FRONTEX

RECORD OF PROCESSING ACTIVITY ON PERSONAL DATA FOR DATA CONTROLLERS

i. Processing parties

CONTROLLER NAME	CONTACT DETAILS
IFC	HoO.IFC@frontex.europa.eu
DATA PROTECTION OFFICER NAME	**CONTACT DETAILS**
DPO	DATAPROTECTIONOFFICE@FRONTEX.EUROPA.EU
PROCESSOR NAME	**CONTACT DETAILS**
ICT	HoU.ICT@frontex.europa.eu
JOINT CONTROLLERS' NAME	**CONTACT DETAILS**
N/A	N/A

ii. Processing activity

NAME OF THE ACTIVITY

JORA users administration

PURPOSE OF THE PROCESSING OF PERSONAL DATA

JORA system records and processes personal data of system users for administrative purposes. The data subjects are internal Frontex users (staff members of the Agency) and external users (non-Frontex staff), whose personal data are recorded and managed in the JORA system. The JORA system administrators are having access to the personal data of data subjects in order to managing their accesses to different JORA modules.

OTHER PURPOSES

◉ No other purposes

○ If you are going to use the data for other purposes, please explain below:

Click or tap here to enter text.

NECESSITY OF THE PROCESSING OF PERSONAL DATA

The registered personal data of data subjects in JORA are necessary to process the access requests and to enable the users' access to the requested modules/functions of the JORA system.

DATA SUBJECTS

☒ **For Administrative data**

☒ Staff
☒ SNEs, including SGOs
☒ Trainees
☒ Outsourced personnel
☒ EBGT members
☒ Member States contacts
☐ Other contacts Please specify here.
☒ Others **Third Country (TC) users, EU Agencies and EU Institutions, International Organizations**

☐ **Under Article 48 Frontex Regulation**

☐ Returnees under Article 48 EBCG Regulation
☐ Escorts
☐ Monitors
☐ Medical personnel
☐ Others Please specify here.

☐ **Under Article 47 Frontex Regulation**

☐ Suspects of cross border crime
☐ Suspects of terrorism
☐ Persons who have crossed the external border without authorisation
☐ Others Please specify here.

CATEGORIES OF PERSONAL DATA

☒ **For Administrative data**

☒ Name
☒ Surname
☐ Date of Birth
☒ Picture
☒ Communication data (email account, telephone number, address work or personal).
Email, phone numbers
☐ Financial information (bank account or others).
Please specify here.
☐ Others
Please specify here.

☐ **Under Article 48 Frontex Regulation**

☐ Name
☐ Surname
☐ Date of Birth
☐ Picture
☐ Others
Please specify here.

☐ **Under Article 47 Frontex Regulation**

☐ Name
☐ Surname
☐ Date of Birth
☐ Picture
☐ Others
Please specify here.

DATA RETENTION

Data category	**Time limit**
Name, surname, picture, e-mail, phone number	Personal data fields deleted 12 months after the user accounts are deactivated in Frontex systems: - Internal accounts are deactivated automatically at the end of the contracts - External accounts are deactivated automatically 120 days after last successful login Personal data fields subject of deletion according to the above mentioned process: - Name, Surname, Picture - Communication data (e-mail, phone numbers)
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.

iii. Disclosure of personal data

RECIPIENTS WHERE PERSONAL DATA IS DISCLOSED
FRONTEX UNITS *(Please list all units/sectors to whom the data will be disclosed):*
Frontex IFC for administrative and support services. Frontex ICT for administrative and support services. In addition, personal data is not visible to units/sectors in particular, but to other users of the system in a need to know basis. - Access managers can see all Administrative Data of users participating in Frontex operations and activities they manage - Data reporters, validators and owners can see only Name and Surname of other users participating in the same Frontex operations and activities they participate when dealing with reports shared among them.
MEMBER STATES AUTHORITIES OR THIRD PARTIES WITHIN THE EU
- Access managers can see all Administrative Data of users participating in Frontex operations and activities they manage. - Access managers to the application can see all Administrative Data of fellow countrymen. - Data reporters, validators and owners can see only Name and Surname of other users participating in the same Frontex operations and activities they participate when dealing with reports shared among them.
THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS *(If this is the case, please document the additional safeguards in compliance with Art. 48 of the DPR):*
- Data reporters, validators and owners can see only Name and Surname of other users participating in the same Frontex operations and activities they participate when dealing with reports shared among them.

