

MANAGEMENT BOARD DECISION No 58/2015
of 18 December 2015

**adopting Implementing Measures for processing personal data collected
during joint operations, pilot projects and rapid interventions**

THE MANAGEMENT BOARD

Having regard to the Frontex Regulation¹, in particular Article 11a thereof,

Whereas:

- (1) The Charter of Fundamental Rights of the European Union guarantees the respect for private and family life (Article 7), establishes the right to data protection (Article 8(1)) and refers to the data protection principles (Article 8(2)). The Charter became part of the Treaties and therefore legally binding to EU institutions and bodies as well as Member States when they are implementing Union law.
- (2) Article 11c read together with Article 11a of the Frontex Regulation requires that the Data Protection Regulation² applies to the processing of personal data collected by the Member States during Joint Operations, Pilot Projects and Rapid Interventions.
- (3) The Data Protection Regulation sets out the principles and rules applicable to all EU institutions and bodies and protects the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
- (4) Implementing Measures for processing personal data referred to in Article 11c of the Frontex Regulation should specify the procedures regarding the data (the source, the categories of data, storage and archiving, the data authentication process, its transmission to Europol or other Union law enforcement agencies).
- (5) Implementing Measures should also detail roles and responsibilities of persons and entities involved in processing of personal data.
- (6) Implementing Measures for the application of the Data Protection Regulation should be adopted by the Management Board.
- (7) Management Board Decision No 34/2015 of 10 September 2015, in particular Article 10 thereof, foresees separate implementing measures for data processing in Frontex operational activities.
- (8) Implementing Measures should be established after consultation with the European Data Protection Supervisor (EDPS), the EDPS was notified on 25 September 2015.
- (9) EDPS delivered its opinion on 8 December 2015.

¹ Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union OJ L 349, 25.11.2004, p.1, as last amended.

² Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2001 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ L 8, 12.01.2001, p. 1.

HAS DECIDED AS FOLLOWS:

CHAPTER I GENERAL PROVISIONS

Article 1 **Subject and Scope**

1. This Decision lays down the specific measures regarding the processing of personal data collected by the Member States during Joint Operations, Pilot Projects and Rapid Interventions and transmitted to Frontex, pursuant to Article 11c of the Frontex Regulation.
2. This Decision has to be read in conjunction with the Management Board Decision No 34/2015 of 10 September 2015 adopting Implementing Measures for the application of the Data Protection Regulation by Frontex.

Article 2 **Definitions**

1. For the purpose of this Decision the definitions included in the Data Protection Regulation and in the Frontex Regulation apply.
2. For the purpose of this Decision:
 - a) 'Data Controller' is the Head of the Risk Analysis Unit;
 - b) 'Anonymised data' are personal data that have been manipulated so that data subjects can no longer be identified;
 - c) 'Intelligence Officers' are Member State officials responsible for gathering the collected personal data and transmitting it to Frontex;
 - d) 'Cases' are comprised of personal data and contextual information which, when assessed together, add value to the purposes in Article 3 of this Decision;
 - e) 'Case-by-case basis' means a non-automatic and non-systematic process, subject to a decision assessing the necessity and proportionality of the transfer of cases to Europol or other Union law enforcement agencies;
 - f) "Data subjects" are persons who are suspected, on reasonable grounds, by the competent authorities of the Member States of involvement in cross-border criminal activities, in facilitation of illegal migration activities, or in human trafficking.

Article 3 **Purposes for processing personal data**

1. Frontex processes personal data only for the following two purposes:
 - a) The transmission on a case-by-case basis to Europol, or other Union law enforcement agencies;
 - b) The use for the preparation of risk analyses, the results of which should be depersonalised.
2. Non-expired personal data (processed in Frontex for less than 90 days) may be used multiple times for both or either of the purposes defined in the Article 11(c) (3) of the Frontex Regulation.

Article 4

Source and scope of personal data

1. The main sources of personal data collected by Member States and transmitted to Frontex are debriefing activities and other actions foreseen in the Operational Plan of the respective Joint Operation, Pilot Project and Rapid Intervention.
2. The conditions under which each Member State is expected to transmit personal data to Frontex is set out in specific provisions of the respective Operational Plan.
3. Frontex does not process personal data relating to victims of human trafficking, smuggled migrants or persons in need of international protection.
4. 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.

