they are transmitted or made available. As far as possible, in all transmissions of operational personal data, the providing Member State shall add necessary information enabling Frontex to assess the degree of accuracy, completeness and reliability of operational personal data, and the extent to which they are up to date.
6. Member States shall notify Frontex without delay if it emerges that incorrect operational personal data have been transmitted or operational personal data have been unlawfully transmitted. In such a case, the operational personal data shall be rectified or erased.
7. The providing Member State designates points of contact for the exercise of data protection responsibilities and informs Frontex.

Article 22

Appointment and Responsibilities of the Intelligence Officers

1. Member States will ensure to nominate and appoint Intelligence Officers during the duration of a Joint Operation or Pilot Project.

2. Member States will ensure that there are Intelligence Officers at all times available for the validation of personal data in the context of a Joint Operation or Pilot Project, to ensure business continuity and transmission of data in due time.

3. The nominated Intelligence Officers will ensure that the collection and transmission of operational personal data at Member State level complies with the 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 convictions, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Likewise, the Intelligence Officers will ensure that the collection and transmission of operational personal data complies with this Management Board Decision and with the provisions of the Operational Plan.

4. The Intelligence Officers will signal the existence of a suspicion of cross border crime or terrorism, in accordance with Article 47(1) (a) of the Regulation.

5. The Intelligence Officer will respond to requests from Frontex in due time for more information following inconclusive authentications of operational personal data.

6. The Intelligence Officer may be the data protection contact point, in particular for liaising in case data subject rights are exercised against Frontex database.

Article 23

Roles and Responsibilities of Frontex

1. Pursuant to Article 44(1) of the Frontex Regulation, Frontex is fully responsible for developing and operating an information system that is able to exchange classified operational personal data. This system is JORA (Joint Operations Reporting Application).

2. Frontex is responsible for the data collected and transmitted by Frontex own staff, in particular with regard to lawfulness, fairness, accuracy, quality and reliability of the data.
3. Frontex is responsible for data protection and data security once the verification process has successfully been finalized.
4. Frontex is responsible for the integrity and confidentiality of the operational personal data whilst processed by Frontex.
5. Frontex is responsible for ensuring the envisaged data storage limitations.
6. Frontex is responsible for providing Member States with access to JORA (Joint Operations Reporting Application) for transmitting operational personal data to the Agency.
7. Frontex is the sole responsible for keeping logs of the processing operations occurred within the information system and within the process of analysis.
8. Frontex is the sole responsible for the collection and processing of personal data stemming from Open Source Intelligence (OSINT).

Article 24

Joint responsibility of Frontex and Member States

1. When data is collected by Member States, these are responsible for its content, lawfulness, fairness, accuracy, quality and reliability upon the moment of a successful validation process in accordance with their respective legal framework.
2. Pending the successful validation process, Frontex will be only responsible for the security of the information system on which the data are transmitted, pursuant to Article 69oe of the Data Protection Regulation, in particular for the confidentiality, availability and the integrity of the operational personal data whilst it is transmitted.
3. MSs are exclusively responsible for the accuracy of data from the moment of transmission to successful validation.
4. The content of the uploaded personal data remains the joint responsibility of Frontex and the sending Member State, until the authentication process has been completed, when the operational personal data is then a sole responsibility of Frontex until the moment of further transmission or deletion.
5. With regards to the right to be informed, Member States are responsible for facilitating this right to the data subjects via appropriate means.
6. Frontex provides within its webpage information related to the processing of operational personal data. This information will be easily accessible, concise and intelligible, and in addition provides the means for the exercise of the right to access, rectification, erasure, rights of access on data under criminal investigations and proceedings, and the possibility to exercise these rights via the European Data Protection Supervisor.
7. With regards to the obligations established by the Data Protection Regulation in relation to the notification of personal data breaches to the European Data Protection Supervisor, Frontex will inform the European Data Protection Supervisor if that breach compromises the confidentiality, availability and the integrity of the operational personal data while the transmission is occurring. Frontex has also the obligation of notification of potential personal data breaches if the operational personal data is compromised after the verification phase is completed.

