(To be filled out in the EDPS' office)
REGISTER NUMBER: 1301

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 17/04/2015

CASE NUMBER: 2015-0346

INSTITUTION: FRONTEX

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001([1])

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER

HEAD OF RISK ANALYSIS UNIT (RAU)
FRONTEX
PLAC EUROPEJSKI
00-844
WARSAW POLAND

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

The Risk Analysis Unit (RA U).

All processing will take place at the Frontex headquarters in Warsaw, Poland with no possibility for teleworking, and no processing will be sub-contracted to a third party.

3/ NAME OF THE PROCESSING

Processing of Personal Data for Risk Analysis (PeDRA), operating under Article 11c of the Frontex regulation.

4/ PURPOSE OR PURPOSES OF THE PROCESSING

According 10 the Frontex Regulation (Article 11c 3), Frontex may only process personal data collected by Member Stales during Frontex coordinated Joint Operations, pilot projects and rapid interventions for the following two purposes:

[1] OJ L 8, 12.01.2001.

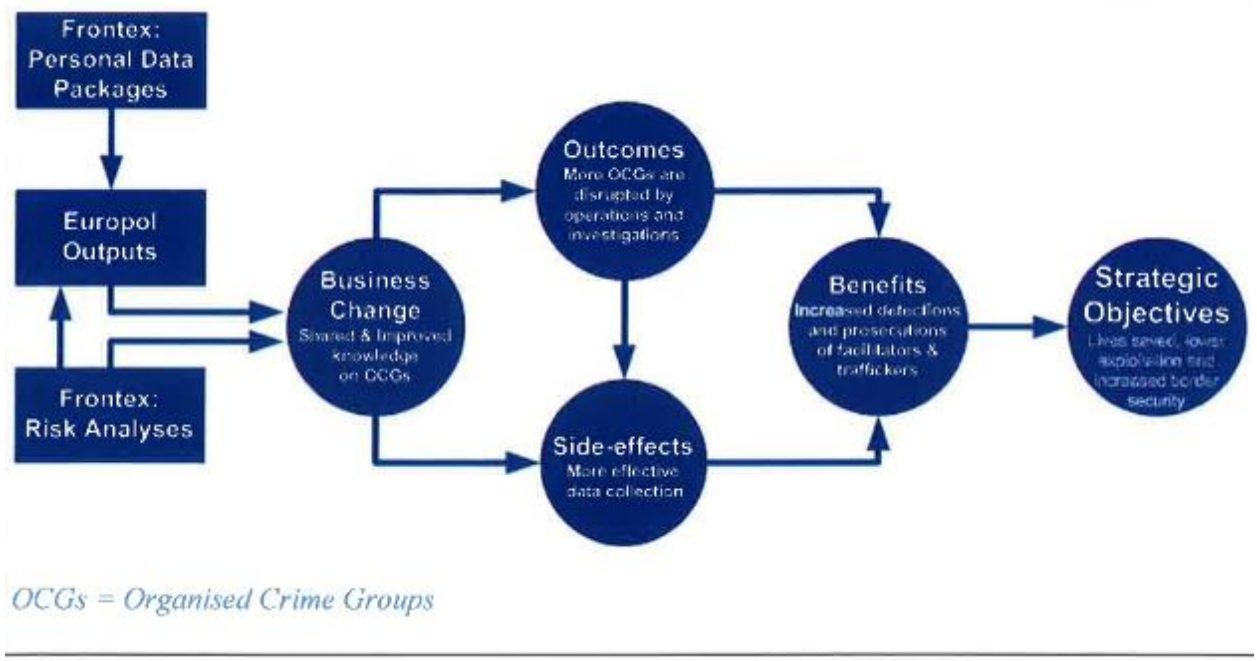
[2] **Please attach all necessary backup documents**

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 shall be depersonalised.

Please refer to product descriptions Annexed to the PeDRA Business Case (v4) for more information on these two PeDRA outputs.

These PeDRA outputs will contribute to the following strategic objectives: reducing loss of life at sea, reducing the risk of exploitation of vulnerable groups and increasing border security. 1n these terms, the measureable benefits from PeDRA will be increased inhibitions, detections and arrests of facilitators, traffickers and cross-border criminals made possible by a more effective operational response at the border (Front ex) and more successful investigations (Europol).

The relationship between the outputs, outcomes and benefits is expanded in more detail in the PeDRA Business Case (v.04).



5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

Consistent with Article 11c (2) of the Frontex Regulation, the data subjects will be persons suspected on reasonable grounds by the competent authorities of the Member States, of involvement in facilitation of illegal migration, human trafficking or other cross-border criminal activities.

The data subjects themselves will not be providing any personal data, rather information relating to the data subjects will be collected by Member States from, inter alia, recently arrived migrants and other sources originating from routine border control and operational activities. Such personal data are already routinely collected by Member States.

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA
(including, if applicable, special categories of data (Article 10) and/or origin of data)

As far as possible the processed personal data will conform to the Universal Messaging Format and will include categories such as:

a) Name(s) of subject
b) Gender
c) Nick name
d) Nationality (ies)
e) Names of known accomplices
f) Organised crime group
g) Registered business
h) Personal address
i) Safe house address
j) Means of communication (telephone, social media handle)
k) Means of transportation (vehicle registration, boat name)
l) Weapon
m) Photograph(s)
n) Non-offence event
o) Offence event
p) Ethnicity of subject
q) Sexual orientation

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

Member State representatives are not normally in contact with the data subjects. This is because data subjects are suspects of criminal activity usually operating in third countries. Migrants, who remain anonymous, are the main data providers, and they are informed of the use of any personal data they are providing. Collection of personal data takes place under the national data protection regulation of the hosting Member State.

Frontex is not permitted, according to its Regulation, to conduct investigations. Therefore Frontex will make no attempt to contact the data subjects.

Data subject's rights pursuant to Article 13 will be assessed on a case-by-case basis but exemptions such as Article 20 I (a) are expected to apply as the personal data will further processed for the prevention, investigation (by Europol), detection and prosecution (by Member States) of criminal offences.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS
(Rights of access, to rectify, to block, to erase, to object)

The rights of access, rectification, blocking, erasure, and objection are going to be limited in the light of Article 20 exceptions, especially as data subjects are limited to those individuals suspected of criminal activity.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

Processing will be mainly automated but occasionally manual, especially during early developmental stages of the project.

The flow of personal data and processes are as follows:

1. Personal data are collected by Member State representatives during Frontex coordinated operational activity. Guidelines and business justifications for PeDRA are provided to Member States at the beginning of the operation in the form of an operational plan, as per Article 3a of the Frontex Regulation.
2. Personal data are collected by Guest Officers, deployed from various Member States to the operational area and operating under the national data protection regulation of the hosting Member State.
3. Personal data will be transmitted by a single point of contact (Hosting Member State - Intelligence Officer) in each Joint Operation to Frontex using a secure web application (.Joint Operation Reporting Application - hereafter JORA).
4. Transmissions received by Frontex will be automatically authenticated in terms of checking the source and structure of each transmission
5. Transmissions that pass the Authentication are made available to PeDRA Analysts in the Risk Analysis Unit and temporarily kept in an isolated location in the JORA database until the legality check is completed.
6. Personal data will be opened and subject to a legality check (correct data subjects, collected during an operation etc.), which will be conducted by a PeDRA Analyst in the web application (JORA).
7. Personal data that pass the legality check will then be stored in JORA database, separated from other non-personal operational and statistical data collected in the same system
8. Personal data that fail the legality check will be temporarily stored until the legality is confirmed. During this process Frontex may ask the hosting Member State for additional information regarding their legality. The decision to processes personal data is retained by Frontex.
9. PeDRA Analysts process personal data to form Personal Data Packages (PDP5) to meet the needs of recipient union agencies, for example Europol.
10. PeDRA Analysis use personal data to form risk analyses, the results (lj which are depersonalised
11. PDPs are transmitted to Europol via a secure channel (SIENA), while risk analyses are disseminated to regular consumers of Frontex depersonalised risk analysis products
12. After maximum of 3 months from the final validation check, personal data and all backups are Deleted from the PeDRA file management system
13. Personal data and logs of all processing are transferred to an inert encrypted archive for historical and audit purposes. Access to the archive will be limited to the controller and the data protection officer upon specific and strictly controlled circumstances (to be arranged). The erasure of inert encrypted archive will be supervised by data protection officer (the data and log files will be archived for a limited time only 2-3 years and it will be revised on yearly basis).
14. All processing will be automated and will be electronic. Some manual processing might be implemented but automated processing is the general principal of personal data processing.

More information can be found in the Business Requirements Document (BRD) and the technical proposal document jar JORA.

10/ STORAGE MEDIA OF DATA

Personal data files will be temporarily stored prior to having passed the legality check and can be easily rejected and erased if they don't pass the legality check.

JORA system will allow the PeDRA analysts to store the legally checked daily report files in JORA database and make it available only for PeDRA Analysts.

All files will be stored in a secured Frontex ICT environment and any use of data or other physical media while printing/exporting functionality will only be available for the PeDRA Analysts - any printed personal data will be shredded at the end of each day according to a strict clean-desk policy. PeDRA Analysts will not be permitted to take personal data (printed or electronically stored) out of the Frontex premises.

Storing of personal data will only be available to PeDRA Analysts and every access to the data will be logged by system in log files (read, close and store).

Expired data (date of final validation check + 3 months) will be removed from PeDRA file management and JORA system and sent to the inert encrypted archive. The data in inert encrypted archive will made available to controller and the data protection officer on request.

Reading, copying, alternation or removal of storage media will be available to authorized personnel only.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

The specific legal basis for processing of personal data in the PeDRA project is Article 11c of Frontex Regulation.

All processing will be done in full compliance with the Frontex Regulation (Council Regulation (EC) No 200712004 of 26 October 2004, OJ L 349101, 25.11.2004, as last amended) and the Data Protection Regulation (EC) 45/2001. This legal framework is supplemented by Frontex internal rules related to processing of personal data.

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

Personal data will be transmitted on a case-by-case basis 10 Europol or other Union law enforcement agencies in the form of Personal Data Packages (PDPs). Such transmissions will be subject to specific working arrangements.

The recipient agencies (only transmissions to Europol are foreseen at the present stage of the project) will be required to provide business justifications for the personal data and feedback on its efficacy.

More details can be found in the Business Case for transmission of personal data to Europol.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

Personal data will be used for both transmission to Europol and for Frontex risk analyses and then finally deleted no later than three months after the data are received in Frontex

Once PDPs have been transmitted to Europol or other law enforcement agencies, there may be the need 10 clarify details during subsequent judicial proceedings. Therefore there is the need to keep the processed personal data beyond its expiry date (3 months) in an inert archive away from the operational area. Access will be limited to the controller and the data protection officer and only in limited set of predetermined circumstances (to be agreed). The data in that archive will not be anonymised as it will be necessary to identify the exact individual during criminal proceedings.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS *(Please, specify the time limits for every category, if applicable)*

N/A

14/ HISTORICAL, STATISTICAL OR SCIENTIFIC PURPOSES
(*If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification)*

N/A

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Frontex is not permitted to transmit personal data to third countries or international organisations.

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING *(Please describe)*

AS FORESEEN IN:

☒ Article 27.2.(a)
(Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,)

The processing will include data of persons suspected of involvement in cross-border criminal activities, facilitating illegal migration or human trafficking (Art. 27.2 a) of the Reg. 45/200/).

☐ Article 27.2.(b)
(Processing operations intended to evaluate personal aspects relating to the data subject,)

☐ Article 27.2.(c)
(Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,)

☐ Article 27.2.(d)
(Processing operations for the purpose of excluding individuals from a right, benefit or contract)

☐ Other (general concept in Article 27.1)

17/ COMMENTS

No processing of personal data is currently taking place under PeDRA.

A Pilot Exercise will be launched once Prior Checking has been completed. This Pilot Exercise will focus on a limited range and volume of personal data to test procedures, and will be followed by a staggered roll out to all Joint Operations.

PLACE AND DATE: WARSAW, POLAND, 14/04/2015

DATA PROTECTION OFFICER: ANDRZEJ GRAŚ

INSTITUTION OR BODY: FRONTEX