Handbook to the Operational Plan

Joint Maritime Operations
# INDEX

**Table of Contents**

1. GUIDELINES FOR DEBRIEFING ACTIVITIES  
   1.1. Introduction 6  
   1.2. Debriefing 6  
   1.3. Tasks of Debriefing Experts  
      1.3.1. Preparation for debriefing 6  
      1.3.2. Identifying migrants for interview and checking belongings 8  
      1.3.3. Conducting debriefing sessions 8  
      1.3.4. Reporting 9  
   1.4. Use of Interpreters 10

2. GUIDELINES FOR SCREENING ACTIVITIES 11  
   2.1. Introduction 11  
   2.2. Screening 11  
   2.3. Tasks of Screening Experts 11  
   2.4. Preparation for screening 11  
   2.5. Checking belongings 11  
   2.6. Conducting screening interviews 12  
   2.7. Working as a team with interpreters 13  
   2.8. Results of screening interviews 13

3. GUIDELINES FOR FINGERPRINTING AND REGISTRATION 14  
   3.1. General Information 14  
   3.2. Tasks of experts 14  
      3.2.1. Informing of migrants 14  
      3.2.2. Use of force 15  
      3.2.3. Referral - Damage of the fingertips 15  
      3.2.4. Reporting 15  
   3.3. Use of cultural mediators / interpreters 15  
   3.4. Vulnerable groups 15

4. "HOT SPOTS" AND EU REGIONAL TASK FORCE 17  
   4.1. General Information 17  
   4.2. Roles of EU Agencies 17

5. FRONTEX ONE-STOP-SHOP (FOSS) 19  
   5.1. FOSS general Information 19  
   5.2. FOSS access procedures 19  
      5.2.1. FOSS access authorization 19  
   5.3. Roles & Responsibilities 21  
      5.3.1. National FOSS User Coordinator 21  
      5.3.2. Area of Interest Owner 21  
      5.3.3. User Administrator's (FSC) - FOSS Service Manager 21  
   5.4. Navigation In FOSS 21
6. COMMUNICATION WITH THE PRESS
6.1. Introduction
6.2. Press communication rules
   6.2.1. General
   6.2.2. Tasks of press offices in the context of Joint Operations
   6.2.3. Management of Press Requests
   6.2.4. Specific guidelines for participating officers if approached by the media
   6.2.5. Contact details

7. JOINT OPERATIONS REPORTING APPLICATION (JORA)
7.1. JORA General Information
   7.1.1. JORA product & service management
   7.1.2. JORA Roles and Responsibilities
7.2. JORA Access Request Procedure
   7.2.1. Background
   7.2.2. Initial Access Request to the JORA System
   7.2.3. Access Request to specific operation
   7.2.4. Access Request Process
7.3. Contact Details
7.4. JORA Incident Template Attributes’ List

8. SERIOUS INCIDENT REPORTING
8.1. Introductory Information
8.2. Definition
   8.2.1. Serious Incident (SI)
   8.2.2. Serious Incident Report (SIR)
8.3. Roles and responsibilities
   8.3.1. Participant of Frontex activities in the field
   8.3.2. Frontex staff in the operational area (FSO, FOC, etc.)
   8.3.3. Operational Manager (OM)
   8.3.4. FSC Senior Duty Officer (SDD)
8.4. Content of a SIR
8.5. SIR procedure - Chronology of reporting serious incidents
   8.5.1. Initial SIR
   8.5.2. Formal SIR
   8.5.3. Updated SIR
   8.5.4. Final SIR
8.6. Reporting of SI with alleged violation of fundamental rights (FR)
   8.6.1. Reporting mechanism
8.7. Frontex internal follow up procedure / SIR-Coordinator
8.8. Personal Data
8.9. Public access
8.10. Serious Incident Catalogue
   8.10.1. Serious Incident Categories
8.11. Serious incident Reporting Mechanism
8.12. List of potential fundamental rights violations within Frontex activities
9. ARRANGEMENTS OF DEPLOYED RESOURCES

9.1. Operational Resources Management System (Opera)

9.1.1. Responsibilities
9.1.2. Registration of Human Resources
9.1.3. Registration of Technical Equipment

9.2. Technical equipment deployed by Member States

9.3. Management of the operational assets deployed by Frontex

9.4. Firearms and ammunition transportation

10. PROCESSING PERSONAL DATA FOR RISK ANALYSIS (PeDRA)

PILOT EXERCISE FOR DEBRIEFING ACTIVITIES

10.1. Aims, objectives and description
10.2. Legal basis
10.3. Scope of personal data
10.4. Interoperability
10.5. Involved actors
10.6. Roles and responsibilities
10.7. Work flow and responsibilities under the PeDRA Pilot Exercise
10.8. What is personal data?
10.9. Access requests

11. OTHER FRONTEX PRODUCTS AND SERVICES

11.1. Eurosur Fusion Services

11.1.1. Introductory Information
11.1.2. Maritime Services
11.1.3. Vessel Detection Service
11.1.4. Weather Services
11.1.5. Other Services

11.2. Medium Altitude Long Endurance (MALE) Remotely Piloted Aircraft Systems (RPAS) aerial surveillance trial

11.3. Frontex Positioning System

11.4. Frontex Compatible Operational Image

11.5. Staff Exchange
11.6. Yellow Pages

12. TEMPLATES (EXAMPLES)

12.1. Serious Incident Report Template
12.2. Technical Equipment Mission Report
12.3. PeDRA Interview Template
12.4. Document Alert Template
12.5. User Access Request Form - FOSS
12.6. Intelligence Officer Report
12.7. Team Leader's Daily Report
12.8. Team Leaders - Landing Report
12.9. FSO Daily / Flash Report
12.10. Report from Participant
12.11. Final Report from Member State
12.13. JORA End-user Feedback Template 81
12.15. Weekly Advanced-Level Document Officer report 83
12.16. Daily screening report 85

13. ACRONYMS 86
1. GUIDELINES FOR DEBRIEFING ACTIVITIES

1.1. Introduction

As Frontex is an intelligence driven organization, its aim is to improve its intelligence capability enabling the Agency to better focus its activities, resulting in more effective operations.

At all types of borders, relevant information collected during interviews and debriefings can be effectively channelled to national authorities conducting border checks and surveillance or criminal investigations linked to facilitation and organized crime networks.

Interviewing activities are carried out for the purpose of obtaining information either from detected persons that have entered illegally the European Union via the external borders in order to produce intelligence about country of origin, reason for travelling, routes and modus operandi or involvement of facilitators in which case it is called debriefing, or from third country nationals entering the EU at border-crossing points.

In Joint Operations where the PeDRA Pilot Exercise has been launched, interviewing activities also represent an important source of personal data relating to suspects of facilitation, trafficking in human beings, and other cross-border crimes.

1.2. Debriefing

Debriefing means collecting information by Interviewing migrants detected for illegal border-crossings; the collection of information must be conducted with the consent of the migrant being interviewed on a voluntary and anonymous basis, built on trust and confidentiality between the Debriefing Experts and the migrants. No negative legal consequences arise with regard to the immigration process as a result of the migrant consenting to being debriefed. The information collected must be processed and is then turned into intelligence for further analysis and will then contribute to decisions concerning operational responses.

Debriefings carried out during Frontex coordinated Joint Operations aim at enhancing operational actions of Frontex and Member States through increased awareness and also supporting criminal investigations in Member States by collecting relevant information. In Joint Operations where the PeDRA Pilot Exercise has been launched, debriefings also support investigations performed by Europol, as Europol is a recipient agency receiving personal data generated during debriefing activities, from Frontex.