Chapter IV
Data protection

Article 25

Joint Controllership - General principles

1. The Joint Controllers shall, taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of the processing as well as risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of operational personal data.
2. The Joint Controllers creates and enforces the procedures necessary to ensure that the security of the operational personal data is safeguarded in the organizational part of the process under his/her responsibility described here above and requires from ICT to implement in the systems the necessary technical security controls so that 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.
3. In respect of automated processing, the controllers shall, following an evaluation of the risks, implement measures designed to:
    a. deny unauthorised persons access to data processing equipment used for processing (equipment access control);
    b. prevent the unauthorised reading, copying, modification or removal of data media (data media control);
    c. prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
    d. prevent the use of automated processing systems by unauthorised persons using data communication equipment (user control);
    e. ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation (data access control);
    f. ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication (communication control);
    g. ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems, and when and by whom the data were input (input control);
    h. prevent unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);
    i. ensure that installed systems may, in the case of interruption, be restored (recovery);
    j. ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored personal data cannot be corrupted by means of a malfunctioning of the system (integrity).
4. By adopting such security measures, Frontex will:
    a. Ensure that personal data processed by third parties, notably subcontractors and service providers selected by Frontex, afford the same level of protection as if they were processed by Frontex own means and services. To that end, contractual measures will be taken via data protection agreements;
    b. Ensure that operational personal data cannot be accessed by administrators, except in exceptional circumstances and with the explicit approval of the Data Controller and after informing the Frontex Data Protection Officer;
    c. Ensure that logs of the systems are performed without faults, which the appearance of faults in the functions is immediately reported (reliability) and that stored personal data cannot be corrupted by system malfunctions (integrity).
5. The infringement of the obligations stated in point 3 and 4 above constitutes a personal data breach that is to be reported following the procedure described in Article 17a of this Management Board Decision.
6. New technical means for processing data for risk analysis purposes may be introduced only if all reasonable measures for ensuring that their use is consistent with the rules on the protection of operational personal data in accordance with the Data Protection Regulation. The Executive Director shall consult the EDPS in advance in all cases where the introduction of such technical means raises problems for the application of these data protection rules.
7. Due to the frequent updates of the systems to keep them as secure as possible and the potential change in the underlying technologies, the Data Controller reports to the Data Protection Officer the IT technical measures that it takes to protect the personal data subject to this Decision and every subsequent change.

Article 26

Joint Controllership - Security Roles

1. The Data Controller is responsible for ensuring that:
    a. Review procedures are adopted, to ensure that the processing of personal data takes place in compliance with this Decision and to frequently improve the measures put in place in order to protect the operational personal data.
    b. Questions and concerns regarding the protection of data, subject to this Decision that are processed through the information system are timely addressed to the Data Protection Officer.
    c. Conducts a privacy impact assessment when 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;
2. The Frontex Data Protection Officer is responsible for:
    a. Internal data protection audits are conducted; highlighting possible deficiencies and measures to strengthen data processing procedures adopted by the Data Controller;
    b. Provides advice to any question related to the processing of operational personal data, in particular for data protection impact assessments;
    c. Ensures the internal application of this Decision and monitors its compliance, with the Data Protection Regulation and with the policies of the controller in relation to the protection of operational personal data, including the assignment of responsibilities, the raising of awareness and training of staff involved in processing operations, and the related audits;
    d. Ensures that data subjects are informed of their rights and obligations pursuant to the Data Protection Regulation and other Management Board Decisions;
    e. Ensures that the rights and freedoms of data subjects are not adversely affected by processing operations;
    f. Provides advice where requested as regards the necessity for a notification or a communication of a personal data breach;
    g. Consults with the EDPS in case of doubt as to the need for a data protection impact assessment or prior consultation;
    h. Responds to requests from the EDPS and cooperates and consults either at the EDPS request or on his or her own initiative;
3. The ICT Security Officer is responsible for:
    a. Ensuring the appropriate technical measures and IT operational procedures are implemented whenever Frontex' ICT Systems (electronic communications infrastructure, applications, systems, information technology means and tools) used for the processing of operational personal data to this Decision;
    b. Maintaining the appropriateness of the adopted measures by regularly performing a security assessment in cooperation with the DPO at least once a year;
    c. And ICT risk analysis and technical audit in cooperation with the DPO;
    d. Bringing to the attention of the DPO and Data Controller any concern, indication or suspicion that an implementation or change in Frontex' security environment or information technology environment may have an impact on personal data protection and privacy;
    e. Implementing any security-related controls or other procedures.