CHAPTER II

PROCESSING OF PERSONAL DATA

Article 5

Responsibilities in the host Member State

1. Member States are responsible for collecting personal data during Frontex coordinated Joint Operations, Rapid Interventions or Pilot Projects.
2. Member States are responsible for the security and data protection during all processing of collected personal data, until the moment of transmission to Frontex.
3. Pursuant to the provisions of the Operational Plan, Intelligence Officers are responsible for:
 - a) ensuring that only personal data that comply with the Data Protection Regulation, the Frontex Regulation, this Decision and the provisions of the Operational Plan are transmitted to Frontex;
 - b) responding to requests from Frontex for more information following inconclusive authentications of personal data in Frontex.

Article 6

Roles and Responsibilities in Frontex

1. Frontex Situation Centre is responsible for providing Member States with access to JORA (Joint Operations Reporting Application) for transmitting personal data to Frontex.
2. Frontex Situation Centre is responsible for managing access rights to the JORA.
3. Frontex is responsible for the security of the personal data from the moment it has been uploaded to the reporting system.
4. The content of the uploaded personal data remains the joint responsibility of Frontex RAU and the sending Member State, until the authentication processes have been completed.

Article 7
Data Structure

1. Wherever possible, personal data must be collected, reported and processed in accordance with the structure and data model of most current version of the Universal Messaging Format Police Information Model, in which information is organised by:

- a) Person;
- b) Organisation;
- c) Location;
- d) Item;
- e) Connections;
- f) Event.

2. All processing operations, such as receipt, storage, consultation and transmission, is logged, electronically where possible, in the interests of monitoring and evaluation.

Article 8
Categories of data

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

- a) Name(s) of subject;
- b) Nick name;
- c) Nationality/-ies;
- d) Name of known accomplices;
- e) Organised crime group;
- f) Registered business;
- g) Personal address;
- h) Safe house address;
- i) Means of communication (telephone, social media handle);
- j) Means of transportation (vehicle registration, boat name);
- k) Weapon;
- l) Photograph(s);
- m) Offence event (description of criminal offence);
- n) Non-offence event (meeting or communication or any other event linked to the criminal offences that fall under the scope of the present Decision).

Article 9
Special categories of data

1. Frontex does not process special categories of data as defined in Article 10(1) of the Data Protection Regulation.

2. Exceptionally, by derogation to paragraph 1, Frontex may process data on the ethnicity of the data subjects, where:

- a) knowing the ethnicity of a subject will add value to risk analyses, by being more applicable in that criminal, geographical or cultural context than nationality, or;
- b) knowing the ethnicity is likely to assist recipient agencies in identifying individuals by being more applicable in that criminal, geographical or cultural context than nationality.

3. Ethnicity is to be treated with respect as an integral part of an individual's identity, similar to that of nationality.

4. Use of ethnic data for discriminative purposes is forbidden.

Article 10

Channels for transmission of data

1. Member States must use the personal data reporting channel within JORA for transmitting personal data to Frontex:
 - a) access to the personal data reporting channel in JORA is strictly limited in Member States to Intelligence Officers nominated for the transmission of personal data to Frontex;
 - b) in the unlikely event that no Intelligence Officers are nominated or available in the Member State, temporary access to JORA may be granted to other nominated and authorised individuals. In such circumstances, Article 5 (3) applies;
 - c) personal data sent to Frontex via a channel other than JORA, will not be further processed by Frontex under any circumstances and in such case, the sent data will be destroyed;
 - d) in the event that personal data are sent to Frontex via a channel other than JORA, the Intelligence Officer of the sending Member State will be informed for monitoring purposes;
 - e) in the event that personal data are sent to Frontex via a channel other than JORA, the transmission will be logged for monitoring and evaluation purposes.
2. Frontex uses the Secure Information Exchange Network Application (SIENA) tool for transmitting personal data to Europol:
 - a) personal data and supporting information is transmitted to Europol on a case-by-case basis;
 - b) personal data is transmitted to Europol only if the conditions set out in Article 15 of this Decision are fulfilled.
3. Frontex uses adequate secure channels for transmissions of personal data to other Union law enforcement agencies.