iv. Privacy Statement

PRIVACY STATEMENT/ DATA PROTECTION NOTICE	
FOR MORE INFORMATION INCLUDING HOW TO EXERCISE YOUR RIGHTS TO ACCESS, RECTIFICATION, OBJECT AND DATA PORTABILITY (WHERE APPLICABLE). FOR DRAFTING OF THE PRIVACY STATEMENT, PLEASE FOLLOW ART. 15-16 OF THE DPR.	*Please insert a link if available, or the text of the privacy statement:* Privacy notice for processing personal data of JORA system users: This privacy notice is available to JORA system users within JORA system. Frontex collects and manages personal data of JORA system users (considered as data subjects) in accordance with Article 87 (c),(d) and (h) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. This information is necessary for the performance of tasks carried out by Frontex in accordance with Art. 10 (1)(a)(f) of REG (EU) 2019/1896. Personal data is processed related to data subjects as name, surname, photo, telephone number, e-mail address. The personal data is retained for administrative purpose (managing access rights in the JORA system) and kept for 12 months after the user is deactivated from the Frontex systems. Frontex internal users' account are deactivated automatically at the end of their contracts with the Agency. External users' accounts are deactivated automatically 120

	days after the last successful login to the Frontex IT environment. After this period the personal data are deleted. In accordance with Regulation EU 2018/1725 of 23 October 2018, the data subjects have the right to access their personal data (Art. 17), to exercise the right to rectification (Art. 18), to obtain of erasure of personal data concerning him or her (Art. 19), to restrict of processing of his or her personal data and have the right to data portability (Art. 22). There is no automated individual decision-making or profiling when personal data is processed during access rights management to the JORA system. The Head of IFC of Frontex is the Controller of the processing of the data hoo.ifc@frontex.europa.eu . Requests of data subjects should be directed to jora@frontex.europa.eu . Any question with regard to the processing of personal data may be forwarded also to the Frontex Data Protection Officer (DPO) at dataprotectionoffice@frontex.europa.eu . Any request to either the Controller or the DPO which is not related to data protection and the exercise of the rights granted under Regulation 2018/1725 will not be responded to.

v. Data security

ORGANISATIONAL MEASURES		
JORA system is LIMITED. JORA system is part of Frontex applications and systems benefiting from ICT policies and security measures.		
TECHNICAL MEASURES		
	Check (Yes/No)	Description (if Yes)
Pseudonimysation or encryption	☐/☒	Click or tap here to enter text.
Measures to ensure:		
▪ Confidentiality of data	☒/☐	Confidentiality is achieved in JORA application by authentication and authorization (using ADFS claims) and Attribute-based access control (ABAC), an extension of Role-based access control, to access the resources of the application. JORA system administrators and access managers are having access to the personal data of data subjects according to the need-to-know bases and based on formal access authorization.
▪ Integrity of data	☒/☐	Data integrity is enabled by the chosen database management system, SQL Server, by the following 3 integrity constraints: entity integrity, referential integrity and domain integrity.
▪ Availability of data	☒/☐	Information is available 24/7. A SLA between IFC and ICT in in place to guarantee the availability. JORA system is constantly being monitored to detect downtimes. The personal data of the data subjects are available for administrators and for JORA system access managers based on formal authorization.
▪ Resilience of systems and services	☒/☐	ICT guarantees a high level of resilience of JORA System by monitoring activities.
Restoration of availability and access to personal data in a timely manner	☒/☐	ICT guarantees the restoration with regular backups according to Frontex ICT backup policy.
Process for testing, assessing and evaluation of the effectiveness the measures	☒/☐	IFC performs regression tests on a monthly basis. ICT conducts periodically penetration tests.
LEGAL BASIS		
	Check (Yes/No)	
For the performance of a task carried out in public interest or under Frontex Regulation	☒/☐	*Please name the task:* Point (a), (c) and (h) of Article 87 (1) of EBCG Regulation EU 2019/1896
For complying with a legal obligation upon the Unit/Agency		*Please specify the legal obligation:* Point h) of Article 87 (1) of EBCG regulation (collecting of personal data for administrative purposes)
For contractual reasons of the data subject	☐/☒	Not applicable.
The data subject has given consent for one (or more) purposes as listed above	☐/☒	*Please explain how the consent is gathered:* Point h) of Article 87 (1) of EBCG regulation (collecting of personal data for administrative
For protecting the vital interests of the data subject	☐/☒	*Please specify:* Data subjects are cooperating with Frontex according to point (a), (c) and (h) of Article 87 (1) of EBCG Regulation EU 2019/1896

Date:

Data Controller

Signature:

List of attachments or hyperlinks: