FRONTEX

MANAGEMENT BOARD DECISION 68/2021

of 21 December 2021

adopting the rules on processing 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)(ae) 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) 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.

(3) The Agency may process personal data for the purposes set out in Article 87 of the Regulation. Personal data which qualifies as operational personal data as defined in Article 3(2) of the Data Protection Regulation processed for the purpose of Article 87(1)(d) of the Regulation should be out of the scope of this Decision. When processing operational personal data, the Agency applies Chapter IX of the Data Protection Regulation.

(4) The Agency, as part of the European Border and Coast Guard, together with the border management authorities of the Member States[3], is responsible for implementing European Integrated Border Management. In accordance with Article 87 of the Regulation for the performance of its core tasks the Agency may process personal data for a number of purposes.

(5) While performing its core tasks the Agency, in order to monitor its actions and ensure full compliance with fundamental rights obligations, including obligations stemming from the Charter of Fundamental Rights of the European Union, should be able to deploy image and voice recording devices where the national legislation of the host Member State or host Third Country so allows. The intrusion upon the privacy of the deployed team members and other individuals should be limited to the purpose of ensuring the respect of fundamental rights. In particular, in operational areas where use of force by the deployed team members is expected to occur on a regular basis the deployment of body cameras, as a preventive measure, may serve the purpose of decreasing the risk of physical attack against the deployed team members as well as to mitigate the risk of abusing power by them.

(6) The Agency's core operational tasks may require occasional processing of special categories of personal data, for example, racial or ethnic origin or political opinions, religious or philosophical beliefs for the purpose of identifying vulnerable persons during the operations or for risk analysis on illegal border crossings to assess the migratory trends including the push- and pull-factors of illegal immigration at the external borders. Equally, processing genetic data and/or biometric data, fingerprints or photographs can be absolutely necessary for the

[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).*

[3] *For the purpose of this Decision, 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.*

purpose of uniquely identifying a natural person while providing operational and technical assistance to the Member States such as screening migrants through migration management support team deployments. The health status of an individual may be necessary for the purpose of providing sufficient medical support during specific operational activities especially in hotspot areas or to identify vulnerable persons. In particular, the Agency shall identify persons in need of international protection, victims of trafficking of human beings, unaccompanied minors and persons in a vulnerable situation in view of referring those persons to the competent authorities of host Member States.

(7) Pursuant to Article 91(1) of the Regulation, personal data shall be deleted as soon as they have been transmitted to the competent authorities of Member States, other Union bodies, offices and agencies, in particular EASO, or transferred to third countries or international organisations or used for the preparation of risk analyses. The transmission of personal data to the aforementioned authorities shall be performed in accordance with the principles of necessity and proportionality, following a case-by-case assessment. The retention period shall, in any event, not exceed 90 days after the date of the collection of those data. Data shall be anonymised in the results of risk analyses.

(8) These implementing measures are without prejudice to the provisions of the Management Board Decision 56/2021[4] of 15 October 2021 concerning the tasks, duties and powers of the Data Protection Officer as well as rules concerning Designated Controllers in Frontex.

HAS DECIDED AS FOLLOWS:

Article 1
Object

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

Article 2
Repeal

This Decision repeals and replaces Management Board Decision 58/2015 of 18 December 2015 adopting Implementing Measures for processing personal data collected during joint operations, pilot projects and rapid interventions.

Article 3
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 personal data by the Agency

[4] *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.*

ANNEX
Rules on processing personal data by the Agency

CHAPTER I
General provisions

Article 1

Subject and scope

1. This Annex shall apply to the processing of personal data by the Agency for all purposes foreseen in Article 87 of the European Border and Coast Guard Regulation (hereinafter "the Regulation") with the exception of processing of personal data which qualifies as operational personal data as defined in Article 3(2) of the Data Protection Regulation for the purpose of Article 87(1)(d) of the Regulation.
2. Chapter IV of this Annex applies only to the processing of personal data by the Agency when carrying out activities for the purposes of Article 87(1)(a), (c) and (e) of the Regulation, without prejudice to Chapters I to III of this Annex.
3. This Annex shall apply without prejudice to Management Board Decision 56/2021[5].

Article 2

Definitions

For the purposes of this Annex, and without prejudice to the definitions provided for by the Regulation and the Data Protection Regulation, the following definitions apply:

(a) "Designated Controller" means designated controller as referred to in Article 1(c) of Management Board Decision 56/2021.

(b) "Deletion" means the irreversible deletion of personal data.

(c) "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.

CHAPTER II
Roles and responsibilities

Article 3

Internal arrangements concerning the engagement of processors by the Agency

1. Where the Agency intends to engage an external data processor, in accordance with Article 10(3) of Management Board Decision 56/2021, the Designated Controller shall ensure that the data processing agreement is concluded. These requirements shall also apply where the external data processor is being selected following a procurement procedure.
2. While selecting an external data processor, the Designated Controller shall evaluate and verify the processor's compliance with the EU Data Protection framework.

[5] *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.*

Article 4

Transfers of personal data to third countries or international organisations

Before transferring personal data to third countries[6] or international organisations, designated controllers shall ensure that:

(a) such transfers are documented through the record of processing activities referred to in Article 31(5) of the Data Protection Regulation, and in accordance with Management Board Decision 56/2021. This shall include information on the transfer tools[7] referred to in Chapter V of the Data Protection Regulation to be used as well as information on any onward transfers of personal data from the third country or international organisation in question to another third country or to another international organisation,

(b) a Transfer Impact Assessment is carried out where such data transfers are conducted based on Article 50 of the Data Protection Regulation,

(c) they seek the Data Protection Officer ('DPO')'s advice on the use of one of the transfer tools referred to in Chapter V of the Data Protection Regulation, in particular where a transfer based on Article 48 of the Data Protection Regulation requires additional safeguards, or when applying derogations as referred in Article 50 of the Data Protection Regulation, and

(d) where applicable, technical measures are in place to ensure that personal data is transferred securely with the use of encryption.

CHAPTER III
Processing of personal data

Article 5

Security measures and data protection by design and by default

1. To ensure a secure electronic and physical environment which prevents breaches of security related to personal data the Agency shall perform:
   (a) thorough and regular assessment of the effectiveness, reliability and resilience of information systems, tools and technologies selected and used for the security of personal data in electronic form, and
   (b) thorough assessment of the effectiveness of measures adopted for the security of personal data processed or stored in the form or physical documents, such as the access to premises, offices and hard copies of documents containing personal data.

   The result of these assessments shall be transmitted to the DPO.
2. The Agency shall adopt and implement a security policy for the proper use of IT tools and systems as well as for the prevention of physical security incidents, that includes an adequate definition of roles, responsibilities and procedural steps.
3. Designated Controllers shall implement data protection by design and by default measures, before starting to process personal data. In particular, Designated Controllers shall:
   (a) ensure the security of personal data throughout their life cycle, including secure destruction methods, proper encryption measures, pseudonymisation measures and robust methods of controlling authentication and access rights,
   (b) adopt technical measures which minimise the ability to identify, observe and link personal data to an individual to the minimum necessary, and
   (c) ensure the protection of personal data throughout the entire lifecycle of processing operations, by all actors involved in these processing operations.
4. When implementing data protection by default the Agency shall ensure that:

---

[6] For clarity, such transfers refer to transfers of personal data to recipients established outside the Union. The scope is not restricted to authorities of such countries.

[7] I.e. transfers on the basis of an adequacy decision (Article 47 of the Data Protection Regulation), transfers subject to appropriate safeguards (Article 48 of the Data Protection Regulation), transfers or disclosures not authorised by Union law (Article 49 of the Data Protection Regulation) and derogations for specific situations (Article 50 of the Data Protection Regulation).

(a) the purpose of processing personal data is defined prior to initiating a processing activity,

(b) the data minimisation requirements are satisfied by defining in the most restrictive way possible the categories of data to be processed for each specific purpose prior to the collection of personal data,

(c) appropriate technical and organisational measures are in place in terms of regulating access rights to personal data. Access rights refer both to physical and electronic access to data, and shall be granted individually and assessed periodically, and

(d) third parties involved in the processing of personal data, adhere to the level of data protection required by the applicable legislation.