Article 27

Data subject rights

1. Pursuant to Article 81 of the Data Protection Regulation, the rights foreseen in Articles 79, 80 and 82 of the Data Protection Regulation may be restricted wholly or partly by the Data Controllers on individual basis, as long as it is necessary for the purposes listed in Article 81 of the Data Protection Regulation.

2. The restrictions only apply to the data subjects listed under Article 90 of the Regulation.

3. Pursuant to Article 84 of the Data Protection Regulation, exercise of rights may be conducted through the European Data Protection Supervisor.

Article 28

Notification of a personal data breach to the European Data Protection Supervisor

1. In case of a personal data breach, the Controller notifies without undue delay and, when feasible, not later than 72 hours after having become aware of it, the breach to the European Data Protection

Supervisor or the competent National Data Protection Authority, depending on the responsibility for the processed personal data.

2. The notification to the EDPS is not necessary if it is unlikely to result in a risk to the rights and freedoms of natural persons. In order to demonstrate the assessment, the Controller keeps a register of breaches stating the likeness of those risks to occur.

3. The notification contains at least the following information:

    a. Description of the nature of the personal data breach including, when possible, the categories and number of data subjects affected and the categories and number of personal data records concerned.

    b. Name and contact details of the Data Protection Officer.

    c. Description of the likely consequences of the data breach, both for the organisation and the data subject.

    d. Description of the measures taken or proposed to be taken by the Controller to address the breach, including measures to mitigate the possible negative effects.

    e. When the notification has not been made within 72 hours, the reasons for the delay.

4. Where, and in so far as, it is not possible to provide the information referred to in paragraph 2 at the same time, the information may be provided in phases without undue delay.

5. The Controller documents any personal data breach referred to in paragraph 1 in an internal register, comprising facts, effects and remedial actions taken. The Controller informs the Data Protection Officer.

6. Where the personal data breach involves personal data transmitted by or to the competent authorities, the Frontex controller communicates the information referred to in paragraph 3 to the competent authorities of the Member States concerned without undue delay.

Article 29

Communication of a personal data breach to the data subject

1. Pursuant to Article 93 of the Data Protection Regulation, Frontex, jointly with the Member States, may communicate the existence of a personal data breach that results in high risks to the rights and freedoms of the data subjects.

2. When the data breach affects the operational personal data referred to in Article 47(1)(a) or (c) of the Regulation , Frontex may delay, restrict or omit the communication of personal data breaches to the data subjects, pursuant to Article 93,5 of the Data Protection Regulation.

3. This restriction will only be applicable when:

    a. Avoids obstructing official or legal enquiries, investigations or enquiries;

    b. it avoids prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

    c. protects public security of the Member States;

    d. Protects national security of the Member States;

    e. Protects the rights and freedoms of others.

4. When delays, restrictions or omissions to the communications to the data subject apply, the Controller keeps a register justifying its decision, which will be priory consulted with the Data Protection Officer.

5. The notification of a personal data breach to the data subject will not be necessary if any of the following conditions apply:

    a. The controller has implemented appropriate technological and organizational protection measures, and that those measures were applied to the operational personal data affected by

the breach, in particular those that render the operational personal data unintelligible to any person who is not authorized to access it, such as encryption;

b. The controller has taken subsequent measures which ensure that the high risks to the rights and freedoms of the data subjects is no longer likely to materialize;

c. The communication to the data subject would involve a disproportionate effort. In such case, the controller emits a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The communication to the data subject describes, in a simple and plain language, the nature of the personal data breach and will contain at least the information and recommendations of Article 25(3)(a) of this Decision.

CHAPTER IV
FINAL PROVISIONS

Article 30

Monitoring and Evaluation

1. Monitoring indicators are routinely collected and regularly evaluated by Frontex to establish the:
   a. Volume and data quality of personal data transmitted to Frontex by Member States;
   b. Value added to the purposes listed in Article 3 of this Decision by further processing in Frontex;
   c. Extent to which the recipient agencies use personal data transmitted by Frontex for the legitimate performance of tasks covered by the competence of the recipient.

Article 31

Entry into Force

This Decision enters into force following its signature.
Done by written procedure, xx xxxx xxxx

For the Management Board

Chairperson