

From: [REDACTED]
To: European Data Protection Supervisor
<EDPS@edps.europa.eu>
[REDACTED]
CC: [REDACTED]
[REDACTED]
Sent at: 15/04/15 20:48:52
Subject: Notification for prior checking from Frontex regarding PeDRA project

Dear Mr Buttarelli,

Please find attached a Notification for prior checking regarding PeDRA project.

That case has been already consulted with your staff as an Article 46(d) consultation. The case number was **2014-0978**.

The Notification is accompanied by a cover letter of the Frontex Executive Director Mr Leggeri, and few attachments to the Notification.

This set of documents has been sent to you by post today.

Depending on the content of your future prior-checking opinion, Frontex will deliver you the final version of the operational Implementing Measures for PeDRA for consultation in line with Art. 11a of the Frontex Regulation. We also understand that prior checking also covers the changes that we need to make to our ICT systems so that they can accommodate the processing of personal data and that we are unable to progress with these changes until the prior checking has been finalised.

I take this opportunity to thank you for a successful cooperation at the staff level with the members of your Prior Checks and Consultations' team.

Yours

[REDACTED]
[REDACTED]
[REDACTED]

FRONTEX

www.frontex.europa.eu

Plac Europejski 6, 00-844 Warsaw, Poland · Tel: +48 22 205 9500 · Fax: +48 22 205 9501

DISCLAIMER: This e-mail message, including any attachments, cannot be construed as automatically constituting any form of commitment by Frontex, unless its contents clearly indicate otherwise. It is intended solely for the use of the addressee(s). Any unauthorised disclosure, use or dissemination, either in whole or in part, is prohibited. If you have received this message in error, please notify the sender immediately via e-mail and delete the e-mail from your system.

Mr Giovanni BUTTARELLI
European Data Protection Supervisor
Rue Wiertz 60 - B - 1047 Brussels

Subject: EDPS' prior checking of the PeDRA project

Your ref: GB/OL/sn/D(2015)0464 C 2015-0129
Our ref: /14.04.2015 5961/15.04.2015
Please quote when replying

Warsaw, 14 April 2015

Dear Mr Buttarelli,

I write in reference to Article 11c of the Frontex Regulation and Frontex's plans to apply it in line with the relevant data protection rules. First of all, thank you kindly for your prior approval of the draft working arrangement with Europol, expressed in your letter of 24 March 2015.

Secondly, this letter and the attached documents represent the submission of a formal Notification of the intent of Frontex to further process personal data collected by Member States, whereby the data subjects will be suspects of criminal activity as per Article 11c (2) of the Frontex Regulation. Recent events in the central Mediterranean resulting in substantial loss of life, reinforce the priority for law enforcement agencies at the EU level to process and exchange personal data relating to the perpetrators of such crimes. As you will know there has already been much work done, both by Frontex and the EDPS towards to implementation of this activity, including:

- a successful period of consultation between Frontex and the EDPS on the draft Notification sent to you for consultation in December 2014,
- drafting of new working arrangement between Frontex and Europol that was recently approved by the EDPS,
- initial consultation on the future *operational* Implementing Measures for PeDRA to be adopted by our Management Board (MB) once approved by the EDPS.

The Processing of Personal Data for Risk Analysis (PeDRA) was launched in Frontex in mid 2014 with Stage 1 focussed on preparing this Notification. The documents attached to the Notification include the business case, business requirements documentation and a proposal for a technical solution for the exchange and processing of personal data. All of these documents have already been reviewed by your team and discussed in detail with the PeDRA team here in Frontex. It is on this basis that we are led to believe that there are currently no major obstacles for a swift prior-checking, but if there is any more information you need we have staff ready to reply post haste.

I take this opportunity to assure you that Frontex will in no case start processing operational personal data under PeDRA project before at least following four conditions are met:

- Working Arrangement signed and placed on our website for transparency purposes;

- Memorandum on adequacy (Art. 9 of the Data Protection Regulation) adopted by our DPO;
- Prior checking procedure regarding the attached Notification completed positively;
- Operational Implementing Measures for PeDRA drafted, agreed with EDPS and formally adopted by the MB.

Depending on the content of your future prior-checking opinion, Frontex will deliver you the final version of the operational Implementing Measures for PeDRA for consultation in line with Art. 11a of the Frontex Regulation. That future prior-checking may also influence the final shape of the ICT solutions to be applied. In case of any fine tuning, you will be updated accordingly.

Regarding the new *administrative* Implementing Rules, which have been also pre-consulted with your staff members, please be informed that these draft rules are not part of the PeDRA project since they are going to cover horizontally all data processing operations in Frontex. Therefore, they will be sent to you for your final approval separately in few days.

When publishing our Notification for prior-checking on your website, please kindly eliminate personal data present there.

Last but not least let me kindly express my wish to take the earliest opportunity to meet you personally in Brussels, probably in May.

Yours sincerely,



Fabrice Leggeri
Executive Director

c/c:

- EC, DG Home
- Management Board of Frontex

Annex:

- Notification for prior checking for PeDRA project, signed by the Frontex DPO;
- Attachments to the Notification:
 - o PeDRA Business Case for PDPs to Europol;
 - o PeDRA Business Case v4;
 - o PeDRA Business Requirements Document;
 - o PeDRA Technical Proposal - JORA).

(To be filled out in the EDPS' office)

REGISTER NUMBER:

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION:

CASE NUMBER:

INSTITUTION:

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

INFORMATION TO BE GIVEN²

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 (RAU).

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

¹ OJ L 8, 12.01.2001.

² **Please attach all necessary backup documents**

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

4/ PURPOSE OR PURPOSES OF THE PROCESSING

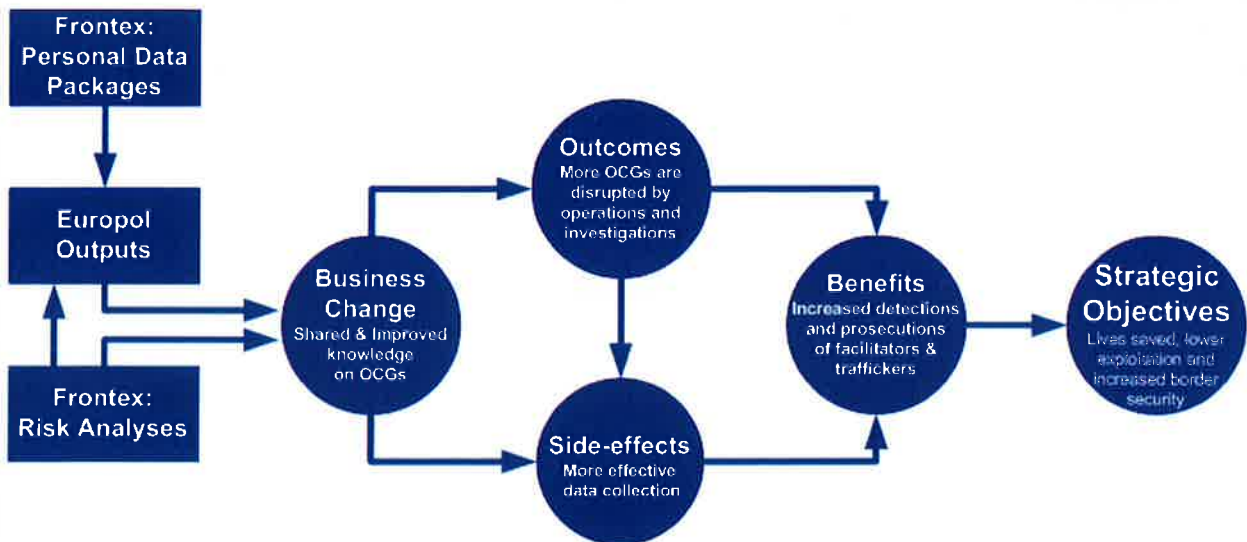
According to the Frontex Regulation (Article 11c 3), Frontex may only process personal data collected by Member States during Frontex coordinated Joint Operations, pilot projects and rapid interventions for the following two purposes:

- 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 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. In 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 (Frontex) 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).



OCGs = Organised Crime Groups

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 1(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:

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 be made available to controller and the data protection officer on request.

Reading, copying, alteration 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 2007/2004 of 26 October 2004, OJ L 349/01, 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 to 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 to 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

n/a

(Please, specify the time limits for every category, if applicable)

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*):

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. 45/2001).

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.

18/ MEASURES TO ENSURE SECURITY OF PROCESSING³ :

Please check all points of Article 22 of Regulation (EC) 45/2001

(a) Prevention of any unauthorised person from gaining access to computer systems processing personal data;

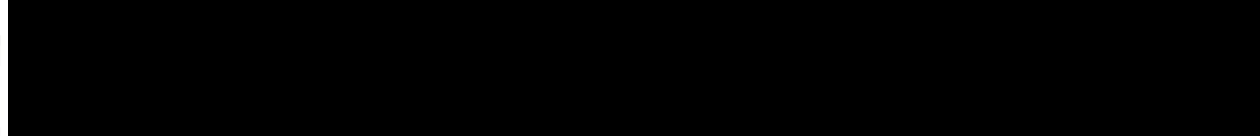
³ Not to be published in the EDPS' Register (Art. 27(5) of Regulation (EC) N°: 45/2001)



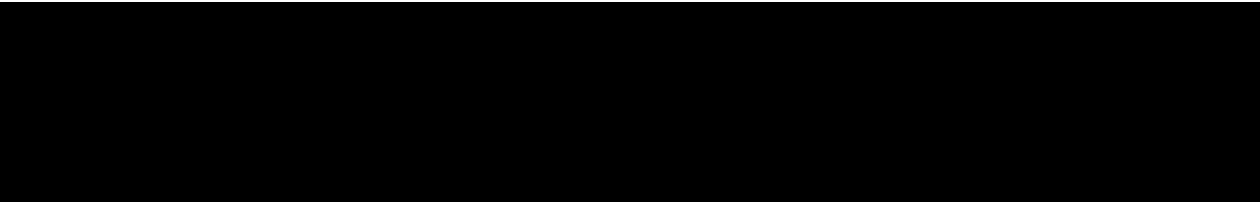
(b) preventing any unauthorised reading, copying, alteration or removal of storage media;

Storage media data will be protected against unauthorized access while copying of data to removal media will be disabled.

(c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;




(d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities;



(e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers;



(f) recording which personal data have been communicated, at what times and to whom;



(g) ensuring that it will subsequently be possible to check which personal data have been processed, at what times and by whom;

(g) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body;

(i) ensuring that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation;

Personal data communication will be encrypted and transferred through a secure data channel. For this purpose a VPN connection is foreseen between the transmission stations.

(j) designing the organisational structure within an institution or body in such a way that it will meet the special requirements of data protection.

Internal organisational (human resource, policies and procedures) measures will be adopted to govern, structure and enable the processing of personal data. A Pilot Exercise will address this development on a small scale and in a more controlled environment.

PLACE AND DATE:

DATA PROTECTION

INSTITUTION OR BO



(To be filled out in the EDPS' office)

EDPS OPINION

OF DATE:

CASE NUMBER:

(To be filled out in the EDPS' office)

FOLLOW UP *(in case of acting measures to be taken)*

Warsaw, 03 September 2014
File n°: Final

PeDRA

Business Case for transmission of personal data to Europol



Executive Summary

The purpose of the Business Case for onward transmission of personal data to Europol from Frontex is to provide an overview of the PeDRA project and to furnish Europol with the basic information needed to prepare to become a recipient of personal data from Frontex coordinated operational activity and to establish a basis for the assessment of the project success.

Following the 2011 amendment to the Frontex Regulation (EC) 2007/2004¹, the agency now has a legal basis to further process personal data in the operational sense² – but only personal data collected by Member States during or in the context of Frontex coordinated operational activities, and only data relating to persons suspected by Member States on reasonable grounds of involvement in facilitation, THB or CBC. Such data may be generated by migrant interviews, mobile forensics or confiscated documents.

The PeDRA project aims to contribute to the strategic objectives of preventing loss of life, reducing the risk of exploitation of vulnerable groups and increasing the border security and the internal security of Member States by combating cross-border crime. The measurable benefits from the onward transmission of personal data to Europol will be increased investigations and prosecutions of facilitators, traffickers and cross-border criminals because of a more effective operational and investigative response by Europol.

Consistent with Prince2® methodologies, the approach of PeDRA is to focus on deliverables. Frontex will generate from the personal data two distinct and legally mandated deliverables. Firstly, personal data will be used for risk analysis, the results of which shall be depersonalised and disseminated via regular channels. In addition personal data will also be transmitted to Europol on a case-by-case basis, together with necessary contextual information.

In addition to the products produced by Frontex it is expected that Europol will generate outputs based on the transmitted personal data. Upon receipt of personal data from Frontex, Europol will presumably embark on its own analytical processes to produce its own deliverables which will, in line with data protection principles, need to be described and agreed upon in advance. These may be tangible and widely disseminated deliverables in terms of analytical reports, or less tangible in terms of summary descriptions of the use of the data or support for investigations or operational activities. In any case Europol deliverables will be fed back to Frontex in depersonalised formats for measuring project benefits and maintaining a continued business justification.

The project is scheduled to take three years in stages that are characterised by increased sources, volume and complexity of personal data transmitted by Member States, and by an increase in the automization of the personal data filing system. The project approach in Stage I is to first work towards overcoming the project dependencies, such as producing new implementing rules, a new working arrangement with Europol, producing a technical proposal for the reporting platform, and drafting and operational plan in cooperation with Member States. Once these tasks have been completed, all the necessary paperwork will be submitted to the European Data Protection Supervisor for prior approval, a process that can take up to a year from

¹ EC 1168/2011

² As opposed to administrative functions, and also to a limited extent in Eurosur which is in any case covered by separate legislation

the moment of application. After approval has been granted the documentation will be put before the Frontex Management Board for adoption.

First, a Pilot exercise will involve a pre-existing data-stream (migrant interviews) from a limited number of Member States hosting Frontex operations. Transmissions will be authenticated and the content will be subject to a legality check by Frontex, so that any data that is not permitted by the Frontex regulation will not be accepted into the PeDRA file management system.

The unstructured, qualitative interview reports, which usually come in PDF or MS Word formats, will be categorised according to source and content and will be complemented with contextual information, relevant analytical products and statistical data before onward transmission to Europol in the form of Personal Data Packages (PDPs). It is acknowledged that this should take place quickly and efficiently, and it is not foreseen that any data will be withheld by Frontex.

Stages II and III will involve an expansion in terms of data complexity to also potentially include mobile forensics and fraudulent documents, and also an expansion in terms of data sources to include all Frontex joint operations.

Table of Contents

Executive Summary	3
1. Purpose of the document	6
2. Background and current situation	6
3. Project Description	6
3.1. <i>Objectives</i>	6
3.2. <i>Scope</i>	6
3.3. <i>Exclusions from the scope</i>	8
3.4. <i>Project Approach</i>	8
3.5. <i>Timescale and Milestones</i>	12
4. Stakeholders	14
4.1. <i>Stakeholder analysis</i>	14
5. Benefits	16
6. Project Organisation	18

1. Purpose of the document

The purpose of the Business Case for onward transmission of personal data to Europol is to provide an overview of the overall PeDRA project, provide the basic information needed for Europol to prepare to become a recipient of personal data from Frontex, and establish a basis for the assessment of the overall success. It forms the agreement between the PeDRA project management team and counterparts in Europol.

2. Background and current situation

Following the 2011 amendment to the Frontex Regulation (EC) 2007/2004³, the agency now has a legal basis to further process personal data in the operational sense⁴ – but only data collected by Member States during or in the context of Frontex coordinated operational activities, and only personal data relating to persons suspected on reasonable ground of involvement in facilitation, THB or CBC.

Such personal data are only to be used for two specific purposes: 1) risk analyses on Frontex and 2) to produce PDPs for transmission to Europol or other Union law enforcement agencies. This document refers to the onward transmission of personal data to Europol.

3. Project Description

3.1. Objectives

The PeDRA project aims to contribute to the strategic objectives of preventing loss of life, reducing the risk of exploitation of vulnerable groups and increasing the border security and the internal security of Member States by combating cross-border crime. The measurable benefits from the onward transmission of personal data to Europol will be increased investigations and prosecutions of facilitators, traffickers and cross-border criminals because of a more effective operational and investigative response by Europol.

These Strategic Objectives shall be worked towards in a series of activities separated into work streams, delivered in a multi-stage project. The focus will be on the products and deliverables which will contain the personal data relating to individual suspected of facilitation, THB or BSB to create business changes. The activities will empower Member States to securely transmit to Frontex, relevant and pre-agreed personal data collected during or in the context of Frontex coordinated operations, and for Frontex to store, analyse at the EU level and disseminate the personal data in strict accordance with its mandate and commitment to the principles of data protection and preservation of human rights.

At the functional level, the PeDRA project is the mechanism that is being put in place to implement Article 11c of the Frontex Regulation which empowers the Agency to further process a limited range of personal data collected by Member States.

3.2. Scope

This section outlines the exact scope of the overall PeDRA Project. The scope is strictly limited by the Frontex Regulation but has been drafted from the perspective of

³ EC 1168/2011

⁴ As opposed to administrative functions, and also to a limited extent in Eurosur which is in any case covered by separate legislation

business needs of Frontex and Europol. The spirit of data protection legislation is that the only processes that are allowed are those that are explicitly permitted – hence the popular principle of ‘whatever is not forbidden is allowed’ does not apply here.

According to Article 11c paragraph 1 of the Frontex Regulation, Member States⁵ are permitted to transmit to Frontex personal data collected during or in the context of joint operations, pilot projects and rapid interventions. Hence, Frontex itself will not be collecting any personal data whatsoever, instead data collection will be the sole responsibility of the Member State, who will take a decision to transmit to Frontex.

Data can only be transmitted to Frontex if they are collected both during and in the context of Frontex operational activity. In some circumstances it could be foreseen that relevant data collected away from the operational area may be legally transmitted to Frontex if it can be shown that the data were collected during and in the context of the operation - as stated in the regulation.

According to Article 11c paragraph 3, personal data shall be further processed by the Agency only for the two following purposes, which correspond exactly with the analytical activities and the outputs of the project:

- (a) the transmission, on a case-by-case basis, of personal data to Europol or other Union law enforcement agencies
- (b) the use of personal data for the production of risk analyses, the results of which will be depersonalised

Box 1 The two legally-bound outputs (deliverables) of the PeDRA Project (article 11c para 3.)

Because of the strict usage limitations, from a legal perspective Frontex shall not use personal data for other purposes, such as situational awareness, nor will it be possible for the agency to receive personal data collected out of context of Frontex coordinated activities, or relating to data subjects other than those identified in Article 11c.

According to Article 11c paragraph 2, data subjects should be limited to persons who are suspected, on reasonable grounds, by the competent authorities of the Member States of involvement in cross-border criminal activities, in facilitating illegal migration activities or in human trafficking activities. If the reasonable grounds is not immediately apparent to Frontex, the PeDRA team will request from the sending Member State justification for the data transmission.

According to Article 11c paragraph 5, the processing of such personal data shall respect the principles of necessity and proportionality. The personal data shall not be used by the Agency for the purpose of investigations, which remain under the responsibility of the competent authorities of the Member States.

According to Article 11c paragraph 5 the processing of such personal data shall be limited to those data that are required for the two activities and outputs listed above.

⁵ Hosting or participating

3.3. Exclusions from the scope

The principle of what is not forbidden is allowed is not applicable in the context of data protection legislation. Hence the scope is limited to what is specifically permitted in the Frontex Regulation and the Data Protection Regulation.

According to Article 11c (5) personal data will not be used by the agency for the purpose of investigations. Also prohibited in the regulation is the onward transmission or other communication of personal data processed by the Agency to third countries or other third parties.

Personal data collected under PeDRA cannot legally be used for any other purposes except for risk analyses and onward transmission to Europol.

Any personal data sent to Frontex from other sources (EU delegations, private or anonymous sources) will not be processed under the PeDRA project, as it comes from outside of Frontex joint operations and therefore cannot be legally used for risk analysis or to transmit to Europol.

3.4. Project Approach

The PeDRA Project Approach is to focus on products (which are the outputs or deliverables of the project) and the business changes, outcomes and benefits that the products will enable, create or contribute to. Hence the *raison d'être* of the PeDRA is to produce effective and targeted products that will support Frontex, Member States and Europol⁶ in the fight against facilitation, THB and other cross-border crimes.

The following section contains information on the project structure i.e. the different stages of the project, and within each stage of the project the different work streams (WS) are highlighted.

Structure

This document refers to the overall PeDRA Project, which is expected to run for 3 years, from 2014 to 2016. However, in the interests of time, in March 2014 Stage I was already launched as a lean project known as the PeDRA Pilot which is just the first year of the overall PeDRA Project, as illustrated in Figure 1.

⁶ and other union law enforcement agencies, but subject to data protection principles of necessity and proportionality, specific working arrangements and prior authorisation from EDPS

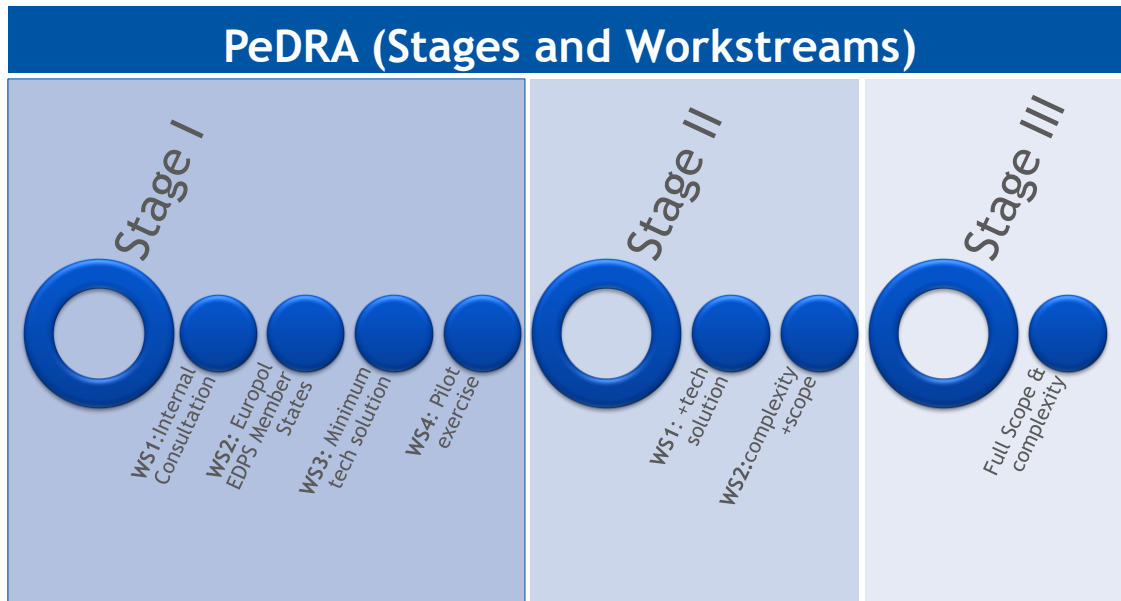


Figure 1 The currently on-going PeDRA Stage I represents the first of three stages of the overall PeDRA Project. Each stage is characterised by increasingly sophisticated technical solutions, data complexity and scope. Stage I will conclude after the Pilot Exercise, currently planned for Q2 2016

STAGE I (2014-15)

Stage I of the project has four work streams (WS) as follows:

WS1 Internal Consultation Process - RAU.

Each Unit in Frontex has been consulted by RAU through a series of formal discussions to clarify the details of the mandate, as well as roles and responsibilities for the work streams.

WS2 Create administrative products

- a) New WA with EUROPOL: Any exchange of personal data with Europol must be covered by a new, specific working arrangement. Negotiations are already underway to produce a new working arrangement between Europol and Frontex, which will contain the possibility to share personal data between the agencies.
- b) Draft Operational Plan: A working group is being formed with Member States to oversee planning of reporting personal data from joint operations. A draft Operational Plan will be created for use in Frontex operations from which personal data will be transmitted.
- c) New Implementing rules: New implementing rules need to be drafted which accommodate PeDRA and outline the new roles and responsibilities of the Controller and the DPO.
- d) EDPS: All documentation will need to be submitted to the EDPS for Prior Approval. This process can take a year from the moment of application.

WS3 Design and Installation of minimum technical requirements (MTR)

In the scope of pre-project activities aiming at facilitating the design of this project, work has been done to identify the personal data that will be exchanged in the context of the Pilot Exercise and this information is being documented for the technical stakeholders (ICT) to provide the following solutions:

- i. reporting platform from the operational area
- ii. secure transmission to Frontex
- iii. authentication
- iv. legality check
- v. storing
- vi. analysis
- vii. secure transmission to Europol

There is a consensus to use pre-existing platforms wherever possible rather than designing a bespoke solution. Options include using SIENA or the Eurosur network (not the platform) or even producing a secure e-mail system.

A business requirements document (BRD) has been produced which contains use cases and business rules and a data model has been created.

WS4 Design, launch and review of a pilot exercise

The Pilot exercise will be deployed once all four dependencies have been resolved. The scope of the Pilot Exercise is to be decided but will focus migrant interviews, and on the collection and transmission to Frontex of personal data in order to test the technical solution in place.

STAGES II & II (2015-2016)

The PeDRA Project is characterised by successive waves of increasingly sophisticated technical solutions and transmitted data. In contrast the analytical outcomes will be launched in their completed form but based on reduced scope data during the early stages of the project.

WS1 Gradual development of technical solutions

For the Pilot exercise much of the technical solution is expected to be bare minimum and much of the processing will be manual rather than automatic. In successive waves of increased complexity the technical solution will be expected to become more automated. Nevertheless, even at the very first stage all the principles of the data protection legislation will need to be complied with and so from that perspective the minimum technical solution for the Pilot exercise will already have to satisfy the EDPS that data securing and suitable access management is in place.

WS2 Increased complexity of transmitted data

Once the technical solution has been tested during the Pilot Exercise there will be the possibility to extend the data collection to include other data streams such as mobile forensics and documents discarded in boats etc.

WS3 Analytical outcomes

Consistent with Prince2® methodologies, the approach of PeDRA is to focus on deliverables. Frontex will generate from the personal data two distinct and legally mandated deliverables. Firstly, personal data will be used for risk analysis, the results of which shall be depersonalised and disseminated via regular channels. These risk analyses will focus on the names, and activities of organised crime groups involved in facilitation, THB and other CBCs.

In addition, personal data will also be transmitted to Europol on a case-by-case basis, together with necessary contextual information. Europol will then embark on its own analytical processes to produce its own deliverables which will, in line with data protection principles, need to be described in advance. These may be tangible deliverables in terms of analytical reports, or less tangible in terms of support for investigations or operational activities. In any case Europol deliverables will be fed back to Frontex in depersonalised formats for measuring project benefits and maintaining a continued business justification.

Output 1: Risk analyses

The personal data will be used to produce risk analyses, the results of which will be depersonalised. The risk analyses will inevitably focus on the names, structure, *modus operandi* and operational areas of organised crime groups involved in facilitation, THB and other cross border crimes.

As the results of the risk analyses will be depersonalised they may well be included as chapters in other regular reports or they may represent a new regular product. The reports are likely to be classified but they may be distributed using Frontex standard channels.

Output 2: Personal-data packages

Personal data will be transmitted to Europol in the form of personal data packages (PDPs) containing not only personal data (raw and processed) but also contextual information needed to interpret the personal data. Contextual information will include statistical data relating to detections in the area of question, recent risk analyses, and any other supplementary information needed to interpret the personal data such as nationalities, *modus operandi*, locations etc.

According to the Frontex regulation transmissions to Europol will take place on a case by case basis which is to say, not systematically or automatically but following a decision in line with data protection principles of proportionality and necessity.

Although the regulation states that other union law enforcement agencies may also receive personal data from Frontex, it is foreseen that Europol will be the main recipient of PDPs.

These reports will need to be transmitted to Europol via a secure channel, mostly likely SIENA which has already been installed in Frontex. The skills exist in RAU to produce such cases but expected time costs for processing data and producing cases are expected to be high.

As well as the two Outputs from Frontex it is expected that outputs will also be generated by Europol based on the personal data transmitted by Frontex.

Output 3: Europol products/reports/feedbacks

In the interests of measuring benefits and maintaining a continued business justification of the transmission of personal data, use of the data in Europol will need to be documented and regular outputs produced. These may include analytical reports on facilitation⁷, THB or cross border crime, or they may be summary documents to show how and where the personal data were used in analytical processes, and to support operational and investigative activities.

In the absence of such products, it will be problematic to measure benefits and a continued business justification for the transmission of personal data will be difficult to maintain.

3.5. Timescale and Milestones

With four external dependencies each with its own independent timescale, and the influence of an unfamiliar external regulator EDPS who will oversee the Pilot exercise as well as two of the external dependencies, producing a realistic timeline is a difficult exercise.

The PeDRA milestones, which can also be seen on Figure 2, are as follows:

1. Completion of the Internal Consultation Plans and Project planning (end 2014)
2. Formation of working group with MS (end 2014)
3. Addressing the external dependencies which need to be overcome before the Prior checking can be submitted (end Q1 2015)
4. Gaining Prior approval from EDPS (end 2015)
5. Procuring and installing technical solution (end Q1 2016)
6. Launch of Pilot Exercise (Q2 2016)
7. Launch of Stage II (Q2 2016)
8. Launch of Stage III (Q4 2016)

⁷ EUROPOL REPORT: FACILITATED ILLEGAL IMMIGRATION INTO THE EUROPEAN UNION September 2009

Stage	WS	Activity	Start	Finish	Duration	Timeline														
						2014	2015				2016				2017				2018	
						Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	
I	1	Internal consultation	01/10/2014	25/11/2014	8w	■														
I	2	Europol Working arrangement	01/10/2014	24/03/2015	25w	■	■	■	■											
I	2	Implementing rules approved by MB	01/10/2014	24/03/2015	25w	■	■	■	■											
I	2	Draft operational Plan with MS	01/10/2014	25/11/2014	8w	■														
I	3	Plan for technical solution	01/10/2014	24/03/2015	25w	■	■	■	■											
I	2	EDPS Prior Checking process	24/03/2015	28/12/2015	40w															
I	3	Procurement of technical solution	01/01/2016	25/02/2016	8w															
I	3	Installation of technical solution	25/02/2016	20/04/2016	8w															
I	4	Pilot Exercise	25/04/2016	20/05/2016	4w															
I	4	Prototype products produced	20/05/2016	09/06/2016	3w															
I	4	Evaluation and end Stage I report	09/06/2016	29/06/2016	3w															
II	1	Increased scope of data collection	29/06/2016	27/12/2016	26w															
II	2	Increased technical solution	29/06/2016	27/12/2016	26w															
III	1	Full scope of data collection	02/01/2017	22/12/2017	51w															
III	2	Full technical solution	02/01/2017	22/12/2017	51w															

Figure 2 Timeline for the PeDRA Project

4. Stakeholders

4.1. Stakeholder analysis

The stakeholders of the PeDRA Project are numerous and diverse, and include external and internal users, as well as external and internal suppliers. They are presented here in

Supply - Advisors

This is a group of stakeholders who are judged to have high interest and influence on the project because of their advisory or regulatory roles. Their interest is expected to be at the highest level during the initial stages of the project, and their roles might be expected to be reduced to systematic monitoring in the later stages of the project.

Supply - providers

There are several internal suppliers who will have a very strong influence on the project as they will play important roles in the supply chain as providers. Joint Operations Unit will project manage the operational activities in the context of which Member States will collect and transmit the personal data to Frontex. RAU will provide services such as the legality check, and also analysis of the data and case production. FSC will be expected to provide support in terms of transmission of PDPs to Europol and to advise and work in cooperation with ICT when it comes to installing or upgrading any reporting tool.

Direct Users of personal data output

Europol will be the recipient of PDPs containing personal data. The data will probably be imported into the Europol Information System to look for cross matches with previously stored data from other sources. Europol will not need to delete data after three months and so the personal data from Frontex will be available to support investigations for an extended period. Europol is not currently regulated by the EDPS but has its own Joint Supervisory Board.

RAU will also use the PDPs to feed back into the analytical cycle within the Agency, although all data will be deleted or anonymised after three months.

Indirect users of depersonalised risk analyses

Member States as well as EU Agencies and internally JOU & FSC will be recipients of the risk analyses via regular channels. Frontex will also use the risk analyses to feed back into the analytical cycle and risk analyses will be available for the Commission and other EU Agencies as is the case with other Frontex products.

Potential future involvement

According to Article 11c paragraph 3a other Union law enforcement agencies are identified as being potential users of the project products. The term 'Union law enforcement agency' does not have any legal basis but an initial consultation has identified Eurojust, as other potential future direct users. However, any onward transmission of personal data would be subject to EDPS prior checking, and would need to be shown to be necessary and proportional and subject to a specific working arrangement.

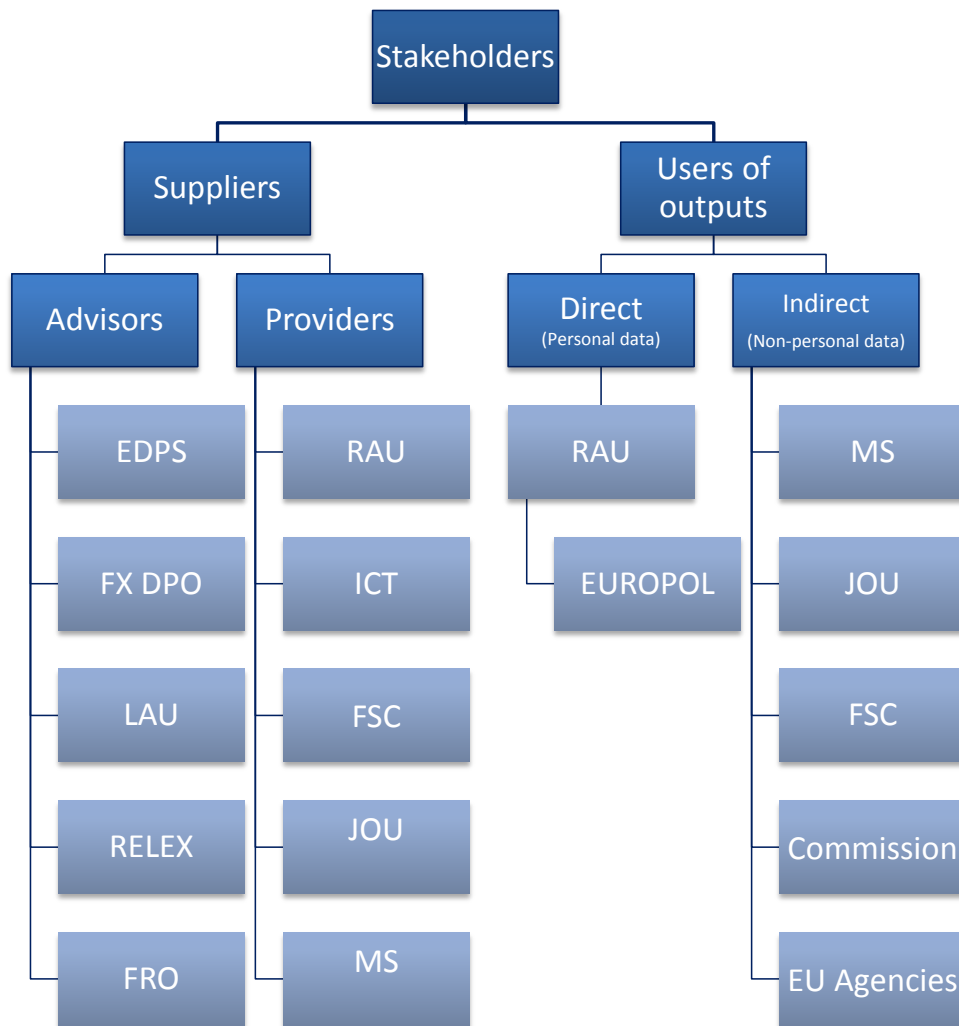


Figure 3 Hierarchy of stakeholders in the PeDRA Project in terms of their roles in producing the project outputs by supplying expertise (advisors) or resources (providers), and those stakeholders that will use the project outputs directly (containing personal data) or indirectly (depersonalised data)

Table 1 External Stakeholders for the PeDRA

External Stakeholder	Role	Responsibility	Interest (needs, wants)	Success Criteria
EDPS	Supplier Advisor	Prior checking, data protection and procedural advice, inspections	Prior checking application, availability for inspections	Compliance with data protection legislation
Member States	Supplier Provider	Collection of personal data and reporting to Frontex	Easy to use reporting tool and procedures, limited additional workload	Quality personal data reported in sufficient quantity to generate effective outputs
Member States	Direct User	Use of depersonalised risk analysis reports for planning operational activities	Clear, high quality useful risk analyses	More targeted response and situational awareness
Europol	Direct User	Use of IPs for investigations and disruption of OCGs	Effective IPs containing raw data and context	Operational successes
Commission	Indirect user	Use of depersonalised risk analysis reports	Clear, high quality useful risk analyses	Business change of more knowledge about OCGs

5. Benefits

A benefit is a measureable improvement resulting *from the output of the project* that is perceived as an advantage to one or more stakeholders in terms of meeting their strategic objectives. Here we list the direct and indirect users of the outputs and briefly document the nature and magnitude of their benefits and how they will be measured.

The two outputs from the project will enable the business change of more knowledge and awareness of the structure and activities of organised crime groups involved in facilitation, trafficking and other cross border crimes, which will enable more effective responses in terms of operational responses from Frontex and Member States and investigations from Europol and Member States.

These business changes will create the outcome that more organised crime groups will be disrupted by the operations and investigations. The outcome of more disruptions will result in the measurable benefit of more detections of facilitators and traffickers and also more arrests of members of organised crime groups. This benefit will help to achieve the strategic objective of saving migrants' lives, lower exploitation by traffickers and lower cross border crime (Figure 6).

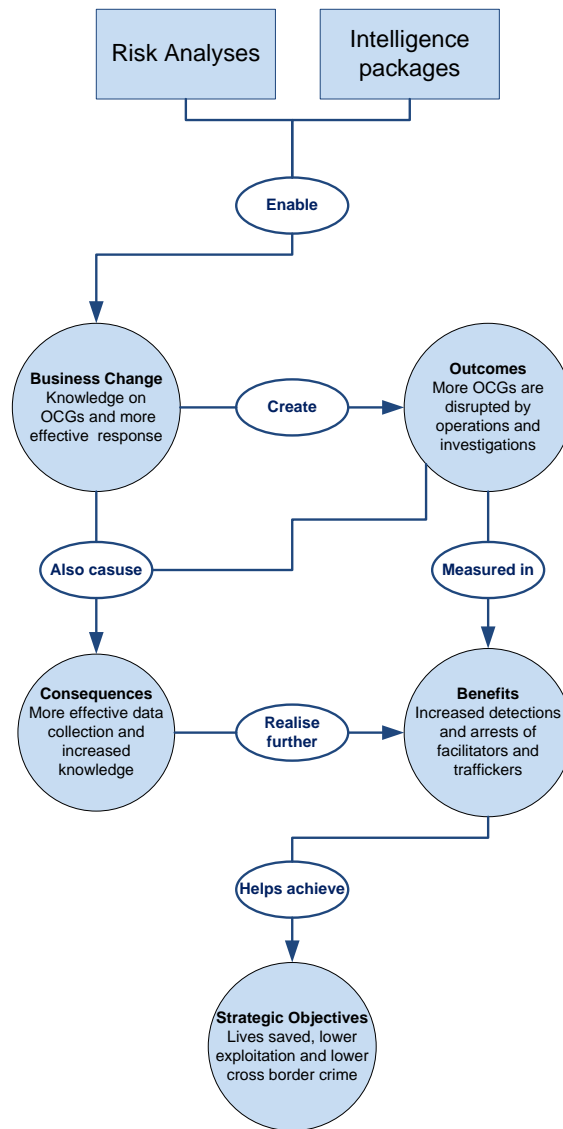
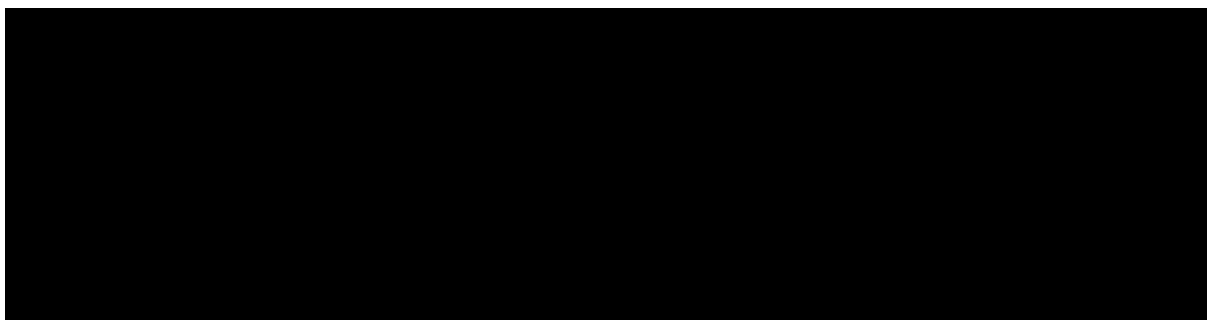


Figure 4 Relationships between PeDRA outputs (deliverables), outcomes and measurable benefits

As well as benefits from the outputs Frontex as a whole will benefit from an increased role in crime analysis and in the law enforcement community as a whole. There is the capacity for Frontex to process large volumes of personal data from its operational activities and so Frontex may become a hub for such data, hence consolidating its role in border security.

Europol



coordinated operational activities. The benefit of this data stream to Europol will be a rich and focused database containing information about the activities of OCGs involved in facilitation, THB and cross-border crime, which can be used to support investigations.

6. Project Organisation

The project organisation structure has four levels of management: Corporate Management, Directing, Project Management and Product Delivery.

1. The Cooperate management includes the Directorate who will endorse the project approach and the implementing rules, take decisions as to the overall objectives and will be responsible for launching or terminating the project.
2. Directing the project will be the Project Board consisting of the Project Executive/Project [REDACTED] who will be the main decision maker in terms of how to reach the project objectives, and [REDACTED] who will be the Senior User (representing the needs of the users of the personal data and the products - outputs) and [REDACTED] who will assume the role of Senior Supplier (representing the interests of the Member States who will supply the personal data).
3. Managing the project will be the Project Manager, [REDACTED], who will be responsible for the day to day running of the project.
4. Delivering the outputs will be the analytical team led by Team Leader [REDACTED]

Amendment Record

Date	From version	To version	Description of change	Change made by
06.01.2013	-	0.1	Document created	
28.01.2013	0.1	1	Endorsed by Directorate Board	
06/06/2014	1	1.2	Amendments	
30/06/2014	1.2	1.3	Comments	
04/06/2014	1.3	1.4	Amendments	
03/09/2014	1.4	1.5	Updates	
06.09.2014	1.5	2.0	Updates	
21/11/2014	2.0	3.0	Updated graphics	
04/12/2014	0.3	0.4	Undated product descriptions	

Executive Summary

This document serves to formally identify the projects objectives, benefits and business justification for the Processing of Personal Data for Risk Analysis (PeDRA) project. Consistent with Prince2 standards, which expect a continued business justification, this is an updated version of the initial v1 case that was endorsed by the Frontex Directorate Board in January 2013. New additions to the document include the data flow diagram and a more detailed outline of the outputs and benefits of the different project stages. It has been updated in parallel with the production of a full Project Initiation Document (PID) that was formally adopted by the Directorate Board in September 2014.

Frontex is an intelligence-led agency that has been processing non-personal data from Member States and open sources since 2006, but there has been growing recognition that Frontex coordinated operational activities represent a major opportunity for the collection, analysis and controlled distribution of personal data relating to individuals involved in border-related criminal activities such as facilitation or irregular migration, trafficking in human beings (THB) and other cross border crimes.

It is important to highlight that large volumes of personal data are already collected by Member States during Frontex operations, and that under Member State national regulations it is possible for the component authorities to share personal data with other Member States and with Europol. Member States have in the past sent personal data from Frontex joint operations directly to Europol, but without contextual information such as final destination country or links to organised crime, the data often fails Europol's mandate check.

To make more efficient use of personal data collected by Member States during Frontex joint operations, the 2011 amendment to the Frontex regulation allows the Agency to further process personal data collected by Member States during Frontex joint operations, and PeDRA is the first step in allowing Member States to transmit such personal data in a secure manner to Frontex for further processing at the EU level.

In the Programme of Work 2014¹, Reference 10 Risk Analysis, states that the Risk Analysis Unit (RAU) should work towards providing depersonalised analytical reports based on PeDRA, and transmission of Personal Data Packages (PDPs) on a case-by-case basis to union law enforcement agencies. Similarly, under Goal 1 – Situational Awareness, priority 7 states that the agency '*Should develop the process and exchange of information containing personal data to and within existing structures of law enforcement agencies for legitimate purposes*'.

Three business options to achieve these strategic goals are presented here. The first is doing nothing, but this would squander the opportunity of analysing and sharing valuable (and already collected) data to prevent loss of life, reduce the risk of exploitation of vulnerable groups and increase border security. The

¹ Reg. No 1899/05/02.2014

second option is to proceed with a personal-data project, with initially limited scope in terms of data sources, volume and complexity, but with all data protection procedures in place. The third option is to develop and launch a full scale project involving all Frontex operational activity and all types of personal data. The second option was selected by the Frontex Directorate Board in 2013, and so current plans are for PeDRA to be managed in three stages of successively increased complexity and scope, beginning with a Pilot exercise at the end of Stage I, once legal and administrative procedures have been put in place.

PeDRA will contribute to the following strategic objectives: preventing loss of life, reducing the risk of exploitation of vulnerable groups and increasing border security. In tangible terms the measurable benefits from the PeDRA project will be increased inhibitions, detections and arrests of facilitators and traffickers made possible by a more effective operational response at the border by Member States and Frontex and more successful investigations by Europol. These strategic objectives and measurable benefits will be made possible because of the project outputs, which are legally limited in the Frontex Regulation as: 1) Risk analyses, the results of which will be depersonalised, and 2) Personal Data Packages (PDPs) to be transmitted to Europol on a case-by-case basis.

Personal Data Packages: During PeDRA Stage I, Europol will be the only recipient of Personal Data Packages (PDPs) containing personal data². The outcome of transmitting Personal Data Packages to Europol will be to enrich Analysis Work Files (AWFs) with personal data and contextual information relating to the identities and activities of OCGs involved in facilitation, THB and cross-border crime. The contextual information will enable the PDPs to pass the Europol mandate check for acceptance into the AWFs. The measurable benefit of this enrichment will be successful investigations and more effective support to Member States in their activities to dismantle the criminal groups, hence contributing to the strategic objectives.

Risk analyses: Frontex, Member States and the Commission will be the recipients of risk analysis products from RAU with the inclusion of new, more detailed analyses performed on personal data relating to the fine-scale and longitudinal activities of OCGs, although the results will be de-personalised. This will enable Member States to benefit from a more accurate overview when it comes to the activities of OCGs at the borders of the EU, which will support their national investigations and increase their internal security. Frontex will use these risk analyses to contribute to situational awareness and to produce a more focussed operational response at the border.

There are four major dependencies in the PeDRA project. Firstly, Frontex needs to produce new Implementing Rules for handling personal data within the Agency. Secondly, there is the need to update the working arrangement with Europol to accommodate the exchange of personal data. Thirdly, there a draft operational plan for the Pilot Exercise needs to be drafted in consultation

² Frontex regulation states that other union law enforcement agencies may also be recipients of personal data transmitted by Frontex, based on specific working arrangements and subject to data protection principles of necessity and proportionality and prior approval from the European Data Protection Supervisor

with a potential hosting Member State. Finally these three documents, together with a design for a minimum technical solution for transmission, storage and analysis of personal data in Frontex, need to be combined and submitted to the European Data Protection Supervisor for prior approval. After submission, prior approval can take a year or more to achieve and so expectations of stakeholders need to be managed in this regard.

The final section in this document deals with risks, which have been minimised wherever possible. For example the risk that Member States will not be prepared to share personal data has been reduced by seeking to exploit pre-existing data streams. However, the most significant risk is the substantial time period probably required for prior approval from the EDPS. This is being minimized by implementing a strategy of clear planning and transparency, as well as compliance with the legal framework at all times and a zero tolerance for scope creep.

Table of Contents

Executive Summary.....	3
1. Purpose.....	7
2. Background and current situation.....	7
3. Reasons	9
4. Business Options.....	10
5. Expected Benefits	11
6. Expected dis-benefits.....	13
7. Time scale	13
8. Costs	14
9. Major Risks	15
Annex 1 Dependencies.....	17
Annex 2 List of potential data subjects	17
Annex 3 Data-flow diagram	18

1. Purpose

The purpose of this detailed PeDRA Business case is to build upon an original document – the PDP Business Case Outline - that was endorsed by the Frontex Directorate Board back in January 2013. This document benefits from the Internal Consultation Process which took place in Q1 and Q2 2014 involving several Frontex units to discuss the amended regulation and business opportunities.

This document serves to formally identify the projects objectives, benefits and continued business justifications for the PeDRA Project. It contains all standard sections expected in a business case, and levels of detail according to Prince2 standards.

This business case is accompanied by a Project Initiation Document which provides the basic information needed to direct and manage the project, and establish a basis for the assessment of overall success. The PID forms the agreement between the project management team and the Frontex Directorate Board.

2. Background and current situation

Frontex has been processing non personal data and open source information since 2006 but there has been growing recognition that Frontex coordinated operational activities represent a major opportunity for the collection, analysis and distribution of personal data relating to individuals involved in border-related crimes such as facilitation of irregular migration, trafficking in human beings and other cross border crimes such as smuggling of goods and narcotics. Much personal data are already collected by Member State representatives participating in Frontex operations, particularly during surveillance, interviews of migrants and forensic examination of mobile devices, but because of legal constraints, these data are not made available to Frontex for analysis at the EU level. This represents an obstacle in the possibility of exploiting the data for risk and crime analyses at the EU level.

In the 2011 amendment to the Frontex regulation Frontex is now empowered, in a limited capacity, to further process personal data collected by Member States during Frontex coordinated operational activity. PeDRA will be the first operational step in allowing Member States to transmit in a secure manner to Frontex personal data collected during or in the context of Frontex coordinated operational activities, and for Frontex to develop a system to further process the personal data for two purposes defined by the Frontex regulation; to use the personal data for risk analysis, the results of which shall be depersonalised, and to produce and transmit Personal Data Packages containing personal data to Europol³ on a case-by-case basis.

³ or other union law enforcement agencies

The PeDRA Project has three Stages, is scheduled to run for three years (2014-2016) and expects to involve a broad scope of personal data collected during a wide range of operations, for sophisticated analysis using specialist software.

Stage I of PeDRA was launched in October 2014 with PID in September 2014. Stage I has four work streams:

- WS1** New Implementing rules
- WS2** New Working Arrangement with Europol
- WS3** Draft operational plan for Pilot Exercise
- WS4** Design and Installation of minimum technical requirements
- WS5** EDPS notification

Stages II and III are characterised by increased complexity and scope in terms of the number of participating joint operations (data sources), the complexity and volume of the data, and the sophistication and automatization of the technical solution required to securely report, process and transmit the personal data.

Approval references

The Frontex regulation (EC) 2007/2004 as amended in 2011⁴ states that the Agency may process personal data collected by Member States during Frontex coordinated operational activities and transmitted to the Agency in order to contribute to the security of the external borders of the Member States.

In the Programme of Work 2014⁵, Reference 10 under the business area of Risk analysis, states that RAU should work towards providing depersonalised analytical reports based on PeDRA, and initial transmission of Personal Data Packages on a case by case basis to law enforcement agencies.

In the same document, under Goal 1 – Situational Awareness, priority 7 states that the agency '*Should develop the process and exchange of information containing personal data to and within existing structures of law enforcement agencies for legitimate purposes*'. Expected outcomes include

- an efficient law-abiding process for generating, collecting, transmitting, processing and analysing personal data
- the establishment of internal roles and responsibilities with regards to processing personal data
- Roles and responsibilities on personal data transmission to Europol

⁴ Regulation (EU) No 1168/2011

⁵ Reg. No 1899/05/02.2014

- Identification and acquisition of a system for data processing/visualisation and analysis.

Personal data is also mentioned under Priority 4 (Intensify the concept of different types of joint operations and to target Frontex operations aligned with the priorities of the Internal Security Strategy) of Goal 2 – Supporting Response. In this context personal data is expected to help the agency develop joint operations towards crime detection and prevention, including the fight against terrorism.

3. Reasons

Frontex is an intelligence-led agency. In line with analytical principles, risk analyses take into account as many sources of information as possible, because multiple streams eliminate errors and help to corroborate the existence of subtle trends. Until recently Frontex has been limited by its mandate to only process non-personal data and intelligence, but now that legal limitation has been lifted there is a real opportunity to significantly add value the risk analysis capacity of the agency by processing personal data.

It is widely recognised that there is a wealth of personal data already acquired during Frontex coordinated operational activity that would add considerable value to risk analysis processes in Frontex. This includes details on the behaviour of organised crime groups, and those individuals involved in trafficking of human beings. In addition personal data are also collected by Guest Officers deployed by Frontex in such joint operations. When this happens, data are often being passed to the local national authorities, but the data are not made available at the EU level systematically. Personal data already collected by Member State representatives participating in Frontex Joint Operations are sometimes exploited at the national level but frequently such data are not sufficiently processed due to limited resources at the border, especially when large volumes of migrants are arriving within a very short space of time. During these peaks of activity, much personal data can be left unprocessed.

Not only are some personal data not exploited at the national level, data are also only rarely exchanged with Europol – in fact there is no significant flow of personal data from Frontex coordinated operations to any EU agency, which means there is no analysis taking place at the EU level, despite the existence of personal data that would be of interest and use to many Member States away from place of detection (transit countries, destination countries). PeDRA will be the first step to make these data available firstly to Frontex for risk analysis purposes and secondly to Europol to support investigations.

The two outputs from the project will enable the business change of more knowledge and awareness of the structure and activities of organised crime groups involved in facilitation, trafficking and other cross border crimes, which will enable more effective responses in terms of operational responses from Frontex and Member States and investigations from Europol and Member

States. These business changes will create the outcome that more organised crime groups will be disrupted by the operations and investigations. The outcome of more disruptions will result in the measurable benefit of more detections of facilitators and traffickers and also more arrests of members of organised crime groups. This benefit will help to achieve the strategic objective of saving migrants' lives, lower exploitation by traffickers and lower cross border crime (Figure 1).

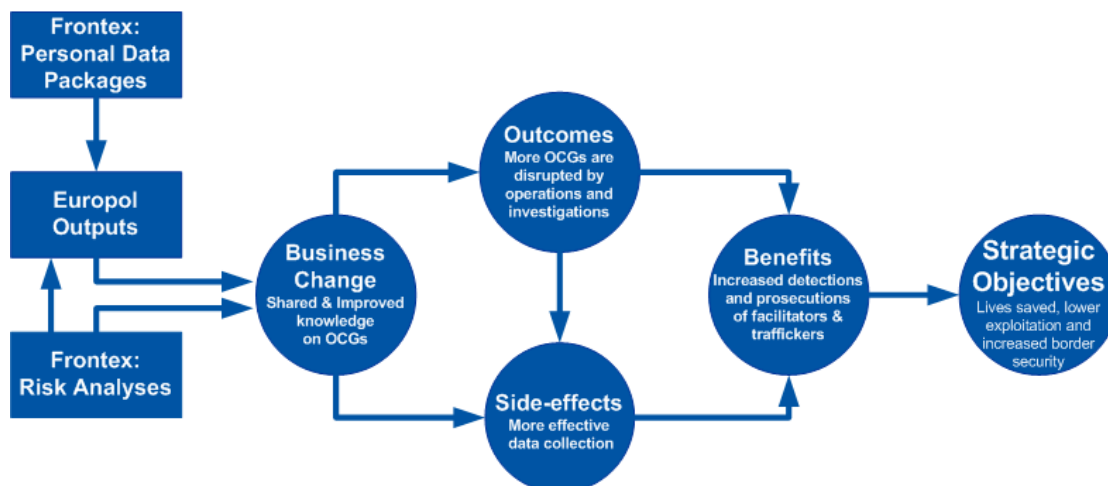


Figure 1 The business changes, outcomes and benefits of the PeDRA Pilot exercise

The business needs of PeDRA refer to the institutional objective of increasing the role of Frontex in contributing to the management of border security. This need will be met by the generation of high quality products and the dissemination to the correct users, as well as a more targeted operational response at the border. At the higher level, PeDRA will enable Frontex to establish itself with a more significant role in the border security community, as the volume of data collected with joint operations is already significant and highly relative to combating cross-border crime. It will also strengthen the relationship and cooperation between Frontex and Europol in line with the general principle of data sharing and cooperation between EU Agencies.

4. Business Options

Do nothing

Article 11c of the Frontex regulation states that Frontex *may* process personal data and so there is no obligation for Frontex to do so. However, as Frontex is an operational agency and the operations are intelligence led, there is an implicit obligation to make as much use as possible of the intelligence collected during the operations, including personal data. For this reason the Do Nothing Option is not considered here.

Full Project

A full technical capacity and scope of data collection is not considered to be a viable option in this case due to the complexity of the project, the nature of the

external regulation and the institutional damage that could result from conspicuous failure.

5. Expected Benefits

A benefit is a measureable improvement resulting *from the output of the project* that is perceived as an advantage to one or more stakeholders in terms of meeting their strategic objectives. Here we list the direct and indirect users of the outputs and briefly document the nature and magnitude of their benefits and how they will be measured.

Frontex – RAU

The Risk analysis unit will be direct user of both the PeDRA Personal Data Packages and the risk analysis reports as additional sources of information to support RAU risk analysis processes. The outcome of this will be a greater understanding of the identities and activities of organised crime groups involved in facilitation, THB and cross-border crime.

The activities include recruitment in third countries, provision of transportation and accommodation services along the route with modalities that allow avoiding law enforcement attempts of detection and apprehension, arranging the gathering of people and their embarkation or their illegal crossing of the land green border or border crossing points at sea, land and air, methods of obtaining fraudulent documentation, secondary movements in other EU Member States after the illegal entry in one MS and methods of payments.

The approach of a pilot exercise was endorsed by the Frontex Directorate Board in 2012.

Pilot Exercise

Although all data protection legislation must be fully complied with before any personal data can be processed, there are several areas where complexity, scope, volume of data and level of automation can be reduced in the form of a Pilot Exercise.

In this case, to reduce the volume of data, just one Joint Operation will be enlisted as the source of the personal data. To reduce the complexity of the data transmitted, the Pilot Exercise will only consider unstructured information collected during debriefing activities which tend to include the names, telephone numbers and addresses of facilitators. Finally, the Pilot Exercise will only employ a basic technical solution in terms of the processing and analysis of the personal data, with many manual processes, which should be feasible given the low volume of expected data during the Pilot.

Increased understanding and more precise risk analyses will convey considerable benefits in terms of an increased role for RAU in supporting stakeholders involved in the fight against OCGs and supporting Member States in coordinating a more targeted response at the border.

Europol

Europol will be a direct user of PeDRA Personal Data Packages based on personal data collected by Member States during Frontex coordinated operational activity. From time to time Member States have been known to send collected during Frontex Joint Operations to Europol – however this data stream is regarded as insufficient. Hence an outcome of the project is a significant increase in the volume of personal data received by Europol from Frontex coordinated operational activities. The outcome of this data stream to Europol will to enrich the Europol Information System (EIS) with personal data and contextual information relating to the identities and activities of OCGs involved in facilitation, THB and cross-border crime. The measurable benefit of this enrichment will be successful investigations and more effective support to Member States in their activities to dismantle the criminal groups, hence contributing to the strategic objectives.

Member States

Member States will be the recipients of risk analysis products from RAU with the inclusion of new analyses performed on personal data. The results will be de-personalised but the reports will contain more details on the identities and activities of specific OCGs and so Member States will benefit from greater awareness of modus operandi and links between groups. In addition, Member States will benefit from the increased possibilities of cross matches of targets of investigations in the Europol Information System and by the enriched data set and Personal Data Packages provided by Frontex, as an intelligence lead for new or ongoing investigations.

Frontex – JOU/FSC

One outcome of the PeDRA project will be risk analyses that are more focussed on organised crime groups involved in facilitation, THB and CBCs. The Frontex joint operation unit will benefit from this outcome by planning more targeted joint operations at the border with focusses on specific modus operandi, while the Frontex FSC will benefit from the risk analyses to contribute to situational awareness.

Commission and other EU Agencies

Other recipients of RAU risk analyses will benefit from new analyses made possible by the processing of personal data.

6. Expected dis-benefits

Dis-benefits result from outcomes and may be seen as a disadvantage by one or more stakeholder. In the case of the PeDRA (and risk analysis in general) these are limited, as the project focusses on exploiting an existing but hitherto unutilized data stream for effective analytical purposes and data sharing.

However, one potential dis-benefit may be reported by users who find new, more complex analytical products more difficult to interpret.

Also increased data sharing will produce significant resource issues for RAU, especially given the novel and specialised nature of the work.

7. Time scale

The currently on-going PeDRA Stage I represents the first of three stages of the overall PeDRA Project expected to run between 2004 and 2016. Each Stage is characterised by increasingly sophisticated technical solutions, data complexity, volume and scope. Stage I will conclude after the Pilot Exercise, currently planned for Q2 2016.

PeDRA has four external dependencies each with its own independent timescale. In addition there is the influence of an unfamiliar external regulator (EDPS) who will oversee and approve the planning and the launch of the Pilot exercise as well as approving three of the external dependencies.

The PeDRA milestones are as follows:

1. Completion of the Internal Consultation Plans and Project planning (end 2014)
2. Addressing the 5 workstreams which need to be overcome before the Prior checking can be submitted (end Q1 2015)
3. Gaining Prior approval from EDPS (end 2015)
4. Procuring and installing technical solution (end Q1 2016)
5. Launch of Pilot Exercise (Q2 2016)
6. Launch of Stage II (Q2 2016)
7. Launch of Stage III (Q4 2016)

A more detailed timeline and a Gantt chart can be found in the PID.

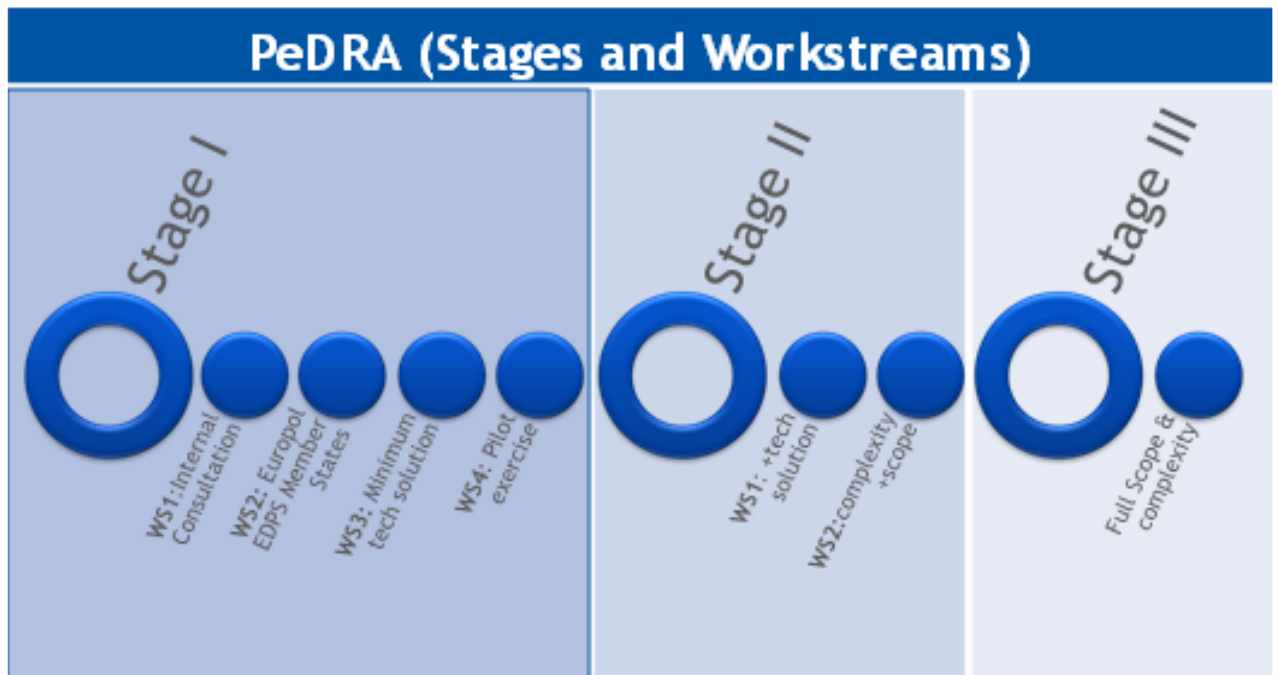


Figure 2 The currently on-going PeDRA Stage I represents the first of three stages of the overall PeDRA Project. Each stage is characterised by increasingly sophisticated technical solutions, data complexity and scope. Stage I will conclude after the Pilot Exercise, currently planned for Q2 2015

8. Costs

The budget for the PeDRA is initially calculated to be EUR 272 714.00 to cover missions to Europol, Member States and EDPS during each stage and for the technical solution that will start as basic in Stage I and then become more complex and automated in Stages II and III

The human resources required for the project will evolve through the different stages of project implementation: only Stage I resources are presented below. The End of Stage Report for Stage I will update the resources required for Stage II and Stage III.

Stage I – Staff

Project Manager	0.6 FTE
Team Leader	0.1 FTE
BI Support	0.3 FTE
Analyst support (project team)	1.3 FTE

Resources from suppliers, advisors required for Stage I

Relex IO	0.5 FTE
----------	---------

DPO	0.3 FTE
LAU	0.3 FTE
ICT	0.2 FTE
JOU	0.1 FTE
FSC	0.1 FTE

9. Major Risks

Category	Risk	Probability	Impact	Countermeasures
Political	MS may require considerable support to understand their role and accept value of benefits; Europol adopting a conservative position, seeing the role of Frontex in processing PD as a threat rather than an opportunity;	Medium	High	Clarify the business case for Frontex and the explain the benefits of processing personal data to Europol and MS
Strategic	Stakeholders expectations too high;	Medium	Medium	Manage expectations
Finance	Hitherto unforeseen procurement costs	Low	Medium	Regular monitoring and timely amendment of budget
Organisational	Limited experience of personal data processing in Frontex Insufficient capacity to support all key aspects of processing personal data for the pilot within the given time framework	Medium	Medium	Objective to create new culture and skills; Effective planning and timelines Consultation with agencies and law enforcement organisations and advice given.
Institutional	Low willingness of MS to provide PD to Frontex; No willingness of MS to host Project	Medium	High	Promote benefits to MS;

Category	Risk	Probability	Impact	Countermeasures
Internal	Reduced priority for PeDRA deriving from unforeseen events; Significant delays in installing technical solutions	Low	Medium	Reporting to Frontex management difficulties related to workload and other priorities; Effective planning and communication between units
Legal	Impact of national legislation of hosting MS in the provision and use of PD to Frontex; Frontex exposed to legal liabilities	low	High	Cooperation with LAU and MS authorities Consultation with EDPS
Legal	Very long delays resulting from EDPS Prior checking	High	High	Diligent application for Prior checking and follow up. Presentation during inspection May 2014
Technical	Unknown impact on information platforms	Medium	Medium	Close cooperation with ICT unit and FSC

Annex 1 Dependencies

Before submitting to EDPS for prior checking for the Pilot Exercise, dependencies 2, 3 & 4 will all need to be completed first.

1. EDPS – Prior Checking to the European Data Protection Supervisor is a key dependency without which it would not be possible for the Agency to process personal data for risk analysis. Prior checking is a lengthy and complex undertaking for which much planning and follow-up is necessary. For instance, gaining Prior approval from EDPS for Frontex to process personal data from Frontex coordinated Return operations took around one year. Other examples on the EDPS website also suggest that a considerable amount of time should be put aside for this task. The Work Stream 4 of Stage I can only proceed once EDPS prior approval has been granted.
2. EUROPOL- According to Article 13 paragraph 2, onward transmission of personal data processed by the Agency to other Union agencies shall be subject to specific working arrangements and subject to prior approval from the EDPS. Hence there is the need to put in place a new working arrangement subject to prior approval from the EDPS. The Work Stream 4 of Stage I can only proceed once prior approval has been granted for the new working arrangement.
3. MS – A Member State will be selected by the Project board for being invited to participate in the Pilot Exercise. This choice will be made based on a prediction of their willingness and capacity to participate. Stages II and III will involve the recruitment of more Member States into the full PeDRA Project.
4. Frontex Management Board: According to article 11a of the Frontex Regulation the MB shall establish measures for the application of Regulation 24/2001 and that these measures will be established after consultation with the EDPS. The DPO and RAU have already drafted new implementing rules but these will not be put before the MB until the EDPS have approved them.

Annex 2 List of potential data subjects

Refer to Article 11a paragraph 2

1. Facilitators:
Recruiters, transporters, locals, organisers, bosses, skippers, public officials,
2. Traffickers:
Recruiters, transporters, locals, organisers, bosses, skippers, public officials,
3. Cross-border crime:
Suppliers, logistics, smugglers, sellers

Annex 4 Product descriptions

As the focus of PeDRA is on the delivery of effective products, this section outlines both of the outputs from the project so that there will be an early consensus on what the project is working towards. There will be the opportunity to update these descriptions at the end of Stage I.

According to Article 11c paragraph 3: *Personal data [referred to in Paragraph 2] shall be further processed by the Agency only for the following two purposes:*

- 1. The transmission on a case by case basis to Europol or other Union law enforcement agencies, subject to Article 13*
- 2. The use for the preparation of risk analyses referred to in Article 4. In the result of the result of the risk analyses, data shall be depersonalised.*

These two purposes coincide exactly with the two outputs of the PeDRA project that are detailed below.

Output 1 Personal Data Packages (PDPs)

[Redacted content]

[Redacted content]

Output 2 Risk Analyses

[Redacted content]

[Redacted content]

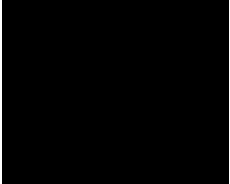
[Redacted content]

Warsaw, {June 2013}
File n°: (0.5)



Distribution:

Amendment Record

Date	From version	To version	Description of change	Change made by
22.05.2014	-	0.1	Document created	
06/06/2014	01.	0.2	Comments	
13/06/2014	0.2	0.3	Comments	
30/06/2014	0.3	0.4	Comments	
03/06/2014	04	0.4	Executive summary	
09/04/2015	0.4	0.4	Minor dits after VC with EDPS	

Executive Summary

The purpose of this document is to describe, accurately and unambiguously in a technology-independent manner, the business requirements for the technical solution for Stage I of the PeDRA project. The main audience for this document is the Frontex ICT Unit and the Frontex Situation Centre, and other internal and external technical partners as deemed necessary. Another intended audience for this document are the business owners (RAU) of the proposed system. In this context, the Project Board will need to confirm that the business requirements have been documented here completely, accurately and unambiguously before ICT and FSC are mobilised to begin designing a technical solution.

Since the requirements are documented here in a technology-independent manner, the PeDRA team and the end-users of the system (processors authorised to process personal data on behalf of the controller - HoRAU) should also be able to comprehend the requirements from this document.

A Pilot Exercise, currently scheduled for Q2 2016, will be the first step in achieving the operational objective of empowering Member States to transmit to Frontex, in a secure manner and compliant with data protection legislation, personal data collected during or in the context of Frontex coordinated operational activities, and for Frontex to develop a system to process such personal data in the context of two outputs defined and limited by the Frontex regulation: 1) to use the personal data for risk analysis, the results of which shall be depersonalised, and 2) to produce and transmit Personal Data Packages (PDPs) containing personal data and contextual information to Europol on a case by case basis.

The objective of the PeDRA is to incorporate personal data collected by Member States during Frontex operational activities into European-level risk analyses and investigations into irregular migration to the EU and Schengen area, with a particular emphasis into the activities of organised crime network. The outcome of PeDRA will be a greater understanding of the identities and activities of organised crime groups involved in facilitation, THB and cross-border crime. The benefit of these outcomes will be more effective border management, tighter border security and increased internal security. These are outlined in more detail in the PeDRA business case (currently v4.0).

The high level business functions which are in scope for the system are: Authenticating the source of the transmission, checking the legality of the data, analysing the data, and access management of the data. Conducting investigations is the only business function that is out of scope as Frontex is forbidden to conduct investigations. There are only two high-level system interfaces which are in scope: A single ICC transmitting daily reports into the system and sequent sending Personal Data Packages to Europol. The high level systems interfaces that are out of scope are: other ICCs, LCCs and team leaders or guest officers transmitting daily reports to Frontex on an ad hoc basis as other actors and locations will not be empowered to send daily reports containing personal data to Frontex; and sending Personal Data Packages other Union Law enforcement agencies.

Stakeholders are the individuals or groups who have a vested interest in this system. The four categories of stakeholders are outlined as: Suppliers (MS, internal Frontex units), Managers (RAU, ICT), Producers (RAU) and Recipients (Europol). Almost overlapping in this case, are the Actors who interact with the system. The Actors for the PeDRA system are: Europol, who are a recipient needing access to the system only to receive transmissions; Member States who are suppliers who need just to transmit data to the system; Operational analysts in RAU who are producers needing read only access to the system; and the PeDRA team who are managers needing the highest level of access to the system such as storing, reading, deleting personal data plus exporting personal data out of the system to Europol.

There are eighteen use cases specifications listed in this document which have been summarised in the table below. Use cases describe the system's behaviour under various conditions as the system responds to a request from a primary actor – hence the primary actor initiates an interaction

with the system to accomplish a goal. In each case in the table below effort has been made to document the difference sequences or behaviour, or scenarios that can unfold depending on the particular request made and the condition surrounding the request.

Table 1 Use case specifications for the PeDRA data-management system

ICC Transmit	Processors open daily reports
Authentication	Processors create an additional file
Notify ICC of unauthenticated transmission	Store additional file
Daily report - Open	Open and edit additional document
Check legality	Create Case Folder
Daily report storage	Send case to Europol
Rejection of non-legal daily report	Case received by Europol
Ask ICC for justification	Delete expired data
ICC respond to request for justification	Access management

In addition and complementarily to the use cases are nineteen business rules that define or constrain some aspect of the system and are intended to assert system structure or to control or influence the behaviour of the system.

Table 2 Business rules for the PeDRA data-management system

Authenticate (1) – source	Post Authentication access – arrive in RAU
Authenticate (2) – file names	Storage – in PeDRA system
Data Subjects - legality	Analyst access – Operational Analysts
Authenticate fail (1) - source	Transmission – to Europol
Authenticate fail (2) – file names	Case production – by PeDRA team
Data Source – ICC	Justification – of legality
Data uses – risk analysis and IPs	Additional files – containing PD
Data expiry – 90 days	Expire data - >90 days
Data legality – prop/necessity	Non-acceptance – non legal data
Data use (2) - investigations	Justification response – from ICC
Data transmission – not to TCs	Store additional file – in predetermined place
Data input – secure channel	Case reception – by Europol

The data requirements for the PeDRA data-management system are very simple indeed, as the daily reports are qualitative and unstructured, usually MS Word or PDF documents. Although the operational analysts will extract the personal data and create additional files, there will be no complex data requirements associated with this procedure. In contrast the security requirements are comprehensive, and are largely determined by the data protection legislation.

This document also contains a description of the non-functional requirements, which define how a system is supposed to be rather than how it behaves. The non-functional requirements are split into three categories: FR1 – transmission of personal data to Frontex, which covers access management, volumes of data etc; FR2 Creation and operation of a secure analytical environment in Frontex, which covers access and file storage and security etc; and FR3 – transmission of Personal Data Packages to Europol, which covers access and compatibility.

Table of Contents

Executive Summary.....	3
Table of Contents.....	5
1. Introduction.....	6
1.1. Document Purpose	6
1.2. Intended Audience.....	6
1.3. Project Background	6
1.4. Purpose of the Business Requirements.....	7
1.5. Business Goals/Objectives to be achieved.....	7
1.6. Benefits/Rationale	8
1.7. Stakeholders	8
1.8. Dependencies on existing systems.....	9
2. Requirements Scope	10
2.1. In Scope	10
2.2. Out of Scope	11
3. Functional Requirements.....	12
3.1. Actor Profiles Specification	12
3.2. Essential Use Case Diagram	13
3.3. Essential Use Case Specifications	15
3.4. Business Rules.....	25
4. Data Requirements	27
4.1. Data Architecture	27
4.1. Data Volumes	27
4.2. Data Retention and Archiving	27
5. Non-Functional requirements	27
4.2. Non-functional requirements 1 (NFR1) - Transmission of personal data to Frontex.....	27
4.3. Non-functional requirements 2 (NFR2) - Creation of a secure operational/analytical environment.....	28
4.4. Non-functional requirements 3 (NFR3) - transmission of Personal Data Packages to Europol .	28
5.1. Security Requirements.....	28
Annex 1 Business requirements	29

1. Introduction

1.1. Document Purpose

The purpose of this document is to describe, accurately and unambiguously in a technology-independent manner, the business requirements for the technical solution for PeDRA. All attempts have been made in using mostly business terminology and business language while describing the requirements in this document. Very minimal and commonly understood Technical terminology is used. The use case method is used in modelling the business requirements in this document.

1.2. Intended Audience

The main audience for this document is the Frontex ICT Unit and the Frontex Situation Centre, and other internal and external technical partners as deemed necessary. The information in this document has been formatted so that it can be used to inform a process to design and propose a technical solution that will allow Frontex to meet the specific business requirements set out here.

Another intended audience for this document are the business owners (RAU) of the proposed system. In this context, the Project Board will need to confirm that the business requirements have been documented here completely, accurately and unambiguously before ICT are mobilised to begin designing a technical solution.

Since the requirements are documented here in a technology-independent manner, the PeDRA team and the end-users of the system (authorised personal data processors) should also be able to comprehend the requirements from this document.

1.3. Project Background

This section describes if these Business Requirements are as a result of any previous meetings, correspondence, legislation etc.

PeDRA is the first step in achieving the operational objective of empowering Member States to transmit to Frontex, in a secure manner and compliant with data protection legislation, personal data collected during or in the context of Frontex coordinated operational activities, and for Frontex to develop a system to process such personal data in the context of two outputs defined and limited by the Frontex regulation: 1) to use the personal data for risk analysis, the results of which shall be depersonalised, and 2) to produce and transmit Personal Data Packages containing personal data to Europol on a case by case basis.

This document is produced under the PeDRA Project Stage I (2014) which was raised using a standard project template in March 2014. The document contributes to the following Stage I objectives:

Objectives of Stage I

- 1) Internal consultation plan: this document will assist in the internal consultation with ICT regarding the planning and implementation of the technical solution
- 2) Establishing contact with EDPS: This document will be partially exploited during the application for prior checking
- 3) Technical solution: the business requirements specified here relate to the technical solution for PeDRA
- 4) Pilot Exercise: The final objective is to run a Pilot Exercise

1.4. Purpose of the Business Requirements

This section describes the purpose of the Business Requirements.

- Business requirements for major enhancements to an existing application.
- Business requirements for new application development.
- Business requirements for replacement application development.
- Business requirements for a request for technical proposals.**

These business requirements have been documented to allow technical partners within Frontex (ICT) to propose technical solutions to meet the needs specified here.

1.5. Business Goals/Objectives to be achieved

This section describes the major objectives to be achieved with the implementation of the Business Requirements.

The objective of the overall PeDRA is to incorporate personal data collected by Member States during Frontex operational activities into European-level risk analyses and investigations into irregular migration to the EU and Schengen area, with a particular emphasis into the activities of organised crime network. At the functional level, PeDRA is the mechanism that is being put in place to implement Article 11c of the amended Frontex regulation empowering Member States to transmit personal data to the Agency, so that Frontex can:

1. improve risk analyses, and to increase the accuracy, efficacy and targeted nature of the operational response coordinated by Frontex
2. process and transmit Personal Data Packages* to Europol or other EU law enforcement authorities to contribute to the fight against migrant smuggling, cross-border crime and trafficking in human beings.

**In the context of PeDRA, an Personal Data Package is defined as a thematic collection of interview reports (containing personal data), plus additional context or analytical files (also containing personal data) providing important context and additional information necessary for effective interpretation and further processing for investigative purposes.*

1.6. Benefits/Rationale

This section describes the major benefits to be achieved with the implementation of the Business Requirements.

The outcome of PeDRA will be a greater understanding of the identities and activities of organised crime groups involved in facilitation, THB and cross-border crime. Increased understanding and more precise risk analyses will produce an increased role for Frontex in supporting stakeholders involved in investigating OCGs and supporting Member States in coordinating a more targeted response at the border and more effective deployment of resources. The benefit of these outcomes will be more effective border management, tighter border security and increased internal security.

The second outcome of PeDRA will be an increase in the volume of personal data generated during Frontex coordinated operational activities, which are received by Europol. This outcome will generate a rich and focussed database containing information about the identities and activities of OCGs involved in facilitation, THB and cross-border crime. The benefit of this outcome will be more effective investigations and a more productive fight against organised crime, hence contributing to the internal security of the European Union.

1.7. Stakeholders

Stakeholders are the individuals or groups who have a vested interest in this system and whose interests need to be considered throughout the project. This section lists the Stakeholders of the PeDRA data-management system for which these Business requirements are documented. They are classified into 4 categories: Suppliers, Managers, Producers and Recipients.

Supplier

A Supplier is a stakeholder that contributes personal data to the system

With respect to the technical solution considered in this document, the only supplier will be a single Member State, who will collect and transmit personal data to Frontex in the form of daily reports. The data will probably come from a single location within the Member State, or it may be the case that data will be collated from multiple locations but in any case there will be just one point of transmission to Frontex. In the context of PeDRA this single location will be the International Coordination Centre (ICC). Access to the system will therefore be necessary in this single external location.

It is important to mention that subsequent to the Pilot Exercise when data streams are extended in both source and complexity, it may be necessary to change this single location in Member States, in order to maximise the flow of data from the extended range of sources.

Managers

Managers are stakeholders who will be responsible for the day-to-day business processes of the system

Managers of the PeDRA technical system will be the PeDRA Project management team in RAU, and a representative from ICT for technical developments and support. The PeDRA team currently comprise of a Project Manager, Senior User, Analyst and project support. Coordination will be necessary between these actors to ensure that the PeDRA system is always effectively managed from a data protection and business continuity point of view.

The PeDRA team will be responsible for checking the legality of the data and then storing it within predetermined locations. They will also be responsible for high-level maintenance tasks such as managing the hierarchical structure of shortage system and the deletion of expired personal data.

Producers

Producers are stakeholders that will produce the outputs of the system

Producers will be limited to authorised personal data processors in RAU (operational analysts) who will be responsible for producing risk analyses, and members of the PeDRA team who will produce intelligent packages based on the personal data. This will be achieved by opening personal data files stored by the PeDRA management team, and creating additional files to be stored in predetermined locations.

Recipient

Europol is the only planned recipient of the Personal Data Packages produced by RAU and so Europol is the only receiver of personal data from the PeDRA technical system. In the future it is conceivable that there will be more recipients, as allowed for in the Frontex regulation, but this is not planned at the present time.

Member States

Member States will be the recipients of the risk analysis products but as these will be depersonalised they can be sent via regular channels. Hence, member States do not need recipient access to the system.

1.8. Dependencies on existing systems

This section describes the dependencies between the Application for which these Business Requirements are written and the other existing applications/systems.

This system does not have any dependencies on any existing systems as it is likely to be standalone i.e. operating in isolation from other internal systems. However, users will be most familiar with Windows applications and so the operational environment would be most effective if it resembles the Frontex ICT network.

2. Requirements Scope

This section shows what business functionality is in scope and out of scope for Implementation. There are many possibilities in implementing Article 11 of the Frontex regulation but this section will outline which functionalities are considered for PeDRA.

This section does not cover the scope of the data subjects which is included in the business case.

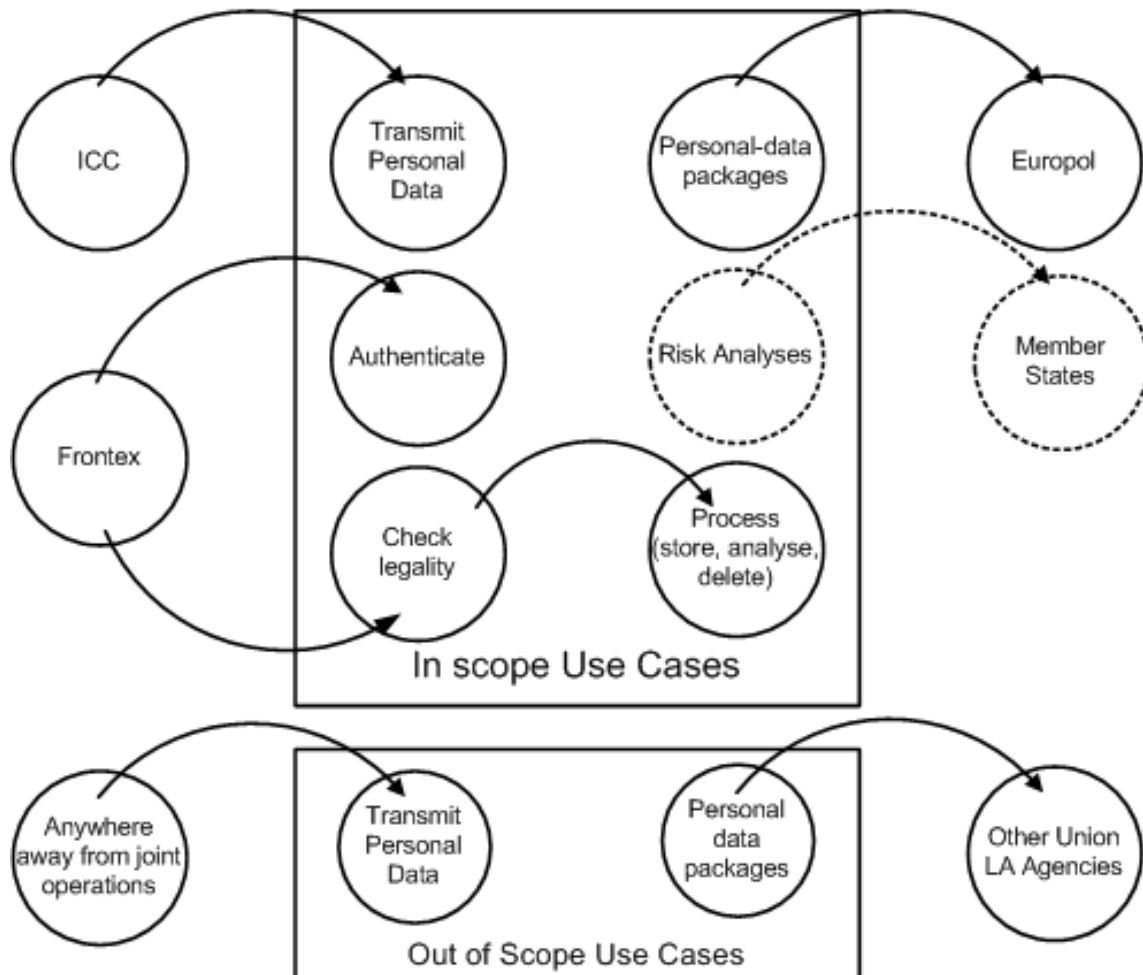


Figure 1 Actors and Use cases (in and out of scope) for the technical solution for PeDRA. Dotted lines show an in-scope use case that can exploit a pre-existing system. Some elements may not scale up to a fully implemented overall PeDRA project.

2.1. In Scope

The high level, in scope, business functions for the system are:

- **Authenticating:** this includes receiving the data from Member States, verifying the identity of the sender and acknowledging receipt. In cases where data are received from unknown sources data should not be accepted.

- Processing personal data: legality check: the personal data will be opened by a PeDRA Analyst to check that the data are legal, necessary and proportional. Further processing includes storing the [legally-checked] personal data in a secure manner. Limited (read-only) access to personal data processors (PeDRA analysts) will allow for data processing to take place to produce Personal Data Packages and depersonalised risk analysis reports. Data will be depersonalised after 90 days of the original transmission.
- Access management: the PeDRA team will manage access to the system in terms of personal data processors (analysts)

The high level, in scope, systems interfaces are:

- A single ICC transmitting daily reports to Frontex: daily reports containing personal data will be sent by a single ICC each day to Frontex.
- Send IPs to Europol: Once Personal Data Packages have been created they should be sent to Europol in a secure manner.

(Send Risk Analyses to Member States: Once depersonalised risk analyses have been produced they can be sent to Member States via regular channels. Hence this requirement can be met with a pre-existing system and is shown in dotted lines in Figure 1).

2.2. Out of Scope

The high level business functions that are out of scope are:

- Conducting investigations: Frontex is forbidden to conduct investigations

The high level systems interfaces that are out of scope are:

- All other ICCs, LCCs and team leaders transmitting daily reports to Frontex: other actors and locations will not be empowered to send daily reports containing personal data to Frontex.
- Send IPs to Other Union Law enforcement agencies: from a legal point of view Frontex can also transmit Personal Data Packages to other law enforcement agencies; however such transmissions must be based on specific working arrangements. No such arrangements exists and so this is out of scope of PeDRA.

3. Functional Requirements

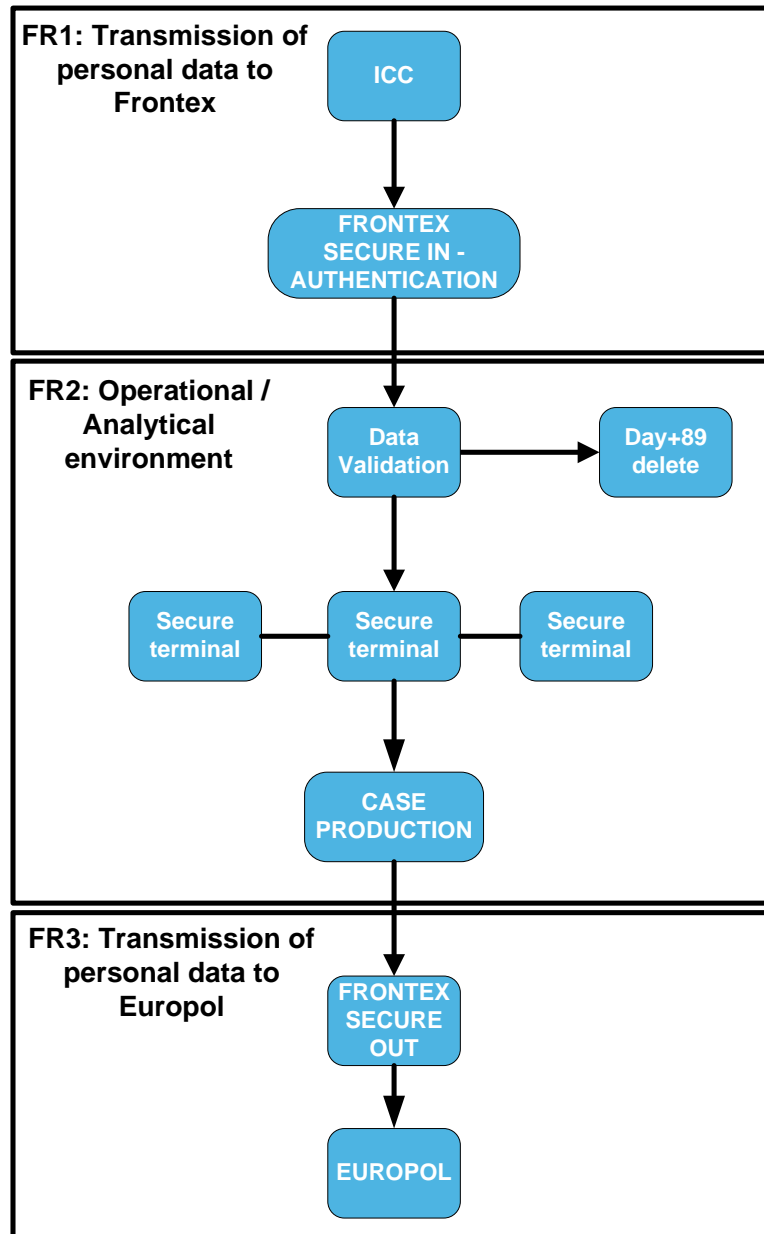


Figure 2 The three categories of functional requirements for PeDRA

3.1. Actor Profiles Specification

This section describes all the Actors and their profiles within the context of the Business Requirements being documented. An Actor is a person or organization that has interactions

with the system. Actors, by definition, are external to the system with which they are having interactions. Actors have goals that are achieved by use cases. Typically, Actors have behaviour and are represented by the roles they play in the use cases. An Actor stimulates the system by providing input and/or receiving something of measurable value from the system.

Essentially there are 4 categories of users for the system. Firstly the Member State ICC is a provider, as this location will send the daily reports that form the basic unit of storage in the system. This sending or transmission is the sole role of the ICC.

RAU is the second actor that will use the system and there will be 2 levels of needs. Firstly the analysts that will be authorised as personal data processors will need read-only access to the daily reports. This read-only access should prohibit renaming files, or storing in original or new locations as this will vastly complicate the deletion of expired data. Case production will involve producing a new document to summarise and contextualise trends.

The second actor in RAU is the PeDRA project management team that will need a higher level of access than the data processors. First the team will be able to store daily reports once the legality has been checked. Immediately after the legality check is the only time that a daily report will ever be stored. The team will also need to be able to send Personal Data Packages containing daily reports to Europol. Finally the team will need to be able to delete Personal Data Packages and all expired personal data.

Table 3 Actors and access types for the technical solution for PeDRA

Actor Name	Actor Type (as in section 1.7)	Access Type needed	Comments
Europol	<input checked="" type="checkbox"/> Recipient <input type="checkbox"/> Supplier <input type="checkbox"/> Producer <input type="checkbox"/> Manager	<input type="checkbox"/> Store <input type="checkbox"/> Export <input type="checkbox"/> Read <input checked="" type="checkbox"/> Receive <input type="checkbox"/> Delete <input type="checkbox"/> Transmit	Needs to be able to receive IPs in a secure manner. They will then import into their own system and hence will not need any other type of access to the PeDRA system
Member State ICC	<input type="checkbox"/> Recipient <input checked="" type="checkbox"/> Supplier <input type="checkbox"/> Producer <input type="checkbox"/> Manager	<input type="checkbox"/> Store <input type="checkbox"/> Export <input type="checkbox"/> Read <input type="checkbox"/> Receive <input type="checkbox"/> Update <input checked="" type="checkbox"/> Transmit	Needs to be able to transmit daily reports to the system
RAU Authorised Data Processors (Analysts)	<input type="checkbox"/> Recipient <input type="checkbox"/> Supplier <input checked="" type="checkbox"/> Producer <input type="checkbox"/> Manager	<input type="checkbox"/> Store <input type="checkbox"/> Export <input checked="" type="checkbox"/> Read <input type="checkbox"/> Receive <input type="checkbox"/> Delete <input type="checkbox"/> Transmit	Limited (read-only) data access to daily reports for analytical tasks.
RAU PeDRA Project Team	<input type="checkbox"/> Recipient <input type="checkbox"/> Supplier <input type="checkbox"/> Producer <input checked="" type="checkbox"/> Manager	<input checked="" type="checkbox"/> Store <input checked="" type="checkbox"/> Export <input checked="" type="checkbox"/> Read <input type="checkbox"/> Receive <input checked="" type="checkbox"/> Delete <input type="checkbox"/> Transmit	Storage of personal data, creation of folders, data processing, deletion of expired data, sending IPs to Europol

3.2. Essential Use Case Diagram

This section depicts the Business Requirements in the form of Essential Use case diagram. In the Use case approach, the Functional Requirements are decomposed into a number of Essential Use cases. Essential use cases are of primary importance early in a project's requirements/analysis phase. Their purpose is to document the business process that the Application must support without bias to technology and implementation.

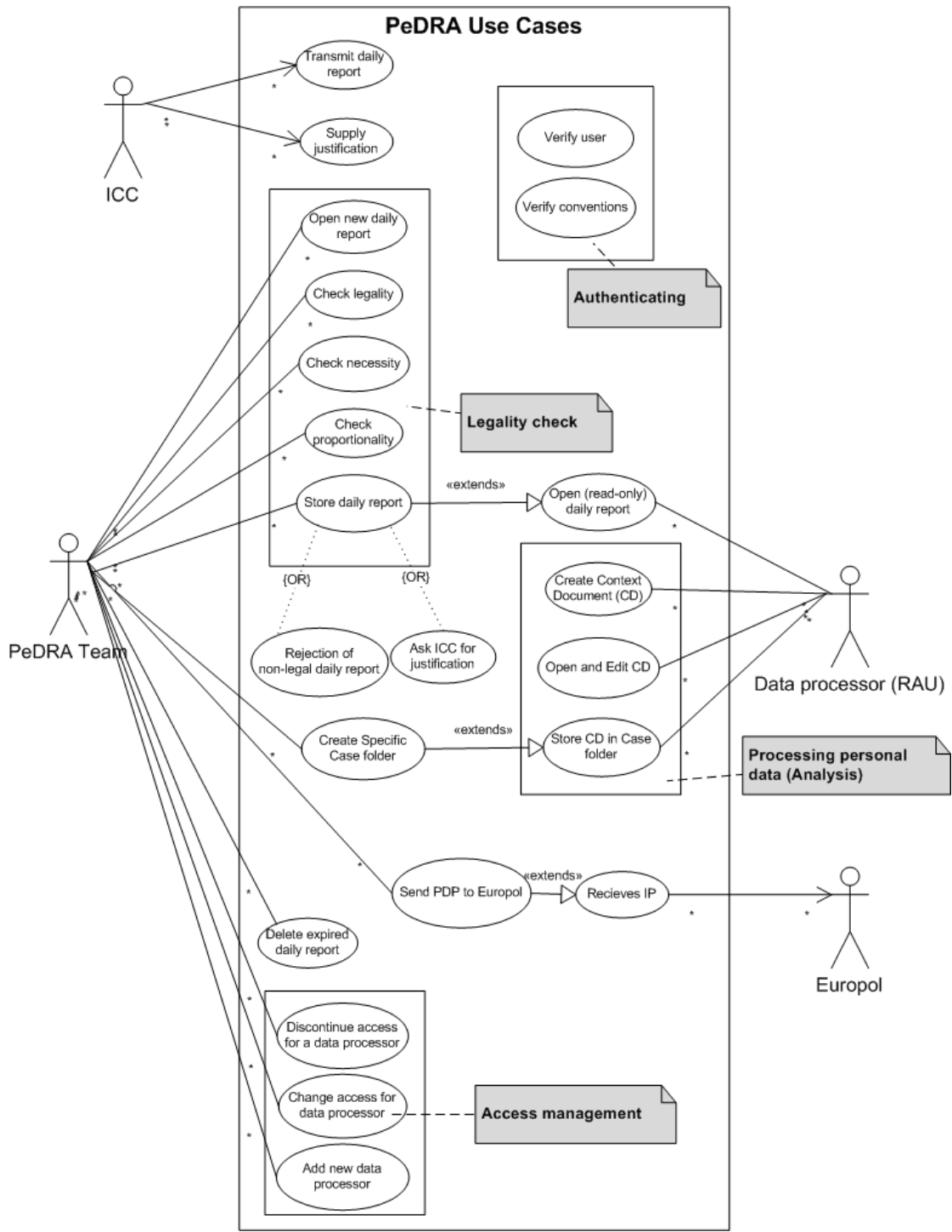


Figure 3 Essential use cases for PeDRA. Business functions are in four categories: Authentication, legality check, data processing/analysis and access management

3.3. Essential Use Case Specifications

This section describes each Essential Use case in tabular form. A use case typically has one basic course of action and one or more alternate courses of actions.