Article 11

Data storage and deletion

1. Personal data expires in Frontex 90 days after its authentication.
2. Expiry dates will be calculated for personal data at the time of authentication.
3. Personal data shall be deleted or anonymised from Frontex operational systems on or before the day of its expiry.
4. Anonymised data are those that no longer contain any identifiers, such that no element is left in the data which could, by exercising reasonable effort, serve to re-identify the person concerned.
5. Pseudonymisation cannot be treated as equivalent to deletion or anonymisation referred to in paragraph 4, because pseudonymised data is still personal data.
6. Deletion or anonymisation of expired personal data applies to:
 - a) personal data in its original form as transmitted by the hosting Member State;
 - b) any other files or documents within Frontex that contain expired data;
 - c) any on or offsite backups containing expired data.

7. Deletion or anonymisation from master databases shall be automatized wherever possible.
8. In the event that deletion or anonymisation is performed manually, a staff-allocation schedule is to be produced to maintain business continuity.
9. Regular checks shall be performed to ensure that no expired personal data remain on Frontex operational systems.
10. Anonymized data relating to thereafter unidentifiable persons may persist indefinitely in Frontex.

Article 12 **Data archive**

1. Archiving of personal data for 3 years beyond its expiry date is permitted, provided that the following safeguards are in place:
 - a) the archive of expired personal data is encrypted and separate from operational systems;
 - b) access to archive of expired personal data is limited to the Data Controller and the Data Protection Officer, and only for confirmed judicial or audit purposes;
 - c) the name, date and reason for access to the archive are electronically logged for audit purposes.
2. Data may be retained in the archive for a period in excess of 3 years depending on the severity of the crime, consistent with the corresponding retention period in recipient agencies.

Article 13 **Access to personal data**

1. Access to personal data in Frontex is limited to the minimum necessary for the purposes listed in Article 3.
2. Personal data are only accessible to the Data Controller and personally nominated risk and intelligence analysts in Frontex who will process personal data on behalf of the Data Controller.
3. Frontex' personally nominated senior risk and intelligence analysts have read/write access to personal data.
4. Frontex' personally nominated risk and intelligence analysts have read-only access to personal data.
5. The copy of the nominations mentioned in the previous paragraphs are sent to the Frontex Data Protection Officer by the Data Controller.

Article 14 **Authentication processes**

1. Frontex reserves the right to accept personal data transmitted by Member States.
2. Decisions to accept personal data from Member States are underpinned by an authentication process.
3. During the authentication process, personal data are stored in a temporary location separate from operational systems.

4. The authentication process consists of two distinct phases: the validation check and the legality check.
5. The validation check shall be twofold:
 - a) source of the transmission - Frontex only accepts personal data transmitted by nominated Intelligence Officers in Member States. Without prejudice to Article 10(1)(b), personal data received from any other source will not pass the validation check;
 - b) data quality - Frontex only accepts personal data that has been collected in a way consistent with the principles referred to in Articles 4 and 9 of this Decision. Data that do not fulfil these conditions will not pass the validation check.
6. The legality check relates to Article 11c of the Frontex Regulation and Article 3 of this Decision:
 - a) source of personal data - as defined in Article 4(1);
 - b) data subjects - as defined in Article 2(2)(f).
7. Personal data that clearly do not pass either the data quality check or the legality check, are deemed to have failed the authentication process and will be deleted from the temporary storage area.
8. If a transmission fails any component of the authentication process, Frontex contacts the Intelligence Officer in the sending Member State and informs about the failure and the reason for the Decision.
9. Where it is not possible to fully complete the authentication process, Frontex may contact the Intelligence Officer in the sending Member State to request for additional material that may further inform the authentication process.
10. In the circumstances referred to in the previous paragraph, Member States will have 7 days to supply additional material.
11. Upon receipt of additional information the authentication process will be re-launched.
12. After 7 days if no additional material has been provided by the hosting Member State, the personal data will fail the authentication process and will be deleted from the temporary location mentioned in paragraph 3.

Article 15

Transfer of personal data to Europol or other Union law enforcement agencies

1. Transmissions of personal data to Europol or other Union law enforcement agencies must:
 - a) be performed only if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient;
 - b) be subject to specific working arrangements;
 - c) be subject to prior approval by the EDPS;
 - d) be on a case-by-case basis;
 - e) respect the principles of necessity and proportionality. Frontex will only process personal data 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 responsibility for the legitimacy of the transfer.

3. The Data Controller is required to:
 - a) verify the competence of the recipient Agency;
 - b) 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 necessity for the recipient Agency.
6. Only the personal data that pass the evaluation may be transferred to the recipient agency.
7. Personal data will be transferred to recipient Agencies only in the form of cases resulting from analytical processes.
8. For monitoring purposes, recipient agencies provide regular feedback regarding the utility of the personal data transmitted by Frontex. The format and periodicity of the feedback are detailed in the specific arrangements.

Article 16

Creation of depersonalised risk analyses

1. Frontex' personally nominated risk analysts have read-only access to personal data in order to support risk analysis processes.
2. Personal data are not included in risk analysis products.
3. Depersonalised data may be included in risk analyses products.
4. The results of depersonalised risk analyses are not be subject to prior checking by the EDPS.

Article 17

Restrictions to the data subject rights

Pursuant to Article 20 (1) (a) of the Data Protection Regulation the rights foreseen in Articles 13 to-17 of that Regulation may be restricted by the decision of the Data Controller on individual basis, documented internally, including the reason for restriction.

CHAPTER III DATA SECURITY

Article 18 **General Principles**

1. The Data Controller creates and enforces the procedures necessary to ensure that the security of the personal data is safeguarded in the organisational part of the process 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.
2. Such measures primarily aim at preventing:
 - a) any unauthorised person from gaining access to computer systems processing personal data;
 - b) any unauthorised reading, copying, alteration or removal of storage media;
 - c) any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;
 - d) any unauthorised persons from using data processing systems by means of data transmission facilities.
3. By adopting such security measures, Frontex will:
 - a) ensure that authorised users of a data-processing system subject to this Decision cannot access personal data other than those to which their access right refers;
 - b) record which personal data have been transmitted, at what times and to whom;
 - c) ensure that it will subsequently be possible to check which personal data have been processed, at what times and by whom;
 - d) ensure that, during transmission of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation;
 - e) 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;
 - f) ensure that personal data cannot be accessed by administrators; except in exceptional circumstances and with the explicit approval of the Data Controller;
 - g) ensure that logs of the systems involved in the processing, transmission and of personal data subject to this Decision cannot be altered by administrator without being noticed;
 - h) ensure that the functions of the system are performed without faults, that the appearance of faults in the functions is immediately reported (reliability) and that stored personal data cannot be corrupted by system malfunctions (integrity).
4. 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 Management Board and the EDPS, the IT technical measures that it takes to protect the personal data subject to this Decision and every subsequent change.

Article 19
Security Roles

1. The Data Controller is responsible for ensuring that:
 - a) review procedures are adopted, and internal and external audits are performed 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 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 and the INFOSEC Officer.
2. The INFOSEC Officer is responsible for:
 - a) ensuring that 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 personal data subject to this Decision;
 - b) maintaining the appropriateness of the adopted measures by regularly performing and at least once a year;
 - c) an ICT risk analysis and a technical audit;
 - d) a privacy impact assessment when significant modifications are introduced in the systems;
 - e) therefore, the INFOSEC Officer takes into account the newly discovered vulnerabilities in IT technologies embedded in the systems used for the processing of personal data subject to this Decision, the "best practices", the cost of the relevant technology solutions that should be proportional to the risks that the processing operation in question entails for data subjects;
 - f) 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;
 - g) implementing any security-related controls or other procedures.

CHAPTER IV
FINAL PROVISIONS

Article 20
Monitoring and Evaluation

1. Monitoring indicators are routinely collected 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 recipient agencies use personal data transmitted by Frontex for the legitimate performance of tasks covered by the competence of the recipient.

Article 21
Entry into Force

This Decision enters into force the day following its signature.

Done by written procedure, 18 December 2015

For the Management Board

[signed]

Ralf Göbel
Chairperson