1.3. Tasks of Debriefing Experts

Debriefing experts’ tasks should be carried out according to proper processes that encompass thoroughly preparing for the interview, properly selecting interviewees as well as conducting in-depth interviewing and reporting. The tasks can be structured as: 1) preparation for debriefing; 2) identifying migrants to be interviewed and checking belongings; 3) debriefing and 4) reporting.

1.3.1. Preparation for debriefing

Prior to the debriefing, the debriefing expert should ensure that proper conditions have been met for interviewing, including the availability of adequate facilities and the necessary equipment to conduct the interview. It is also recommended that refreshments such as water and biscuits are provided during interviewing.

In the event that the conditions for debriefing are unsuitable, the members of the debriefing teams should report the deficiencies and problems to the local officer of the hosting authorities assigned to the team and to the Frontex officer responsible for managing the teams.

Apart from the required basic skills, the debriefing expert should have the necessary background knowledge on the relevant migratory situation affecting the operational area in order to conduct the interview effectively. This includes information concerning:

- The overall situation of migration affecting the area, including routes, modus operandi, main nationalities, profile of migrants, push and pull factors;
- The main countries of origin, transit and departure;
- Facilitation networks;
- Border control and standard measures to be taken by the host MS authorities.
In addition, the debriefing expert should be aware of intelligence gaps\(^1\) and should receive guidelines and background information from the Frontex Operational Analyst or Debriefing Advisor or a member of the Frontex Operational Office concerning what type of information he should concentrate on in order to better focus the interviews.

If available, updated information should be provided, preferably first hand, from the host MS authorities, guest officers or any member of the Frontex staff with regard to the number of irregular migrants detected, including a detailed description of the place, time and method of illegal border-crossing and a list of belongings found on the migrants or in the vicinity of their detection.

The debriefing expert should be informed about the medical condition of the migrant(s) and any measures which have been taken by the national authorities before the interview. In any case, the priority upon arrival is to address the basic needs of the migrants and provide medical assistance, if required. If available, the debriefing expert should have access to other relevant information relating to the migrants during the selection process.

If the interview is carried out in a reception or detention facility, information relating to the work schedule, rules of the facility, the number, the nationality and the gender of the migrants, the availability of interview facilities and migrants for interview should be arranged in advance. A contact person, preferably the head or director of the facility, and a local officer assigned to the debriefing team should be involved in the arrangements as early as possible.

If the debriefing is carried out in the form of a mobile deployment at the place of reception or arrival of migrants, the conditions of interviewing are different to those described above and have to be arranged specifically in time with the procedure applied by the local teams in which the debriefing expert is integrated. Nevertheless, the team members should have the necessary background information and be aware of standard procedures.

Prior to the start of the actual debriefing of migrants, the members of the debriefing teams are required to obtain information and prepare with reference materials which shall be used as reference points from which to pose questions and check answers, such as:

- Names and dates of arrest
- Type of vehicle used
- Place of arrest
- Nationality
- Gender
- Age

In accordance with the respective Frontex Standard Operating Procedure, debriefing experts should observe the following guidelines during interviews:

- If the debriefing expert identifies a migrant suffering from clear signs of post-traumatic stress (physiological disturbance, physical harm, constant loss of memory, etc.), or having other health issues, he/she should notify the local authorities that the traumatized migrant might require special care.
- If during debriefing, the migrant expresses in any form his/her willingness or interest to ask for asylum or international protection or has been a victim of a crime (trafficking, etc.), the debriefing expert will refer the migrant to the national authorities of the host MS for specialized procedures to be implemented after he/she completes the debriefing interview.
- If during a debriefing interview involving experts deployed to operations coordinated by Frontex, the migrant being interviewed claims a possible breach of fundamental rights, the debriefing expert should ask the migrant whether he/she wants to make an official complaint. As a result of this claim, the following scenario will ensue:
  - **YES** – the debriefing expert records the possible breach of fundamental rights in the interview report and informs the national authorities on the alleged fundamental rights violation.
  - **NO** – if the migrant does not want to report the possible breach of fundamental rights, the debriefing expert should not mention it in the interview report.

\(^1\) Intelligence gaps are areas of knowledge that are missing, making the situational picture incomplete.
In both cases the debriefing expert continues the interview unless the migrant wishes to stop it.

1.2. Identifying migrants for interview and checking belongings

Debriefing should take place

Before meeting the

During the identification of migrants for interview, the debriefing experts should be aware of intelligence gaps and the language in which the debriefing team is able to communicate effectively with the migrant.

1.3. Conducting debriefing sessions

Debriefing experts should identify themselves, the interpreter and any other person present, in front of the migrant, explaining in the language they understand the role of the debriefing expert, the procedure to be followed and the reasons for the interview.

The persons alleging a violation of their fundamental rights will be informed of the procedure for reporting such FR violations. Persons requesting protection in any form will be informed of the procedure for launching an asylum application and shall be referred by the debriefing expert to the respective national authority.

If the subject of the debriefing interview is a woman, the debriefing expert should pay special attention to gender specific concerns, and cultural differences in relation to gender, ethnic and religious groups. It is advisable, when available, that female officers interview female migrants as it is likely to raise the level of empathy and create a more relaxed atmosphere. Such interviews could provide additional information in relation to the specific impact of migration on women.

The collection of information during the debriefing of detected irregular migrants must be conducted with the consent of the migrant on a voluntary basis. The debriefing should again be built on trust and confidence between the debriefing experts and the migrants.

Commented [A2]: Debriefing interviews carried out during Frontex coordinated joint operations aim at enhancing operational actions of Frontex and Member States through increased awareness and also at supporting criminal investigations in Member States by collecting relevant information on routes, modus operandi and involvement of facilitators and traffickers of human beings. The collection of information is conducted with the consent of the migrant being interviewed on a voluntary and anonymous basis, built on trust and confidentiality between the debriefing experts and the migrants.

The disclosure of information provided in confidence will harm the confidentiality of the information provided in interviews. In general, it may indeed lead to the possible identification of individual migrants by specific criminals who have been facilitating the travel from the country of origin to the embarkation points and the sea crossing. In addition, this can create a perception that participation in debriefing interviews may put at risk the interviewee or their relatives. Ultimately, migrants will not be willing to take part in debriefing interviews resulting in poorer or less information available as a basis for Frontex operational actions.

Lastly, disclosing the interviews is equivalent to the disclosure of operational information which is the base for the future joint operations which jeopardizes the implementation of the coming operational activities at the external borders.

The aforementioned risk is reasonably foreseeable and therefore, Frontex concluded that the disclosure of the required document undermines the protection of the public interest as regards public security.

Frontex concluded that the interests protected by the right for public access to documents can not undermine the public interest as regards the public security of the citizens living within the European Union.

In light of the above, access to those documents is refused pursuant to Article 47(1)(a) of Regulation No 1099/2001, as their disclosure would undermine the protection of the public interest as regards public security.

The non-disclosed text contains detailed information regarding the modus operandi of law enforcement officials. It contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied in those activities which would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and other cross-border crimes such as facilitation of irregular migration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above, the text is not disclosed pursuant to the exception laid down in the first indent of Article 47(1)(a) of Regulation No 1099/2001 relating to the protection of the public interest as regards public security.
confidentiality between the debriefing experts and the migrant. No negative legal consequences arise with regard to the immigration process as a result of the migrant consenting to being debriefed.

The information collected must be processed and then turned into intelligence. The intelligence aims at enhancing operational activities of Frontex and MS through increased awareness and also supports criminal investigations in the MS by collecting specific information.

If during the interview migrants disclose personal data related to persons suspected of involvement in cross-border criminal activities, in facilitating illegal migration or in human trafficking activities, the debriefing team shall:

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

It may transpire during the interview that the migrant has some information that may help the investigation or that the migrant is aware of the identity of some of the individuals involved in the criminal activities.