Use Case Name	1. ICC Transmit
Description	ICC uses the system to send a daily report package to Frontex
Actors	Authorised personnel in the ICC
Business Rules	Data Input, Data subjects, Data Source, Data legality,
Basic Flow	Alternate Flows
Member State representatives in debriefing teams conduct interviews and collect personal data. Teams can comprise of either national experts coordinated by national authorities, or may be Guest Officers (also Member State representatives) deployed and coordinated by Frontex.) Debriefing reports are sent to ICC under national data protection rules, often via the Member State team leader. This work stream is already in existence. With this system the ICC will then be able to send daily reports containing personal data to Frontex	An alternate flow is a scenario other than the basic flow that leads to success. An alternate flow may deal with a user error as long as it is recoverable. In this case there is little flexibility as the procedure is already in place for MSs. There may be cases where the daily reports are not attached to the message, in which case the system should notify the ICC that a message is being sent with no attachments.
Non-Functional Requirements	<ul style="list-style-type: none"> - Access to the transmission system should be limited to authorised personnel in the ICC - Authorised personnel at the ICC should have to log in to the transmission software with passwords - Access management will be agreed in the operational plan - The system will only be able to send to a single destination - Frontex - Mobile access to the system is not necessary - The transmission system should retain a log of all messages transmitted by the ICC and whether or not they were accepted - The system should be secure enough it ensure that only the ICC and Frontex should have access to view the transmission - The system should as much as possible resemble e-mail, as this is the functionality already deployed for sending daily reports (with personal data omitted) to Frontex. This will increase the likelihood that personal data are shared. - The transmission from ICC to Frontex should take less than 1 hour

	<ul style="list-style-type: none"> - The system should exploit existing network infrastructure as much as possible - There should be a help function within the system for when the ICC is not able to gain access or use its functionality
Pre-Conditions	Member States representatives (Guest officers and others) continue to collect personal data during interviews and are willing and able to use the system to transmit to Frontex.

Use Case Name	2. Authentication
Description	The system automatically checks the source (sending address) of a received transmission and checks the naming conventions of the files.
Actors	The System
Business Rules	Authenticate (1) and (2)
Basic Flow	Alternate Flows
The system receives a transmission and checks its source, because the system is only permitted to receive transmissions from a single predefined source i.e. the ICC. Also the system needs to check the naming convention of the files, to make sure that they were produced and sent by authorised personnel in the ICC.	<p>If the transmission has come from an unexpected source then it is not passed on for the legal check, the PeDRA team should be notified.</p> <p>If the files do not comply with agreed-upon naming conventions, then the transmission is not passed on for the legal check. The PeDRA team should be notified that a transmissions was received from an expected source but did not conform to naming conventions.</p>
Non-Functional Requirements	<ul style="list-style-type: none"> - The authentication process should be automatic rather than manual - Authenticated transmissions should be available within 10 minutes for the PeDRA team to begin the legality check - Authentications and the results should be logged
Pre-Conditions	Transmission received in the system

Use Case Name	3. Notify ICC of unauthenticated transmission
Description	ICC is informed that a transmission was not accepted
Actors	PeDRA Team
Business Rules	
Basic Flow	Alternate Flows
A transmission was not authenticated because files did not comply with naming conventions. The PeDRA team are notified of the authentication fail and the reason, and then the PeDRA team can communicate this to the ICC and invite them to re-transmit.	None

Non-Functional Requirements	- The communication does not have to be secure as it will not contain personal data
Pre-Conditions	A transmission was not authenticated because of non-compliance with naming conventions

Use Case Name	4. Daily report - Open
Description	The PeDRA team unzip or open the daily reports and view the contents
Actors	PeDRA Team
Business Rules	Post authentication access
Basic Flow	Alternate Flows
Report is known to have been sent from ICC, automatically authenticated, and action is started by PeDRA Team to open content	None
Non-Functional Requirements	<ul style="list-style-type: none"> - Opening the daily report should be a few-click operation like unzipping files - Access to authenticated reports should be limited to the PeDRA team so that they can perform the legality check
Pre-Conditions	<ul style="list-style-type: none"> - Transmissions that failed the authentication process (i.e. came from unexpected source) should be visible but not accessible - Daily report should be visible and available within minutes of successful authentication

Use Case Name	5. Check legality
Description	The PeDRA team examine the personal data contained in the daily report files. Then they assess whether the personal data are legal according to the Frontex mandate, and that they are proportional in detail and volume, and necessary for analytical purposes.
Actors	PeDRA Team
Business Rules	Data subjects, Data source, Data legality
Basic Flow	Alternate Flows
Report is known to have been authenticated, and open, the action is started by PeDRA Team to check the content by looking at the data subjects and source and by making sure that it complies with the principles of proportionality and necessity.	None

Non-Functional Requirements	<ul style="list-style-type: none"> - It should be possible to open all expected file formats and view their contents on the screen - Standard file formats such as MS Office, images, PDFs and video should be viewable - Analytical file formats (SAS, i2, JMP, XML, UMF) will not be expected in daily reports - The process should be logged
Pre-Conditions	Completed authentication, and files opened by PeDRA team

Use Case Name	6. Daily report storage
Description	The PeDRA team store the legally checked daily report files in a specific location
Actors	PeDRA Team
Business Rules	Storage
Basic Flow	Alternate Flows
PeDRA Team member stores the daily report files in predetermined single locations (as per ICC and date) and without changing filenames.	None
Non-Functional Requirements	<ul style="list-style-type: none"> - The files should be easily stored within a hierarchical folder system in a predetermined folder for the specific ICC and date - There is no need for storage on other media - There is no need to export the data from the system to an external location - There should be no print facility from the PeDRA system - Only the PeDRA team are able to store personal data - The storage process should be logged, as well as all other subsequent processes (read, close, store)
Pre-Conditions	Completed authentication, files opened and passed legality check.

Use Case Name	7. Rejection of non-legal daily report
Description	The PeDRA team reject the daily report for one of the following reasons. Data were not; <ol style="list-style-type: none"> 1. Legal according to Art 11 2. Proportional 3. Necessary
Actors	PeDRA Team
Business Rules	Non-acceptance

Basic Flow	Alternate Flows
PeDRA Team member does not store the daily report as it contains suspected non-legal data. Instead a decision will be made as to whether or not to contact ICC for justification.	None
Non-Functional Requirements	<ul style="list-style-type: none"> - The files should be easily closed without storage - No automatic save functions should be present
Pre-Conditions	Completed authentication, and files opened and checked for legality, proportionality and necessity but fail on at least one count

Use Case Name	8. Ask ICC for justification
Description	The PeDRA team request justification for one of the following: <ol style="list-style-type: none"> 1. the data subject was suspected on reasonable grounds of involvement in facilitation, THB or CBC 2. Data were collected during or in the context of Frontex operational activity 3. data are proportional 4. data are necessary
Actors	PeDRA Team
Business Rules	Justification
Basic Flow	Alternate Flows
PeDRA Team member contacts the ICC and asks a specific question regarding the legality, proportionality or necessity of a specific piece or group of personal data	None
Non-Functional Requirements	<ul style="list-style-type: none"> - The communication should be secure as it may contain personal data - The communication should resemble e-mail and be similarly immediate
Pre-Conditions	Completed authentication, and files opened and checked for legality, proportionality and necessity but fail on at least one count

Use Case Name	9. ICC respond to request for justification
Description	The ICC provide justification for sending personal data to Frontex, or decline to justify and withdraw transmission
Actors	PeDRA Team

Business Rules	Justification response
Basic Flow	Alternate Flows
The ICC responds to the request for justification in one of the following ways: <ol style="list-style-type: none"> 1. by stating why the subject was suspected on reasonable ground of being involved in facilitation, THB or CBC. 2. by justifying the proportionality 3. By justifying the necessity 4. By acknowledging a lack of legality and asking for the original transmission to be disregarded 	None
Non-Functional Requirements	<ul style="list-style-type: none"> - The communication from the ICC should also be secure as it will probably contain personal data - The communication should resemble e-mail and be similarly immediate
Pre-Conditions	Completed authentication, and files opened and checked for legality, proportionality and necessity but fail on at least one count, and message sent to ICC from Frontex asking for justification.

Use Case Name	10. Processors open daily reports
Description	Authorised personal data processors have read only access to open daily reports
Actors	Personal data processors
Business Rules	-
Basic Flow	Alternate Flows
Personal data processors (analysts) open the daily reports to read and analyse the contents	None
Non-Functional Requirements	<ul style="list-style-type: none"> - The operational environment should be separate from the Frontex network, possibly on other terminals in RAU without internet access - Access to the operational environment should be controlled by a strict security policy (passwords etc), in excess of the Frontex network - Authorised data processors should only have read-only access to the stored daily reports sent from the operations they are assigned to (land, sea, air etc) - File names should not be changeable - It should not be possible for the processors to store the daily reports in different locations

Pre-Conditions	Completed authentication, and files opened and checked for legality, proportionality and necessity and stored in correct location by PeDRA team
-----------------------	---

Use Case Name	11. Processors create an additional file
Description	Authorised personal data processors create an additional file that contains personal data from the daily reports. Two types of additional file only – each with a blank template already created.
Actors	Personal data processors
Business Rules	Additional files
Basic Flow	Alternate Flows
<p>Personal data processors (analysts) use personal data from the daily reports to create an additional file. Additional files can be either analytical files ([REDACTED]) or context documents in MS word.</p> <p>Analytical files may be summaries such as lists of facilitator names and phone numbers used to search against new daily reports.</p> <p>Analytical files may also be Context documents that will be created in cases to be sent to Europol and will contain some personal data to illustrate trends.</p>	None
Non-Functional Requirements	<ul style="list-style-type: none"> - Additional files (analytical files or context documents) will have blank templates created by the PeDRA team containing predetermined structure and also suggestions for information - Documents should be created easily with a NEW command in a system that resembles MS Office - There should also be an export function or copy/paste from daily reports into additional files - Context documents can only be stored in specific case folders created by the PeDRA team (Use case = Create case folder)
Pre-Conditions	Decision taken by PeDRA team to create additional file that contains personal data

Use Case Name	12. Store additional file
Description	Authorised personal data processors store an additional document.
Actors	Personal data processors

Business Rules	Store additional file
Basic Flow	Alternate Flows
Personal data processors (analysts) store new analytical files and Context documents in a secure and predetermined location, with a naming convention	None
Non-Functional Requirements	<ul style="list-style-type: none"> - Additional files containing personal data should be stored securely - Analytical files and context documents should be available for all authorised personal data processors and the PeDRA team so that analyses can be performed at the EU level.
Pre-Conditions	Daily reports authenticated, and checked for legality, proportionality and necessity and stored in correct location by PeDRA team.

Use Case Name	13. Open and edit additional document
Description	Authorised personal data processors open pre-existing additional documents, edit the contents and then store the revised version.
Actors	Personal data processors
Business Rules	Additional files, Store additional file
Basic Flow	Alternate Flows
Authorised personal data processors open pre-existing additional documents, edit the contents and then store the revised version.	None
Non-Functional Requirements	<ul style="list-style-type: none"> - Additional document should be accessible only by authorised personal data processors and the PeDRA team - A full version history should be maintained
Pre-Conditions	Daily reports authenticated, and checked for legality, proportionality and necessity and stored in correct location by PeDRA team.

Use Case Name	14. Create Case Folder
Description	The PeDRA team will create folders within the system in order for analysts to store additional documents within them
Actors	PeDRA Team
Business Rules	Case production

Basic Flow	Alternate Flows
The PeDRA team will decide that a new case or analysis is required so they will create the folder in a suitable place and with a predetermined name convention	None
Non-Functional Requirements	- The folder should be accessible only by authorised personal data processors
Pre-Conditions	New analysis or case deemed necessary

Use Case Name	15. Send case to Europol
Description	The PeDRA team will send cases to Europol
Actors	PeDRA Team
Business Rules	Transmission
Basic Flow	Alternate Flows
The PeDRA team will decide that a new case has been concluded, with at least a context document and some daily reports. These will then need to be sent to Europol in a secure manner.	None
Non-Functional Requirements	- Access to the send facility will need to be limited to the PeDRA team - Decision to send will be taken by the PeDRA team leader
Pre-Conditions	New analysis or case concluded and decision to send

Use Case Name	16. Case received by Europol
Description	Europol will receive a case from Frontex
Actors	Europol
Business Rules	Case reception
Basic Flow	Alternate Flows
Europol will be the only recipient of a case containing daily reports (of part thereof) and a context document	None
Non-Functional Requirements	- Europol will need to ensure that access to the system is limited to authorised personnel e.g. AWF Checkpoint
Pre-Conditions	Case sent by Frontex
Use Case Name	Case rejected by Europol
Description	Europol will reject a case from Frontex

Actors	Europol
Business Rules	Case rejection
Basic Flow	Alternate Flows
Europol will reject the Personal Data Package for data protection reasons i.e. that the data are not necessary or proportional	None
Non-Functional Requirements	<ul style="list-style-type: none"> - Europol will not store the data but will instead need to contact Frontex to explain why the data were not accepted. - This should then feed into our understanding of what Europol needs are, and future decisions to send Personal Data Packages to Europol
Pre-Conditions	Case sent by Frontex but rejected by Europol

Use Case Name	17. Delete expired data
Description	All personal data that has been within Frontex for 90 days must be deleted
Actors	PeDRA Team
Business Rules	Expired data
Basic Flow	Alternate Flows
<p>Daily reports will be deleted manually 89 days after they were received. This is defined by the date that the transmission was received (prior to the authorisation and legality checks)</p> <p>There will be process in the PeDRA team to make sure that this task is always completed.</p> <p>Similarly the expired data will be deleted from additional files (analytical files and context documents) or will be depersonalised.</p>	None
Non-Functional Requirements	<ul style="list-style-type: none"> - Personal data will be deleted from the PeDRA system - Daily backups will remain for not longer than 90 days
Pre-Conditions	Personal data arrived in Frontex 89 days previously and passed the authentication and legality check and was then stored in the system.

Use Case Name	18. Access management
Description	Access to the daily reports, and additional files will be managed by the PeDRA team
Actors	PeDRA Team
Business Rules	Analyst access
Basic Flow	Alternate Flows
Newcomers will be granted access to the daily reports and additional files when necessary. Level of access will be kept to a minimum necessary. Users will be deleted from user list when they leave or are assigned different tasks	None
Non-Functional Requirements	<ul style="list-style-type: none"> - Access management should be limited to the PeDRA team - Access management should be simple to perform
Pre-Conditions	A change in staffing would necessitate a change in access rights

3.4. Business Rules

This section lists and describes the business rules applicable to the proposed system.

Business Rule Id	Rule Name	Rule Description	Rule Source
BR1	Authenticate (1)	Daily reports containing personal data can only be accepted from a single source (the one ICC)	Project scope
BR2	Authenticate (2)	Daily reports can only be accepted if they comply with naming conventions	Project scope
BR3	Data Subjects	Data subjects can only be individuals suspected by MS on reasonable grounds of being involved in facilitation, THB or CBC	Article 11c Operational plan
BR4	Authenticate fail (1)	If a transmission is received from an unexpected source, it should not be authenticated and the PeDRA manager should be informed. No unauthorised communication should be made with the unidentified sender.	Implementing rules
BR5	Authenticate fail (2)	If a transmission is received with files that do not comply with naming conventions it will not be authenticated and the PeDRA team	Implementing rules

		should be informed. The ICC may be contacted to invite to retransmit.	
BR6	Data Source	Personal data can only be collected by Member States during or in the context of Frontex operational activity	Article 11c Operational plan
BR7	Data uses	Personal data can only be used for risk analyses and for transmission on a case-by-case basis to Europol	Article 11c Operational plan
BR8	Data expiry	Personal data shall be deleted after it has been in the agency for 3 months	Article 11c Operational plan
BR9	Data legality	Personal data shall comply with the principles of proportionality and necessity	Article 11c Operational plan
BR10	Data use (2)	Frontex will not use personal data for investigations	Article 11c
BR11	Data transmission	Frontex will not transmit personal data to third countries or third parties	Article 11c
BR12	Data input	The ICC shall transmit daily reports to Frontex using the new secure channel	Operational plan
BR13	Post Authentication access	Access to authenticated transmissions shall only be granted to the PeDRA team	Implementing rules
BR14	Storage	Storage of the daily reports can only be conducted by the PeDRA team, post validation	Implementing rules
BR15	Analyst access	Analysts can only have read only access to the daily reports	Implementing rules
BR16	Transmission	Only the PeDRA team can send cases to Europol	Implementing rules
BR17	Case production	Only the PeDRA team can create new cases	Implementing rules
BR18	Justification	Only the PeDRA team can contact the ICC to ask for justification	Implementing rules
BR19	Additional files	Analysts can create additional files that contain personal data: either context files or analytical files	Implementing rules
BR20	Expire data	Only the PeDRA team can delete expired daily reports	Implementing rules
BR21	Non-acceptance	Only the PeDRA team can decide not to accept daily reports based on lack of legality or justification	Implementing rules
BR22	Justification response	The ICC is allowed to provide proof of suspicion of the data subjects, confirmation of the data source and justification that the personal data were legal	Implementing rules
BR23	Store additional file	Personal data processors store and additional file (analytical file or context document) in a predetermined location and with a strict naming convention	Implementing rules
BR24	Case reception	Europol will need to access the system in a secure manner in order to access, open and store the case	Implementing rules

4. Data Requirements

4.1. Data Architecture

Daily reports with personal data removed, currently arrive as ZIP files. The new system should emulate this format as much as possible in order to reduce procedural change at the ICC. The raw daily reports will have meta data associated with them such as date and time, but will not usually be quantitative. Therefore it is not foreseen that a data architecture need be developed.