Article 6

Personal data breach notifications

1. In the event of any incident that may constitute a personal data breach, in particular a breach of security, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transferred, stored, or otherwise processed, the Designated Controller shall notify the DPO without undue delay after becoming aware of the incident. Thereafter, and where feasible, not later than 72 hours, after the Designated Controller becomes aware of the data breach, the incident shall be notified to the EDPS, in accordance with Article 5(7) of Management Board Decision 56/2021.
2. The Designated Controllers shall ensure that the concerned staff maintain awareness of personal data breach incidents and report immediately any suspicious incidents or confirmed personal data breach incidents to the Information Security Sector.
3. The Executive Director, in consultation with the DPO and the Local Information Security Officer, shall adopt guidelines on the handling personal data breach incidents in the Agency.

Article 7

Storage, anonymisation and deletion

1. The Agency shall store personal data in a way that allows establishing responsibilities for it.
2. In order to ensure the principle of storage limitation, personal data shall be either deleted or anonymised if no longer necessary for the purpose of its processing. In case anonymisation of personal data cannot be ensured, the Agency shall delete the personal data.
3. Automated processing systems developed by the Agency shall allow for the automatic deletion or anonymisation of personal data based on predefined criteria, in accordance with paragraph 2. Deletion or anonymisation of personal data applies to:
   (a) All files or documents within the Agency that contain this data;
   (b) Any on or offsite backups containing this data;
   (c) Any system used to exchange personal data.
4. Regular checks shall be performed to ensure that no personal data is retained contrary to the principle of storage limitation on the Agency's operational systems.

Article 8

Logging

1. For the purpose of ensuring the principle of accountability, automated processing systems in the Agency shall log, as a minimum, the collection, alteration, consultation, disclosure (including transfers), combination or erasure of personal data.
2. Paragraph 1 of this Article shall not apply where logging would be disproportionate in view of the risks for the fundamental rights and freedoms of the data subjects. Designated controllers shall consult the DPO on that assessment.

Chapter IV
Specific rules for selected processing activities

Article 9

General conditions and channels for processing personal data during joint operations, pilot projects, rapid border interventions and migration management support team deployments

1. For the purposes of processing personal data during joint operations, pilot projects, rapid border interventions and migration management support team deployments the data protection requirements are set out in the operational plan in accordance with Article 38(3)(d) of the Regulation.
2. For the purposes of collecting personal data for risk analysis in the course of joint operations, pilot projects, rapid border interventions, and migration management support team deployments, paragraph 1 of this Article applies.
3. The Agency may exchange personal data referred to Article 88(1)(a) and (c) of the Regulation, with the national authorities of the host Member State(s) responsible for the implementation of a joint operation, pilot project, rapid border intervention, or migration management support team deployment, or with relevant Union bodies, offices and agencies, if it is necessary for them to fulfil their tasks, primarily via JORA[8]. Other channels may be established by the Executive Director, subject to the conditions set out in particular in Articles 27, 33, 39 and 40 of the Data Protection Regulation.
4. Where a national authority of a host Member State, the Commission, the EEAS, a Union body, office and agency or an international organisation, referred to in Article 87(1)(c) and (d) of the Regulation, transmits personal data to the Agency it shall indicate for what purpose that data needs to be processed in accordance with this Chapter. The channels referred to in paragraph 3 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 EDPS guidelines.
5. In the event that personal data is sent to the Agency via a channel other than those referred to in paragraph 3 of this Article, the Agency deletes the received personal data.
6. Access to the information exchange systems and applications referred to in paragraph 3 of this Article shall be granted only to duly authorised staff of the Agency, the officials of the relevant authorities of the Member States and Third Countries where relevant, Union bodies, offices and agencies and international organisations in accordance with the operational plans, working arrangements, or other procedures agreed by the Agency with its partners.
7. When providing personal data to national authorities of the host and participating Member States, host Third Countries, relevant Union bodies, offices and agencies or international organisations in accordance with Article 88 of the Regulation, the Agency shall indicate the reliability of the information, and the purposes for which the personal data may be used.

Article 10

Data protection roles and responsibilities

1. The provisions of the operational plan referred to in paragraph 1 of Article 9 of this Annex shall allocate the data protection roles, responsibilities and obligations of the Agency and the host Member State and if applicable the host Third Country, in particular as regards the data subject rights.
2. Where the Agency and the national authorities of the host Member State(s) and/or host Third Country(ies) responsible for the implementation of a joint operation, pilot project, rapid border intervention or migration management support team deployment are joint controllers in

[8] *Joint Operation Reporting Application.*

accordance with Article 28 of the Data Protection Regulation, the dedicated part of the operational plan addressing the data protection requirements in accordance with Article 38(3)(d) of the Regulation shall cover the necessary elements of the arrangement referred to in the first subparagraph of Article 88(1) of the Regulation.

3. The Agency shall ensure that the essence of the provisions of the operational plan referred to in paragraph 2 of this Article is made available on the website of the Agency.

Article 11

Stationary and portable image and voice recording devices

1. For the purpose of performing particular operational tasks during joint operations, pilot projects, rapid border interventions and migration management support team deployments and to ensure the full respect of fundamental rights during those actions automatic and/or manual image and voice recording devices may be deployed to the operational areas by the Agency. Additionally, those devices may facilitate the overall safety and security of the deployed team members and also contribute to an effective control mechanism, in particular to monitor the appropriate application of use of force by the deployed team members.
2. The Agency shall ensure that the automatic and/or manual image and voice recording devices referred to in paragraph 1 of this Article are deployed in full compliance with the data protection requirements of the national law of the host Member State(s) or Third Country(ies), the applicable EU data protection framework, and with this Annex.
3. Prior to the installation of such a device on any technical equipment being deployed by the Agency or by a participating Member State or being carried by the team members in the operational area, the host Member State(s) or Third Country(ies) shall give its explicit agreement in the operational plan. If necessary, a written arrangement between the Agency and the competent national authority, complementing the operational plan may be concluded to address particular data protection requirements.

Article 12

Processing of personal data with third countries for the purpose of performing tasks related to joint operation, pilot project, rapid border intervention or migration management support team deployment

1. Without prejudice to the data protection provisions of the respective status agreement and/or working arrangement and Article 4 of this Annex, the Agency may exchange personal data for the purpose of implementing joint operation, pilot project, rapid border intervention or migration management support team deployment with the authorities of the Third Country concerned in accordance with the operational plan.
2. In the absence of an adequacy decision in accordance with Article 47 of the Data Protection Regulation, the operational plan shall include appropriate safeguards in accordance with Article 48 of the Data Protection Regulation. It shall be ensured that the operational plan is legally binding on the Agency and on the national authority of the host Third Country responsible for the implementation of a joint operation, pilot project, rapid border intervention or migration management support team deployment.
3. The dedicated part of the operational plan addressing the data protection requirements in accordance with Article 38(3)(d) of the Regulation shall set out the roles and responsibilities of the Agency and the national authority of the host Third Country responsible for the implementation of a joint operation, pilot project, rapid border intervention or migration management support team deployment.
4. When a national authority of a host Third Country transmits personal data to the Agency, Article 9(4) of this Annex shall apply.

Article 13

Data model

1. Personal data for the purpose of Article 87(1)(a), (c) and (e) of the Regulation shall be collected and processed based on a data model which comprises, but is not limited to the following entities:
   (a) Person;
   (b) Organisation;
   (c) Location;
   (d) Item;
   (e) Connections;
   (f) Event;
   (g) Telephone numbers;
   (h) Means of transportation;
   (i) Financial means;
   (j) Identification documents;
   (k) Photo.
2. The Agency's data structures referred to in paragraph 1 may be adjusted depending on the necessity and proportionality assessment preceding the operational activities.

Article 14

Types of personal data including special categories

1. Whenever possible, personal data shall include data categories set out in a non-exhaustive list in points (a) to (r) below, however, the operational plan may further specify which of the categories below are processed in accordance with Article 88(1) of the Regulation:
   (a) Name(s) of the data subject;
   (b) Nickname 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) Biometric data as defined in Article 3(18) of the Data Protection Regulation;
   (h) Membership of organised crime group;
   (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, licence plate, chassis number, flight tickets, etc.);
   (m) Weapon(s);
   (n) Illegal goods;
   (o) Photograph(s)[9];
   (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 personal data only if strictly necessary to achieve the purpose of referred to in points (a), (c) and (e) of Article 87(1) of the Regulation. For that purpose, special categories of personal data are:
   (a) Racial or ethnic origin;
   (b) Political opinions, religious or philosophical beliefs;
   (c) Genetic data and/or biometric data, fingerprints or photographs for the purpose of uniquely identifying a natural person;
   (d) Health status.

[9] *Unless it falls under the specific category of point (c) of paragraph 2 of Article 14 of this Annex.*