Interviewees should be informed of the purpose of the interview and the fact that the information provided will be transmitted to the national authorities.

The primary focus of the debriefing interview should be on gathering information that will be useful in the investigation and in facilitating the exchange of information with the national authorities.

To increase the effectiveness of interviews, the following steps should be taken:

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

1.3.4. Reporting

Debriefing Experts shall draft interview reports on a daily basis and submit them to Frontex and the national authorities in line with the Operational Plan. Any delays should be notified and explained. Each interview must be documented.

Commented [A3]: Debriefing interviews carried out during Frontex coordinated Joint Operations aim at enhancing operational actions of Frontex and Member States through increased awareness and also at supporting criminal investigations in Member States by collecting relevant information on routes, modus operandi and involvement of facilitators and traffickers of human beings. The collection of information is conducted with the consent of the migrant being interviewed on a voluntary and anonymous basis, built on trust and confidentiality between the Debriﬁng Experts and the migrants.

The disclosure of information provided in conﬁdence will hamper the conﬁdentiality of the information provided in interviews in general. It may indeed lead to the possible identiﬁcation of individual migrants by speciﬁc criminals who have been facilitating the travel from the country of origin to the embarkation points and the sea crossing. In addition, this can create a perception that participation in debriefing interviews may put at risk the interviewee or their relatives. Ultimately, migrants will not be willing to take part in debriefing interviews resulting in poorer information available as a basis for Frontex operational actions.

Lastly, disclosing the interviews is equivalent to the disclosure of operational information which is the base for the future joint operations which jeopardizes the implementation of the coming operational activities at the external borders.

The aforementioned risk is reasonably foreseeable and therefore, Frontex concluded that the disclosure of the required document undermines the protection of the public interest as regards public security.

Frontex concluded that the interests protected by the right for public access to documents can not undermine the public interest as regards public security of the citizens living within the European Union.

In light of the above, to the extent that these documents are refused pursuant to Article 41(1)(a) of Regulation No 1049/2001, as their disclosure would undermine the protection of the public interest as regards public security.

The non-disclosed text contains detailed information regarding the modus operandi of law enforcement ofﬁcials. It contains references to the methods applied by law enforcement ofﬁcers to perform border control tasks in general and to combat illegal activities in particular. Its disclosure would expose the working methods applied by those activities which would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafﬁcking in human beings or terrorism. Therefore, public security will be affected.

In light of the above the text is not disclosed pursuant to the exception laid down in the first indent of Article 41(1a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.
For debriefing interviews a template should be used, however, the debriefing expert should not be restricted by merely following the template during the interview or when completing interview reports but should also provide a summary of the general findings and observations.

It is recommended that a comprehensive report be compiled at the end of the deployment period or in the case of longer periods of deployment, regular comprehensive reports should be compiled. Such reports provide a wider overview and synthesis of individual interviews, putting the collected information into context and should be sent to the host MS and Frontex. They should also include specific parts on fundamental rights related incidents.

The reporting system including the reporting of debriefing officers is

Note that in Joint Operations where the PeDRA Pilot Exercise has been launched, there is a separate template which to be used. This PeDRA template facilitates the export of personal data into Frontex analytical systems.

1.4. Use of Interpreters

Interpreters, preferably who are able to interpret into and out of English are vital to make debriefing successful, although they are not necessarily required in all locations. A large number of migrants arrive at the EU’s external borders on a daily basis and statistics suggest that only one in ten speaks a European language to any useful degree. It is inadequate to rely on migrants, who can speak English or another EU language, to provide an interpretation service for their travelling companions, or even less to establish country of origin or nationality.

Often there is no mechanism to confirm the reliability of any migrant’s claim to have a certain nationality and the nationality claimed is usually accepted at face value. Interpreters can easily identify dialects and have their own specialist knowledge of source and transit countries.

Without them it is almost impossible to carry out in-depth interviews, or establish exactly who the migrants in fact are and where they come from. It is therefore of enormous benefit if MS can supply interpreters whenever possible with the debriefing experts, for those languages most commonly encountered in the host MS (a ratio of one interpreter to one or two debriefing experts is suggested).

Whilst the debriefing expert controls the structure of the interview and asks the questions, the Interpreter should have limited freedom to clarify specific answers and to guide the debriefing expert as to any cultural or linguistic factors which may impact on the direction of the questioning. The Interpreter should be briefed prior to the interview so that the purpose and expectations can be agreed, and both parties, i.e., the debriefing expert and interpreter, can work as a team.

Commentary [A4]: The non-disclosed text contain detailed information related to reporting tools and methods used by law enforcement officials. The text contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied during border control activities which would jeopardize the implementation of future and ongoing operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above the text is not disclosed pursuant to the exception laid down in the first indent of Article 47(1)(a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.
2. GUIDELINES FOR SCREENING ACTIVITIES

2.1. Introduction

A high number of irregular migrants cross the external borders of EU without being in possession of valid travel/identification documents. Screening interviews are carried out to establish a presumed nationality. The interviews are mandatory and allow the host national authority to carry out its national registration procedures. Screening is the first step in any national process, including removal. Screening activities are performed by officers of a competent national authority of a MS as defined in the profile of a screening expert.

2.2. Screening

Screening in the field of irregular immigration means to establish an assumption on the nationality of an undocumented person having crossed, or having attempted to cross, an external border irregularly in view of registering the arrival of the person and returning the Third Country national to her/his country of origin when applicable.

Screening experts perform screening interviews at the request of the host MS authorities. The screening interviews carried out by deployed screening experts should, as a general rule, be performed in close cooperation with a screening expert from the host MS and assisted by an interpreter.

2.3. Tasks of Screening Experts

The screening expert will assist/support officers of the national authority to screen irregular migrants at reception and detention facilities in the operational area of the host MS in order to establish a presumed nationality.

When necessary and if available the screening expert will work together with interpreters provided by the national authority or deployed by a MS.

The screening experts support and cooperate with debriefing experts, by exchanging relevant information.

2.4. Preparation for screening

The screening experts should be aware of the location where he/she will perform the screening interviews. The location should have basic requirements of privacy and conditions for properly conducting interviews. Screening should take place as soon as possible after apprehension in order to obtain a more truthful account from the migrant.

The screening expert should know in advance:

- Name/identification of the screening expert
- Location of the screening interview
- Primary language of the migrant
- Type of interview

2.5. Checking belongings

The screening expert should check the belongings of the migrant in order to ensure that they are not used for the transmission of information on how to return to the MS. This is important in order to prevent the migrant from being able to communicate with other migrants or to facilitate the smuggling of illegal migrants.

Commented [AS]: The non-disclosed text contains detailed information regarding the modus operandi of law enforcement officials. It contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publication would expose the working methods applied in those activities which would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above the text is not disclosed pursuant to the exception laid down in the first indent of Article 41(1)(a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.
2.6. Conducting screening interviews

At the start of each interview the screening experts should introduce themselves and anyone else present to the migrant, explain the procedure that will be followed, the reasons for the screening interview and the role of the interpreter if present.

During the interview the screening expert...

The persons alleging a violation of their fundamental rights will be informed of the procedure for reporting such FR violations, including the possibility to file a complaint with Frontex. The asylum seekers will be informed of the procedure for launching an asylum application and shall be referred by the screening expert to the respective national authority.

If the screening expert identifies an irregular migrant during the interview as vulnerable* he/she should inform the hosting authority before the interview commences or immediately afterwards if the information came to light during the interview.

*Vulnerable persons:

"Vulnerable persons" refers to minors, unaccompanied minors, disabled people, elderly people, pregnant women, single parents with minor children, victims of human trafficking, persons with serious illnesses, persons with mental disorders and persons who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence.

Special considerations to be given to vulnerable persons are defined in the Specific Annex.