4.1. Data Volumes

One report will be sent per day for the duration of the Pilot Exercise (*duration yet to be agreed*). Some daily reports have in the past exceeded 30MB in size as they contain power points presentations including maps of the operational area, and daily events. Not all of these documents contain personal data but for the sake of continuity and to save processing time all files sent with the daily reports will be stored in the PeDRA system.

4.2. Data Retention and Archiving

According to Article 11c all personal data should be deleted after 3 months. This issue is still under discussion as there is a clear business need and judicial obligation to be able to refer back to data at a later date. One option would be to have an archive outside of the operational area and beyond the access of the analysts and also the PeDRA Team. This would be managed by the DPO rather than the PeDRA team. This archive would only be used in the case of a request to verify data from the judiciary or in the case of a request from a data subject – to be clarified.

5. Non-Functional requirements

4.2. Non-functional requirements 1 (NFR1) - Transmission of personal data to Frontex

- Access to the transmission system should be limited to authorised personnel in the ICC
- Access to the transmission software for authorised personnel at the ICC should be controlled by a strict security policy (passwords etc)
- Access management should remain with Frontex ICT in coordination with RAU
- Mobile access to the system is not necessary
- The transmission system should retain a log of all messages transmitted by the ICC
- Only the ICC and Frontex should have access to view the transmission

- The system should as much as possible resemble e-mail, as this is the functionality already deployed for sending daily reports (with personal data omitted) to Frontex. This will increase the volume of data shared.
- The transmission process should be near to immediate
- The authentication process (checking identity of sender, and file naming conventions) should be automatic so that authenticated transmissions are immediately available for data processors
- The system should exploit existing network infrastructure as much as possible
- There should be a contact help function within the system for when the ICC is not able to gain access or use its functionality

4.3. Non-functional requirements 2 (NFR2) - Creation of a secure operational/analytical environment

- The operational environment should be conceptually (or technically) separate from the Frontex network, possibly on other terminals without internet access etc
- Access to the operational environment should be controlled by a strict security policy (passwords etc) in excess of the normal access passwords of Frontex IT
- Access will be limited to authorised personnel, and management will be controlled by the data controller HoRAU
- Access to the *sent* daily reports will be limited to authorised personnel, so that only specific people can perform legality checks and act upon the results
- Only authorised personnel will be able to contact the ICC regarding the legality of the personal data
- Access to the stored daily reports will be limited to authorised personnel
- Authorised data processors should only have read-only access to the stored daily reports sent from the operations they are assigned to
- Members of the PeDRA team will have full access to the stored daily reports
- File names should not be changeable
- It is not necessary for the system to process classified material
- Access to the operational area will be limited to authorised personnel

4.4. Non-functional requirements 3 (NFR3) - transmission of Personal Data Packages to Europol

- Frontex staff should have to log in to the transmission software according to a strict security policy
- Access should be limited to authorised personnel
- Access management should remain with Frontex ICT
- System should be compatible with the Europol system

5.1. Security Requirements

The system must comply with security requirements according to Article 22 of the data protection legislation 45/2001. This stipulation is essential to protect the rights of the data subjects where applicable, and to protect the Agency from reputational damage associated with a suspension of its tasks.

1. Having regard to the state of the art and the cost of their implementation, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected.

Such measures shall be taken in particular to prevent any unauthorised disclosure or access, accidental or unlawful destruction or accidental loss, or alteration, and to prevent all other unlawful forms of processing.

2. Where personal data are processed by automated means, measures shall be taken as appropriate in view of the risks in particular with the aim of:
 - a) preventing any unauthorised person from gaining access to computer systems processing personal data;
 - b) preventing any unauthorised reading, copying, alteration or removal of storage media;
 - c) preventing any unauthorised memory inputs as well as any unauthorised disclosure, alteration or erasure of stored personal data;
 - d) preventing unauthorised persons from using data-processing systems by means of data transmission facilities;
 - e) ensuring that authorised users of a data-processing system can access no personal data other than those to which their access right refers;
 - f) recording which personal data have been communicated, at what times and to whom;
 - g) ensuring that it will subsequently be possible to check which personal data have been processed, at what times and by whom;
 - h) ensuring that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the contracting institution or body;
 - i) ensuring that, during communication of personal data and during transport of storage media, the data cannot be read, copied or erased without authorisation;
 - j) designing the organisational structure within an institution or body in such a way that it will meet the special requirements of data protection.

Annex 1 Business requirements

There needs to be a system in place which takes care of three main functional requirements:

- FR1) secure transmission of personal data from a single ICC to Frontex;
- FR2) a secure operational/analytical environment for storage of the data, logging of each process, analysis of the personal data, case production and expired data deletion;
- FR3) secure transmission of Personal Data Packages to Europol.

Functional requirements (what the system should do – behaviour or function)

Functional requirements 1 (FR1) - Transmission of personal data to Frontex

- A single ICC needs to be empowered to enable them to transmit daily reports containing personal data to Frontex in a manner sufficiently secure to comply with the security requirements laid out in the data protection legislation 45/2001
- At the Frontex end, a secure reception system should only accept transmissions from this single, predetermined source
- At the Frontex end, a secure reception system should only accept transmissions that comply with specific naming conventions
- The data will be zip files (n<=10 per transmission)
- There will be one report sent per day
- The size of the attachments will not exceed 50MB
- The reception system should notify the ICC each time when a message has been accepted or rejected

Functional requirements 2 (FR2) - Creation of a secure operational/analytical environment

- A secure environment needs to be created to enable authorised personal data processors to open the zip files. This could be a number of dedicated secure terminals in RAU only for the purpose of opening and processing daily reports.
- Data processors will need check the legality of the data (proportional, necessary and compliant with Art 11c para 2) by extracting and examining their contents. Files will be PDF, Microsoft Office or media files
- Non-legal data will be deleted and the ICC will be notified by the PeDRA Project Manager
- If is not possible to clarify the legality of the data, the ICC will be contacted by the PeDRA Project Manager for justification of their reasonable grounds
- Legal data will be stored in a secure manner by the personal data processor, compliant with data protection legislation
- Personal data processors should be able to analyse any stored personal data to support risk analysis processes, and for case production
- Analysis will include creating new Microsoft Office data files, standard quantitative analyses ██████████, network analysis ██████████
- Each process should be logged (opening, analysing, creating new files, editing etc)
- The system should highlight for anonymising daily reports that have been stored for 90 days

Functional requirements 3 (FR3) – transmission of Personal Data Packages to Europol

- The PeDRA Project Manager will oversee the production of Personal Data Packages within the secure operational/analytical area.
- Personal Data Packages will contain aspects of the original daily reports, supported by additional material
- The PeDRA Project Manager will need to transmit Personal Data Packages to Europol in a manner sufficiently secure to comply with the security requirements laid out in the data protection legislation 45/2001

Non-functional requirements (how the system should achieve it -measurable)

Non-functional requirements 1 (FR1) - Transmission of personal data to Frontex

- Access to the transmission system should be limited to authorised personnel in the ICC
- Authorised personnel at the ICC should have to log in to the transmission software with according to strict security policy (passwords etc)

- Access management should remain with Frontex ICT in coordination with RAU
- Mobile access to the system is not necessary
- The transmission system should retain a log of all message transmitted by the ICC
- Only the ICC and Frontex should have access to view the transmission
- The system should as much as possible resemble e-mail, as this is the functionality already deployed for sending daily reports (with personal data omitted) to Frontex. This will increase the volume of data shared.
- The transmission process should be near to immediate
- The authentication process (checking identity of sender, and file naming conventions) should be automatic so that authenticated transmissions are immediately available for data processors
- The system should exploit existing network infrastructure as much as possible
- There should be a contact help function within the system for when the ICC is not able to gain access or use its functionality

Non-functional requirements 2 (FR2) - Creation of a secure operational/analytical environment

- The operational environment should be separate from the Frontex network, possibly on other terminals in RAU without internet access
- The operational environment should controlled by a strict security policy (password access etc) protected, in excess of the normal access of Frontex IT
- Access will be limited to authorised personnel, and management will be controlled by the data controller HoRAU
- Access to the *sent* daily reports will be limited to authorised personnel, so that only specific people can perform legality checks and act upon the results
- Only authorised personnel will be able to contact the ICC regarding the legality of the personal data
- Access to the stored daily reports will be limited to authorised personnel
- Authorised data processors should only have read-only access to the stored daily reports sent from the operations they are assigned to
- Members of the PeDRA team will have full access to the stored daily reports
- File names should not be changeable
- It is not necessary for the system to process classified material
- Access to the operational area will be limited to authorised personnel
-

Non-functional requirements 3 (FR3) - transmission of Personal Data Packages to Europol

- Frontex should have to log in to the transmission software with according to a strict security policy (passwords, etc)
- Access should be limited to authorised personnel
- Access management should remain with Frontex ICT
- System should be compatible with the Europol system

Frontex**Joint Operations Reporting Application
and PeDRA****Version 0.1**

Document Information

Document Title	JORA and PeDRA
Project Name	PeDRA
Author	██████████
Reviewer	
Consulted Contributors	FSC, RAU, ICT
Owner of the Document	FSC
Owner of the Process	RAU
Date of Document	2014/15
Status	Consolidated in Frontex, submission to EDPS
Version	0.1

Reference documents

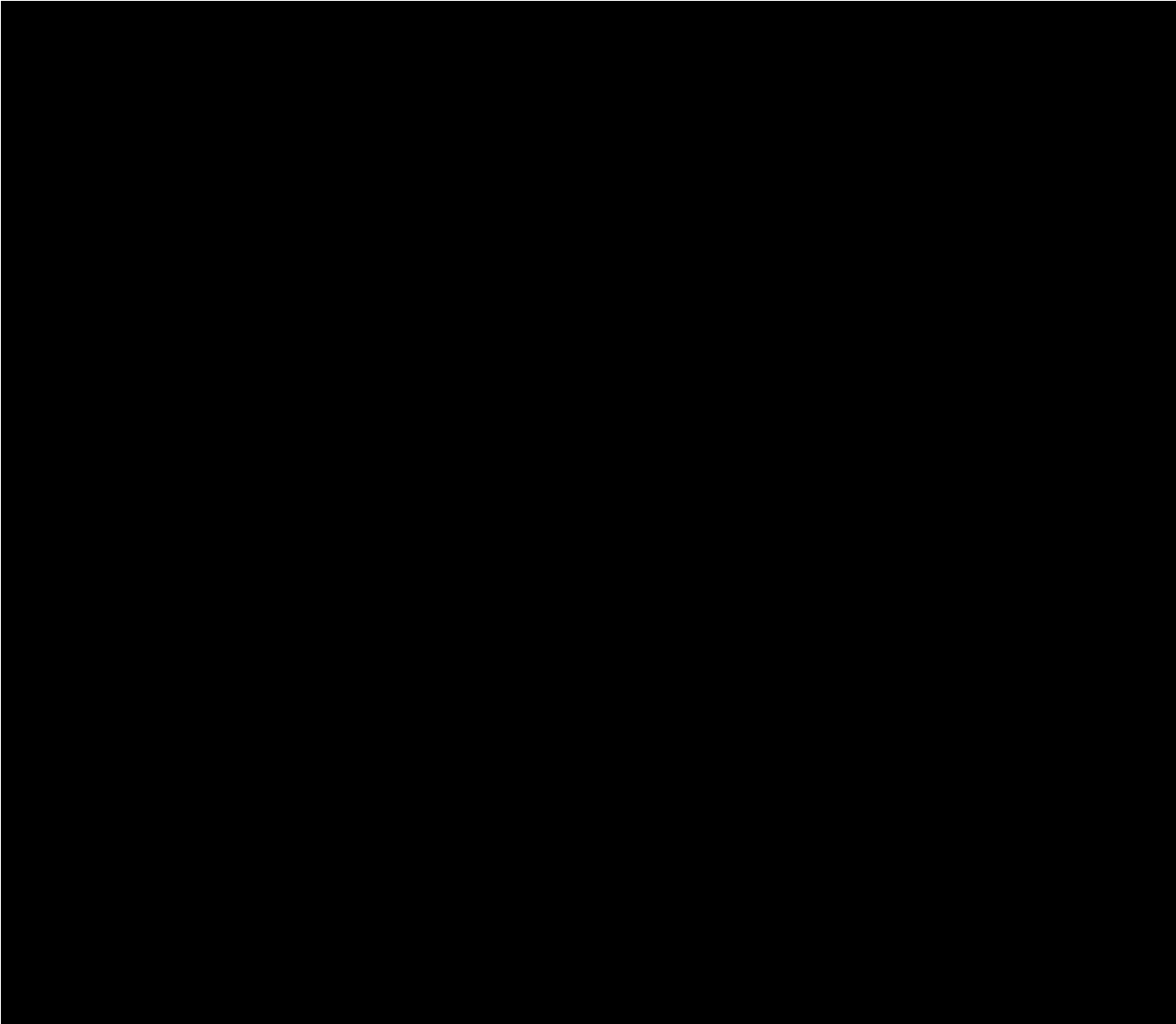
Title	Author	Date
JORA and PeDRA concept	FSC	07.03.2015
PeDRA Business Case v4	RAU	04.12.2014
PeDRA Business Requirements Documentation v4	RAU	03.06.2014
PeDRA Project Initiation Documentation	RAU	09.10.2014

Amendment records

Date	Amendment	Chapter/Page	Author
13.03.2015	Comments and additional text	Many	RAU (TW)
18.03.2015	Final document for EDPS submission	Many	FSC (LGCs)

Table of Contents

- 1. General 4
- 1.1. Description of PeDRA 4
- 1.2. Personal data processing in JORA system 4



2. General

2.1. Description of PeDRA

To make more efficient use of personal data collected by Member States during Frontex joint operations, the 2011 amendment to the Frontex regulation allows the Agency to further process personal data collected by Member States during Frontex Joint Operations, and PeDRA is the first step in allowing Member States to transmit such personal data in a secure manner to Frontex for further processing at the EU level.

PeDRA will contribute to the following strategic objectives: preventing loss of life, reducing the risk of exploitation of vulnerable groups and increasing border security. In tangible terms the measurable benefits from the PeDRA project will be increased inhibitions, detections and arrests of facilitators and traffickers made possible by a more effective operational response at the border by Member States and Frontex and more successful investigations by Europol. These strategic objectives and measurable benefits will be made possible because of the project outputs, which are legally limited in the Frontex Regulation as: 1) Risk analyses, the results of which will be depersonalised, and 2) Personal Data Packages (PDPs) to be transmitted to Europol on a case-by-case basis. For more information on the benefits and business options see the PeDRA Business Case v4.

Stage I of PeDRA was launched in October 2014 after the PID was endorsed by the Directorate in September 2014. Stage I has five parallel work streams:

WS1 New Implementing rules

WS2 New Working Arrangement with Europol

WS3 Draft operational plan for Pilot Exercise

WS4 Design of proposed technical solution

WS5 EDPS notification

This document represents the output from WS4 - Technical solution. It serves the purpose of outlining the proposed steps in designing and installing a technical solution for:

1. Member States to transmit personal data to Frontex,
2. Frontex to process personal data, and
3. Frontex to transmit Personal data Packages to Europol

2.2. Personal data processing in JORA system

JORA (Joint Operation reporting Application) system is in operational use as of 1 January 2012 for all Frontex coordinated Joint Operations (land, sea, air and return operations). Since the system was introduced all Member States have been trained for the system, and managing the operational use of the system.

The JORA system has more than 3 200 users from all over Europe and more than 100 000 (incident) reports were submitted since the system is in operational use.

Using JORA is a good choice for Frontex in order to support personal data processing and PeDRA project due to the following reasons:

- JORA is used for all kind of operations coordinated by Frontex for more than 3 years and confirmed its value
- Since JORA was introduced to operational use in 2012 several new functions and modules were added to the system and the end users adopted the new functionalities easily
- The system has great number of trained end users from all EU Member States and Schengen Associated Countries
- Upgrading JORA would provide good cost-benefit ratio due to cost effective development and minimum training required for PeDRA reporting implementation in JORA
- JORA system was security audited and penetration tests were performed by external contractor and JORA system was updated regarding its security features in accordance with the findings during security audit