Screening interview with an interpreter:

Screening interviews can be performed without an interpreter when the communication is possible, but often the screening experts need to be supported by an interpreter.

The interpreter should be briefed prior to the interview so that the purpose and expectations can be agreed, and both parties can work as a team. Interpreters may work differently from each other and it is important that the screening expert understands the interpreter's preferred style.

The interpreter must be introduced to the migrant, and...

The screening expert should confirm that the migrant understands the interpreter and that he/she is fit and well before they proceed.

The translation should...

During interview the screening expert should...

The interpreter should not...
2.7. Working as a team with Interpreters

A qualified interpreter knows his/her role, limitations, and responsibilities. Whilst the screening expert...

An important task for the interpreter is...

A newly deployed interpreter may not understand the purpose of an identification interview or be acquainted with the general irregular migration situation in the area, or any specific local information (for example the claimed nationalities). Some initial training or background briefing could be necessary.

For security and protection reasons the interpreter should never be alone with the migrant.

2.8. Results of screening interviews

After conducting a screening interview the screening expert will presume the nationality and fill in the presumed nationality in the screening form. He/she should forward the screening form to the responsible officer of the host authority.

At the end of the working day the screening expert will circulate the screening results in line with the reporting procedure set out in the Operational Plan.
3. GUIDELINES FOR FINGERPRINTING AND REGISTRATION

3.1. General Information

In accordance to the Eurodac Regulation, irregular migrants and persons in need of international protection apprehended in connection with an irregular border crossing - except for children under the age of 14 years - must provide their fingerprints.

Conditions and location for registration, including waiting areas, must ensure and respect dignity of the persons involved in the process and take into account vulnerabilities and their prioritization. Dignity, respect and non discrimination for the persons to be registered should always be observed during the process.

Female officers should be preferably used to take fingerprints and registration data of women and children when possible, as this will avoid the risk of gender and cultural bias during the process.

The process led by the Host MS should focus in particular on systematic identification, registration and fingerprinting by the following steps:

- ensuring that fingerprints are taken on land, promptly upon apprehension in connection with irregular crossing of the borders, and in full compliance with the EURODAC Regulation;
- if there is no such possibility, due to the technical problems, at least the initial registration should be performed;
- prioritizing vulnerable categories during fingerprinting and registration, specially unaccompanied minors, families with small children, pregnant women, disabled persons or other vulnerable groups, so that waiting time is reduced to a minimum and referral to protection authorities occurs as soon as possible upon arrival;
- informing migrants in a timely manner of their rights and obligations and consequences of non-compliance with rules on identification;
- taking restrictive measures to prevent absconding in case migrants refuse fingerprinting, however, only as an exceptional measure of last resort that should not be used against vulnerable persons.

3.2. Tasks of experts

Fingerprinting and registration activities shall be carried out according to the host MS’s procedures, in close cooperation with the national experts and under the command and control of a team leader, an officer assigned by the respective law enforcement authority of the host MS.

The tasks can be structured as follows: 1) informing migrants; 2) procedures in case of refusal; 3) lawful use of force; 4) referral and 5) reporting.

3.2.1. Informing of migrants

At the start of the fingerprinting process, experts must inform each person on the obligation to give fingerprints, the purpose for collecting the fingerprints and the manner in which fingerprints will be processed, as required by Article 29 of the Eurodac Regulation. Information should be provided in writing, and where necessary, orally - in simple terms and taking in consideration the gender, age and cultural considerations - in a language the person understands or is reasonably supposed to understand. The cultural mediators / interpreters can be used in case of the language barriers occur. In order to facilitate the information process it is highly recommended that Host MS prepare relevant number of posters in the registration places.

3.2.1. Procedures in case of refusal

When persons refuse to provide their fingerprints, officer should carefully inquire about the reasons for their refusal, and additional easy-to-understand information in a language that they understand about why fingerprints are being taken should be provided, with the support of an interpreter if/when required. The persons to be fingerprinted should be given effective opportunities to voluntarily comply with fingerprinting requirements, including the possibility to stop the process of fingerprinting, provide additional information answering their questions and concerns, and allow for questions from the persons and continue the process at a later stage, allowing for the opportunity to appear for fingerprinting a second time if necessary.
Gender, age and cultural considerations should be always taken into account when further information is required in case of refusals to provide fingerprints.

3.2.2. Use of force

In case counselling and information does not succeed, and if the Host MS does not consider, where other less coercive alternatives to detention cannot be applied effectively, detaining him/her, the Host MS may consider resorting to use coercive measures as a last resort in order to enable fingerprinting of migrants.

Coercive measures against migrants can be used only by the Host MS officers. If the officer of Host MS decides to do this, the migrant will be informed that coercion may be used in order to take his/her fingerprints. If the migrant still refuses to cooperate, the officer may apply the minimum level of coercion required only if strictly necessary, lawful and proportionate to the aim pursued, with due respect to the integrity and dignity of the person concerned.

The procedure for the use of force should include a clear explanation to the migrant of the steps the officer intends to take in order to compel cooperation. The officer should demonstrate that there was no other practicable alternative measure to using reasonable coercion. A case by-case assessment should always be made of whether there is no such alternative, taking into account the specific circumstances and vulnerabilities of the person concerned.

However, people usually considered vulnerable such as children, victims of torture, sexual or gender-based violence and victims of serious crimes or traumatised people should not be coerced into giving fingerprints.

The use of coercion must always be recorded and a record of the procedure be retained for as long as necessary in order to enable the person concerned to legally challenge the actions of the authority.

3.2.3. Referral - Damage of the fingertips

In cases where an applicant has damaged his/her fingertips or otherwise made it impossible to take the fingerprints (such as via the use of glue), and where there is a reasonable prospect that within a short period of time it will be possible to take such fingerprints, experts must refer it to the national authorities so that his/her fingerprints can be taken at a later stage.

3.2.4. Reporting

At the end of the working day the fingerprinting expert have to report to the team leader the results of his activities, number of migrants fingerprinted, refused or not possible, in line with the reporting procedure set out in the Operational Plan. Any use of force must be reported accordingly in the daily report.

3.3. Use of cultural mediators / Interpreters

The use of cultural mediators / Interpreters within the informative sessions regarding the obligations to give fingerprints, the purpose of collecting the fingerprinting and the manner in which fingerprints will be processed is of the utmost importance.

Moreover, possible support of the cultural mediators / Interpreters in the counselling of those migrants refusing fingerprinting is recommended. In those cases where the refusals still remains, the cultural mediators/ Interpreters may also be involved for the explanation of the procedures for the use of force with a clear explanation to the migrant of the steps the officer intends to take in order to compel cooperation.

3.4. Vulnerable groups

Special consideration should be given to the vulnerable persons. “Vulnerable persons” refers to minors, unaccompanied minors, disabled people, elderly people, pregnant woman, single parents with minor children, victims of human trafficking, persons with serious illnesses, persons with mental disorders and persons who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence.
When the officers doubt that the age declared by the undocumented person to be registered (either when declaring that she/he is a minor or an adult), the principle of presumption of minority should prevail and the situation should be immediately notified to the national authorities so that procedure for age determination can be started.

Coercive measures should not apply on vulnerable persons for the purpose of fingerprinting and other alternatives to seek cooperation for fingerprinting purposes should be sought, such as support from social services or organisations specialised in dealing with vulnerable categories, including persons of their own national background if necessary.
4. “HOT SPOTS” AND EU REGIONAL TASK FORCE

4.1. General information

The aim of the “Hotspot” is to provide a platform for EU Agencies to intervene rapidly, in an integrated manner and according to their mandate, in frontline MS when a crisis arises due to a specific and disproportionate migratory pressure at their external borders consisting of mixed migratory flows, and the MS concerned cannot adequately cope with that pressure. The support offered and the duration of such assistance to the MS concerned would depend on its needs and the development of the situation.

The European Union Regional Task Force (EURTFF) represents the platform model implementing the “Hotspot”. As it has been defined by the EU Agencies, it provides for the overall operational coordination of the work of different teams of experts from the EU Agencies involved, it facilitates and manages the information exchange among these teams, and it supports the coordination of its operational efforts with the relevant national authorities.

The implementation of the “hotspots” concept in the scope of Frontex mandate is integrated within the framework of the respective Frontex coordinated joint operation. Frontex will support the host MS in implementation of the following activities, in particular:

- Assistance in identification including nationality screening,
- Referral of people in need of international protection,
- Assistance in registration including fingerprinting, which precedes the asylum applications.

In addition, Frontex will support the host MS in organizing of adequate return assistance with regard to persons upon whose the competent national authorities have issued a return decision.

4.2. Roles of EU Agencies

Frontex, European Asylum Support Office (EASO), Europol and Eurojust provide operational assistance to the MS in accordance with their respective mandate in the field of managing the external borders, dealing with applications for international protection, and combating serious organized crime such as facilitation of irregular migration.

Frontex supports MS in the identification procedures through screening, debriefing, fingerprinting collection and document expertise. Moreover, Frontex provides tailored products and services within the context of Europol.

The concept of the “Hotspot” foresees that the EASO, Frontex and Europol will work on the established hotspots in the operational area to process incoming migrants by coordinating activities and complementing each other. Frontex will assist MS in identification including nationality screening, registration and fingerprinting, which precedes the asylum applications. Those claiming asylum will be immediately channeled into an asylum procedure where EASO support teams will help to process asylum cases as quickly as possible. For those not fleeing a claim for international protection, Frontex will help MS by coordinating the return of irregular migrants. Europol and Eurojust will assist the host MS with investigations to dismantle the smuggling and trafficking networks.

The EURTFF, in close coordination and cooperation with the competent national authorities, will facilitate the overall coordination of the teams of experts from the different Agencies deployed on the hotspots, and ensure information exchange. Depending on whether the major challenge is pressure at the external borders, or processing asylum applications or investigating criminal networks, the relevant Agency takes up the role of coordinator in the EURTFF in cooperation with the competent authority of the host MS. Frontex will take care of the administrative and logistical arrangements in cooperation with the competent authority of the host MS. The EURTFF shall carry out its tasks without prejudice of the competences and responsibilities of the relevant national authorities, and in close collaboration with them.

The operational support to be provided using the “Hotspot” includes:

- Registration and screening of irregular migrants to determine their identity and assumed nationality, and provision of information concerning the asylum process. In case of need, fingerprinting and registration in EUROPOL will be carried out by host MS authorities, and if requested with the support of the TMs. At this stage, each individual undergoes a first screening interview. Following the screening it should be possible to distinguish between the following categories of persons:
- Persons who wish to apply for asylum (actors: national competent authorities with the support of EASO);
- Persons who can be subject to a return procedure in accordance with the EU law (actors: national competent authority with the support of Frontex);
- Persons with regard to whom the situation may remain doubtful: normal procedure applies (actor: national competent authorities).

- Debriefing of migrants supported by Frontex at the hotspot to understand routes, modus operandi and to gather information, including on secondary movements, with a view to contributing towards investigations into smuggling networks and for criminal analysis. Europol is provided with relevant information and intelligence from all debriefing interviews to support and initiate investigation with the concerned MS.

- Stepping up investigations (including forensic/operational support), information and intelligence exchange on facilitation of irregular transit and stay within the EU. This enhanced cooperation should deal with criminal networks facilitating migration to the EU as well as secondary movements from the MS of disembarkation to the final destination (Actors: host MS, in particular national prosecutors and judicial authorities, Europol, Eurojust, if needed).

- Asylum support, in line with the joint processing concept, by channeling asylum seekers into the appropriate asylum procedure (according to the host MS national legal system) and assisting with registration of asylum seekers and subsequent preparation of case files.

- Coordination of the return of migrants that do not have the right to stay in the EU legally, in particular with regard to pre-return assistance and the coordination of return flights. Support for the acquisition of travel documents from countries of origin, including by setting up teams from identified countries of return to carry out interviews and speed-up the issuance of travel documents (Actors: host MS and other MS, which can assist in the contacts with the relevant countries of origin or transit with the support of Frontex).

- Interpretation to facilitate the work of the experts provided by the Agencies for the above tasks will be provided by the Agencies and/or MS.
5. **FRONTEX ONE-STOP-SHOP (FOSS)**

5.1. **FOSS general Information**

The Frontex One-Stop-Shop (FOSS) is a web-based and secure portal providing situational awareness and sharing operational-related information. FOSS serves as a documents repository for this information, where close-to-real-time and up-to-date information is available to multiple users, simultaneously. The information shared in FOSS is organized and clustered in specific areas, according to the relevant topic, and is related to the core business of Frontex: co-operation and operational coordination between MS in the field of border security. Being accessible 24/7 and easy to navigate, FOSS is an effective tool for improving awareness and facilitating the co-operation between Frontex and its partners. During the joint operation, FOSS will be the main platform used for sharing operational-related information between all parties involved. This information will be accessible according to defined standards and amongst users designated respectively for each joint operation.

Access to the FOSS portal is enabled to internal (Frontex staff) and external members of the Frontex-related community. The latter includes representatives from MS, Schengen Associated-Countries and Third Countries, International Organizations and EU institutions cooperating with Frontex. Other experts and entities cooperating with Frontex and with a business need to access information stored on FOSS may also be granted access to the portal, provided that approval through the relevant authorization channels is granted.

5.2. **FOSS access procedures**

FOSS users are divided into "User Groups", with each group being granted a specific access level enabling its members to view or upload information, depending on their specific operational need. For each specific operation/other activity, user groups are divided between those with permanent access (generally Frontex staff, National Frontex Contact Points, National Authorities, etc.) and those with temporary access to the operation/other activity documentation (TM, Observers, etc.).

5.2.1. **FOSS access authorization**

Access to FOSS is granted if the requestor meets the following conditions: has an operational need, provides the required details and is authorized by the relevant authority.

Access is provided to individuals only. A FOSS account is personal and should not be shared.

Relevant Authorities:
- 1st level authorization: NFPOC (National FOSS User Coordinator)
- 2nd level authorization: "Area of Interest Owner" (Operational Manager).

These authorities agree on, and decide, the access levels to be granted to TM and other experts.

5.2.1.1. **Access authorization procedure for TM via OPERA:**

When OPERA is used the process of requesting and authorizing access to FOSS is fully performed through this system, by completing the section "Additional information", under the "Personal registration" form in the "Resources Deployment Tool" page.

- The NFPOC decides if it is necessary to request access to FOSS for a relevant TM.
- By checking the box "Access to FOSS"**" (in the "Additional Information"), the NFPOC authorizes access to FOSS for the relevant TM.

---

* The Operational resources management system (OPERA: https://fs.frontex.europa.eu/oper/) is an integrated system for the management of the operational resources pooled and deployed in Frontex coordinated activities.

* Leaving this box unchecked is a decision of disapproving the access.
The NFPOC completes all the information regarding the period and type of access. In particular the NFPOC will need to specify:

- **Date from** and **Date to** (start and end date) of FOSS access

<table>
<thead>
<tr>
<th>Travel Details</th>
<th>Personal Equipment</th>
<th>Weapons</th>
<th>Technical Equipment</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to FOSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date From</td>
<td>Date To</td>
<td>Type of Access</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Type of Access**, by selecting one the following options:

- Standard overview of JO documents
- Full overview of JO documents
- Full sector overview

---

5.2.1.2. Access authorization procedure for TM (seconded):

- For TM (seconded) the same FOSS access procedures as for Frontex staff apply. Unless otherwise requested by the Operational Manager, the TM (seconded) is granted FOSS access to the relevant content on FOSS for the duration of the secondment through his/her Frontex email.

- Following the end of the secondment at Frontex the FOSS account will be deactivated, unless access was granted with a previously existing FOSS account.

5.2.1.3. Access authorization procedure for the other participants (not inserted in OPERA):

- In the "FOSS User Access Request Form" the NFPOC approves the access request for their personnel deployed to the operation or other parties, by ticking one of the relevant boxes displayed in the form and identifying the joint operation to be accessed.

- The NFPOC sends the duly completed "FOSS User Access Request Form" to Frontex.

- The Operational Manager approves the request and sends the relevant data to the FSC User Administrator, in order to grant access.

---

1 Start and end date can be freely decided, but we recommend requesting FOSS access before the start of the deployment for the TM (for example 30 days in advance). It is also recommended to allow access to operational documents available in FOSS also 30 days after the end of the deployment of the TM.
5.3. Roles & Responsibilities

5.3.1. National FOSS User Coordinator
This function is assigned to the relevant MS’s MFPOC. His/her responsibilities include gathering user data, validating access and providing user data to the "Area of Interest Owner" (Operational Manager).

5.3.2. Area of Interest Owner
This function is assigned to the Operational Manager in charge of the Joint Operation. His/her responsibilities include establishing the structural design and layout of the Joint Operation's specific area (FOSS Area of Interest), uploading content in the Joint Operation's specific area, authorizing user groups and permissions levels, providing all necessary information to the User Administrator.

5.3.3. User Administrator’s (FSC) - FOSS Service Manager
This function is assigned to FSC. His responsibilities include creating, updating, removing and deactivating user accounts, assigning users to a respective group, assigning groups to the Joint Operation's specific area.

5.4. Navigation in FOSS

After logging into FOSS, by scrolling on the section 'Operational Activities' authorized users will be able to access the relevant Joint Operation page, directly from the FOSS homepage. As an example, in the images below the user has been granted access rights to JO Focal Points Sea 2014:

The user can also access the Joint Operation page after having entered the 'Operational Activities' section, either from the left hand side menu, or from the central pane.

Commented [AB]: The non-disclosed text contains detailed information on the means of communication used by law enforcement officials within the joint operation. Their disclosure could lead to possible abusive usage with a view to jeopardize their work and harm the course of future and ongoing operations and thus facilitating irregular migration and affecting public security. In light of the above, the text is not disclosed pursuant to the exception in the first indent of article 4(1)(a) of Regulation (EC) No 1049/2001 relating to the protection of the public interest as regards public security.
6. COMMUNICATION WITH THE PRESS

6.1. Introduction

All Frontex activities are financed from public funds (EU budget) therefore it is Frontex’s obligation to maintain a high level of transparency and openness in its activities. Operations held at the external borders experiencing a high level of migratory pressure often draw a large numbers of international journalists.

It is Frontex policy to facilitate media coverage of all its activities, including operations. Consequently the press office facilitates media visits to the operational areas, including participation of media representatives in patrols and organises media interviews with officers deployed by Frontex.

All press visits are closely coordinated with host MS authorities and are carried out according to procedures defined in the Press Communication Rules in the sub-chapter below.

Press rules may vary depending on the operation; therefore the differences will be reflected in the main part of the Operational Plan.

In some operations Field Press Coordinators seconded from MS will be deployed to host MS to coordinate press requests in the field.

Openness cannot hinder or jeopardise operational activities, therefore several general rules apply.

No information should be released to the media prior to the beginning of the operation.

Operational details, such as operational area, details of technical equipment deployed, shift schedule, etc. are considered sensitive information and are not to be shared with the media.

All participants in the joint operation are obliged to contact the Frontex press office before giving an interview.

6.2. Press communication rules

6.2.1. General

The communication strategy regarding the Frontex mission and activities in general is under the auspices of the Agency.

In order not to jeopardise the outcome of the operation, no information about the operation should be released to the public prior to its beginning. National authorities deploying border guards to the joint operation should also limit their public statements to the general objectives of the operation, numbers and profiles of experts.

Press Offices of Frontex and the host country press office are entirely responsible for coordination of all matters related to interview requests, press visits to the operational area and any other press-related matters related to the joint operation.

Press lines regarding joint border control operational issues and actions as well as specific incidents that might occur, are agreed by Frontex and the host country press office.

6.2.2. Tasks of press offices in the context of Joint Operations

Press visits to the joint operation will be organised by the host MS authorities in cooperation with the Frontex Press Office.

Tasks of the Frontex press office will include:

- Informing the media on Frontex’ mission and activities, as well as on the activities of the Joint Operation. Providing background information and statistical data on migratory movements.
- Being the point of contact for international media requests.
- Media monitoring and analysis of media tendencies (neutral, positive, negative).
• Drafting and distributing press releases, statements and other communications in close cooperation with the competent host country authorities.

**Tasks of the Host Country press office**

• Arranging interviews with representatives of the host MS authorities.
• Being the point of contact for national media.
• Arranging filming opportunities in the operational area.
• Drafting and distributing press releases, statements and other communications related to Frontex activities in close cooperation with Frontex.
• Informing Frontex Press Office about questions from national media regarding the Agency and its activities.

6.2.3. Management of Press Requests

Given that journalists need to obtain authorisation from the host MS authorities to visit the operational area, the following procedures must be followed:

• Individual and on-the-spot media requests must be directed to the Frontex Press Office and press office in the host MS electronically.
• The Frontex Press Office and the press office from the host MS will inform each other about media requests on a regular basis.
• The Frontex Press Office will coordinate the flow of international press requests received, collect information about their needs and direct requests to the press office in the host MS.
• The press office of the host MS will process the necessary authorisations, coordinate the flow of national press requests received and inform Frontex Press Office about the planned presence of the media in the operational area and provide them with necessary assistance on the ground.
• The press office of the host MS will process the necessary authorisations for participation of journalists in patrols and visits to restricted operational areas. The Dedicated Press Officer will inform the interested parties and the Frontex Press Office about the decision.
• The press office of the host MS will host media representatives. Media representatives will be asked to present their press credentials before participating in any activity and to sign a written statement that the host MS or other involved countries’ authorities will not bear any responsibility should anything happen to the media representatives and/or their equipment.
• The press office of the MS which deploys the TM needs to be informed and approve the press request.

6.2.4. Specific guidelines for participating officers if approached by the media:

Participants are allowed to talk to the media only within the limits set by specific guidelines indicated below.

All participants need to contact the Frontex Press Office before agreeing to an interview.

The Press Office will brief the TM prior to the interview about the media, subject of the interview and sensitive topics.

**What you can say:**

• This is a Joint Operation coordinated by the European Border and Coast Guard Agency (Frontex);
• XX EU MS and Third Countries take part in the Joint Operation;
• These countries participate by providing experts in border checks and/or border surveillance and/or second-line activities;
• I am a border guard (or in other cases, adapt the remaining text) from (name of your country) deployed to this operation. I am assisting the host MS's officers in border control activities. I am an expert in (e.g., first-line control, interviews etc.);
• I am not authorised to give the media any more details - please contact the Frontex Press Office.

**What you should NOT say:**
• Do not give details of the operation;
• Do not talk about the exact area covered by the operation;
• Do not give details of the technical means deployed;
• Do not talk about the working schedule;
• Do not discuss the migratory situation in the host MS or the bordering third country;
• Do not talk about individual incidents that may have taken place during the operation;
• Do not try to answer detailed questions about what Frontex is.

Please refer journalists to Frontex spokespersons for further details or call the Frontex Press Office in case of doubt (you can also send an SMS and we will call you back).

6.2.5. Contact details

The contact details of the Frontex Press Office members (Spokesperson and Press Officer) and the press office of the National Authority of the Host MS are indicated in the respective Annex of the Operational Plan "Contact Details".
7. **JOINT OPERATIONS REPORTING APPLICATION (JORA)**

7.1. JORA General Information

7.1.1. JORA product & service management

The FSC JORA Product and Service Management is responsible for the JORA Service Operations, in accordance with the JORA policy and processes. The Product and Service Managers are listed in the JORA Actors Specific Annex.

The Product and Service Managers primary role is to ensure that the system runs properly, in line with the end-users needs and, if necessary, to manage the further developments or readjustments of the system.

The Product and Service Managers also support the correct use of JORA, review quality, efficiency and user-satisfaction of the system in accordance with the needs.

The JORA Product and Service Management is responsible for the following tasks:

- To coordinate and carry out the activities required in order to ensure the daily operational management of the system;
- To communicate with external customers and Frontex entities;
- To manage and maintain the Service-Level Agreement with Frontex ICT;
- To manage the content and the structural design of the application;
- To manage the Requests for Change;
- To identify and assess the training needs, and to plan, coordinate, organize and deliver the relevant training activities, where possible;
- To report risks, statistics and issues to the Business Owners;
- To initiate and coordinate the execution of new developments;
- To provide their expertise to new activities related to the product development;
- To initiate quality checks.

In order to maintain the required operational support, the JORA Product and Service Management provides daily expertise, consultancy and assistance to its stakeholders and customers.

Suggestions and feedback are part of the adopted Continual Service Improvement orientation. Thus, the JORA Product and Service Management welcomes any feedback received from the end users: suggestions, recommendations and Requests for Change are assessed and analysed by the JORA Change Advisory Board. The standard Feedback Form is available on FDIS.

7.1.2. JORA Roles and Responsibilities

All assigned JORA actors are listed in the respective Specific Annex of the Operational Plan.

7.1.2.1. JORA Administrator

- Staff member nominated by the Head of the Frontex Situation Centre;
- Authorized to manage all the roles and processes in JORA;
- May define, modify and delete operations in JORA;
- Acts as the Incident Template Approver, thus validating and publishing an incident template in JORA.

7.1.2.2. JORA Frontex Access Manager

- Operations Manager of the joint operation;
- Creates the operation and its structure in the JORA system according to the Operational Plan;
- Selects and assigns the Incident template creator in the JORA system, and approves the relevant incident template;
7.1.2.3. Delegated JORA Frontex Access Manager

The same set of roles and responsibilities applies to the assigned to the Delegated Frontex Access Manager.

7.1.2.4. FSC Support Officers

The FSC delivers the necessary training for JORA, in accordance with the role and the responsibility of the Support Officers.

FSC ensures that all the support officers having appropriate user rights in the JORA system to perform their tasks during their deployment.

7.1.2.5. JORA National Access Manager

National Access Managers are nominated by their MS / National Authorities.

Responsibilities:

- To approve or reject the Initial Access Requests from member of national entities participating in Frontex operations and to define the operational access rights;
- To manage the users’ accounts for the operation.

7.1.2.6. JORA Incident Reporter

Host MS officer(s) or deployed officer(s) are responsible for the Incident reporting depending on the organization of the daily operational activities. In case deployed officers are involved into the incident reporting working flow it is strongly advised that the host country authorities appoint a local officer for the coordination of the incident reporting in the JORA system (such as incident verifier).

The incident reporters’ main responsibilities are to create, modify, and forward incident reports to the next validation level, in accordance with the Operational Plan.

7.1.2.7. JORA Local Incident Verifier

An officer of a Local Coordination Centre is responsible for the validation of incidents at a local level. Local incident verifiers’ main responsibilities are to verify, modify and forward incidents to the next validation level, in accordance with the Operational Plan.

7.1.2.8. JORA International Incident Verifier

An officer of International Coordination Centre or other authorities responsible for the validation of incident reports. The ICC incident verifiers’ main responsibilities are to verify, modify and forward incident reports to the FSC, in accordance with the structure of the operation.
7.2. JORA Access Request Procedure

7.2.1. Background

The implementation of JORA started in December 2011 with the aim to deliver Frontex and its internal and external stakeholders (MS, specific EU bodies, etc) the capability to send, manage and analyse data related to the incidents occurring during the entire cycle of joint operations coordinated by Frontex.

The operational implementation of JORA has, so far, allowed users to:

- Improve their real-time situation and crisis monitoring;
- Enhance the possibility to gather and analyse the reported data.

Users' access to JORA is an important matter as Frontex strives to protect the confidentiality, the integrity and the availability of all of the joint operations' data by taking all the necessary steps to manage access to the application. On this regard, the JORA Policy v. 3.0 lists some of the access-request key statements that have to be adhered to:

- The purpose of Access Management is to ensure that the right people receive the right information at the right time to the right level of detail;
- All users of the JORA system shall apply the Access Management policies rigorously;
- Access to the JORA (or its parts) shall not be granted until the responsible National and/or Frontex authority properly clears the JORA Access Requester;
- A JORA Access Requester shall not attempt to access JORA if he/she is not cleared by responsible authority;
- Access to JORA Operational Data is logged, tracked, stored and archived;
- Access to JORA is granted based on "need-to-know" principles;
- Only trained and qualified personnel can gain access to JORA operational data;
- Each Operational Plan shall list the JORA Frontex Access Managers and the JORA National Access Managers.

In order

7.2.2. Initial Access Request to the JORA System

Commented [A9]: The non-disclosed text contains detailed information related to reporting tools and methods used by law enforcement officials. The text contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied during border control activities which would jeopardize the implementation of future and ongoing operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings, terrorism. Therefore, public security will be affected. In light of the above, the text is not disclosed pursuant to the exception laid down in the first indent of Article 4(1)(a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.
7.2.2.1. Access Request Information

7.2.2.2. System User

7.2.2.3. Login Requirements
7.2.2.4. Password Requirements

Commented [A11]: The non-disclosed text contain detailed information related to reporting tools and methods used by law enforcement officials. The text contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied during border control activities which would jeopardize the implementation of future and ongoing operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above the text is not disclosed pursuant to the exception laid down in the first indent of Article 4.1(b) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.

7.2.2.5. User Details

The user’s details should be filled out accordingly.

7.2.3. Access Request to specific operation

After the initial access request procedure is completed
Commented [A12]: The non-disclosed text contains detailed information related to reporting tools and methods used by law enforcement officials. The text contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied during border control activities which would jeopardize the implementation of future and ongoing operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above, the text is not disclosed pursuant to the exception laid down in the first indent of Article 4(1)(a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.

7.2.4. Access Request Process
7.3. Contact Details

In case of assistance, users may contact the Incident Reporting Service Management or the Frontex ICT Helpdesk via e-mail or telephone as shown below:

**JORA Service Management (JORA Administrator):**

- **E-mail:** [redacted]
- **Landline:** [redacted]
- **Frontex ICT Helpdesk:** [redacted]
- **Email:** [redacted]

*Commented [A13]: The non-disclosed text contains detailed information on the means of communication used by law enforcement officials within the joint operation. Their disclosure could lead to possible abusive usage with a view to jeopardize their work and harm the course of future and ongoing operations and thus facilitating irregular migration and affecting public security. In light of the above, the text is not disclosed pursuant to the exception in the first indent of Article 4(1)(d) of Regulation (EC) No 1049/2001 relating to the protection of the public interest as regards public security.*
### JORA Incident Template Attributes' List

**General Information**

<table>
<thead>
<tr>
<th>No</th>
<th>Name of attribute</th>
<th>Mandatory*</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Incident number</td>
<td>automatic</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Reporting unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Operational area</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Primary incident type</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Date of reporting</td>
<td>automatic</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Detections initiated by</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Detection date</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Type of detected by</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Subtype of detected by</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Latitude detection</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Longitude detection</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Detection by Frontex financed/deployed asset</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Interception date</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Interception place</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Type of Intercepted by</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Subtype of Interception by</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Latitude interception</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Longitude interception</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Interception by Frontex financed/deployed asset</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Frontex financed/deployed asset involved</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Search and Rescue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Reference to Op area</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

*Please mark the respective cells under "Mandatory" if you deem that the relevant field should be mandatorily filled by the Incident Reporter. By doing so, the Incident Reporter will be compelled to enter the mandatory data to submit the incident Report to the next validation level.
<table>
<thead>
<tr>
<th></th>
<th>Estimated POB</th>
<th></th>
<th>24</th>
<th>Eurosur border section</th>
<th>yes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Incident impact level</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Persons Information**

<table>
<thead>
<tr>
<th></th>
<th>Country of departure</th>
<th>yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Place of departure</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Date of departure</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Disembarkation</td>
<td>yes</td>
</tr>
<tr>
<td>30</td>
<td>Migrants prevented from departure</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>Victims of trafficking</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Death cases</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Personal Information tab</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Documents alerts Information tab</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Attachments tab</td>
<td></td>
</tr>
</tbody>
</table>

**Personal Information TAB**

<table>
<thead>
<tr>
<th></th>
<th>Number of people</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>Age</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>Is adult</td>
<td>yes</td>
</tr>
<tr>
<td>38</td>
<td>Accompanied yes/no</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>Nationality Claimed</td>
<td>yes</td>
</tr>
<tr>
<td>40</td>
<td>Nationality presumed</td>
<td>yes</td>
</tr>
<tr>
<td>41</td>
<td>Nationality confirmed</td>
<td>yes</td>
</tr>
<tr>
<td>42</td>
<td>Gender</td>
<td>yes</td>
</tr>
<tr>
<td>43</td>
<td>Primary role of person</td>
<td>Yes</td>
</tr>
<tr>
<td>44</td>
<td>Reason for refusal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Documents Alert Information TAB</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>Type of document</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Document status</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Forgery type</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>Issuing country</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>Where issued</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>Exhibited/concealed</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>Found at</td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>Gender</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>Nationality of holder</td>
<td></td>
</tr>
</tbody>
</table>

### Additional Information

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>55</td>
<td>Number of transport means</td>
</tr>
<tr>
<td>56</td>
<td>Transport type</td>
</tr>
<tr>
<td>57</td>
<td>Yes</td>
</tr>
<tr>
<td>58</td>
<td>Boat destroyed by</td>
</tr>
<tr>
<td>59</td>
<td>Comments</td>
</tr>
<tr>
<td>60</td>
<td>Yes</td>
</tr>
<tr>
<td>61</td>
<td>Primary smuggling</td>
</tr>
<tr>
<td>62</td>
<td>Quantity of smuggled goods 1</td>
</tr>
<tr>
<td>63</td>
<td>Secondary smuggling</td>
</tr>
<tr>
<td>64</td>
<td>Quantity of smuggled goods 2</td>
</tr>
<tr>
<td>65</td>
<td>Additional vessel information tab</td>
</tr>
<tr>
<td>66</td>
<td>Flags or signs</td>
</tr>
<tr>
<td>67</td>
<td>Total engine power (hp)</td>
</tr>
<tr>
<td>68</td>
<td>Vessel length</td>
</tr>
</tbody>
</table>
8. SERIOUS INCIDENT REPORTING

8.1. Introductory Information

The purpose is to define the steps and actions to be taken in the frame of the reporting of serious incidents, in accordance with the “Frontex Serious Incident Catalogue”. Given the seriousness of the incident reported, as well as the urgency in taking immediate action within Frontex, it is crucial that all actors involved in Frontex activities are acquainted with the procedural steps and understand the importance of “Serious Incident Reports” (SIR) due to the impact these “Serious incidents” (SI) could have on Frontex work, responsibilities and reputation.

8.2. Definition

8.2.1. Serious Incident (SI)

A SI is an event or occurrence, natural or caused by human action, which may affect, or be relevant to a particular Frontex activity, the safety and security of participants in Frontex activities, the Agency’s mission and reputation, or any combination thereof. A SI also includes situations of alleged violations of Fundamental Rights and of EU acquis or international law, particularly related to international protection obligations and of the Frontex Code of Conduct for all persons participating in Frontex activities and for Joint Return Operations coordinated by Frontex.

8.2.2. Serious Incident Report (SIR)

A SIR is a product aimed at informing Frontex Senior Management, MS, the Management Board and other relevant stakeholders, as soon as possible, about the occurrence of a SI as defined in the “Frontex Serious Incident Catalogue” (Chapter 8.10). The production and timely dissemination of a SIR contribute to improve situational awareness and increase Frontex reaction capabilities related to incidents occurred in the frame of Frontex activities. The issuance of a SIR is the first internal step for possible follow-up measures and eventual official statements to be taken by Frontex Senior Management, if needed.

8.3. Roles and responsibilities

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

Commented [A14]: The non-disclosed text contains detailed information related to reporting tools and methods used by law enforcement officials. The text contains references to the methods applied by law enforcement officials to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied during border control activities which would jeopardize the implementation of future and ongoing operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above, the text is not disclosed pursuant to the exception laid down in the first indent of Article 41(3) of Directive No 1049/2001 relating to the protection of the public interest as regards public security.

---

* All persons participating in activities coordinated or led by Frontex

* Frontex activity means any activity coordinated or led by Frontex.
8.4. Content of a SIR

- [Redacted text]

8.5. SIR procedure - Chronology of reporting serious incidents

Every actor involved in Frontex activities

Please note:

8.5.1. Initial SIR

- [Redacted text]
8.5.2. Formal SIR

The FSC

In case more information

8.5.3. Updated SIR

At a later stage.

FSC

8.5.4. Final SIR

8.6. Reporting of SI with alleged violation of fundamental rights (FR)

8.6.1. Reporting mechanism

Commentary (A16): The non-disclosed text contains detailed information related to reporting tools and methods used by law enforcement officials. The text contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities. In particular, its publicity would expose the working methods applied during border control activities which would jeopardize the implementation of future and ongoing operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above, the text is not disclosed pursuant to the exception laid down in the first indent of Article 41(3)(a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.
8.7. **Frontex Internal follow up procedure / SIR-Coordinator**

Due to the possible ________

---

8.8. **Personal Data**

The processing of personal data shall be limited to the conditions defined by the provisions of Frontex Regulation, in particular Articles 11a, b and c and with the provisions of the Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1). 

During 2016, the PedRA Pilot Project will be launched in same Sea Border Operations. The only major changes to operational activities are that debriefers should use a new specifically designed and improved template to report the debriefing activity including any collected personal data, and IOs should upload these debriefing templates to JORA rather than sending them in daily packages. The internal policies of Frontex with regards to processing personal data collected during Joint Operations can be found in Management Board Decision 58/2015.

8.9. **Public access**


8.10. **Serious Incident Catalogue**

8.10.1. **Serious Incident Categories**

Please note: The categories and examples in this catalogue should facilitate the identification of Si but do not represent an exhaustive list:

**Category 1 - Situations of high political and/or operational relevance especially with the potential to affect EU border management of one or more MS** including international crisis situations, such as:

- Terrorist attack in a MS, EU neighboring or other third countries
- Natural disaster in a MS, EU neighboring or other third countries
- Other disasters/man-made disaster (chemical, nuclear) in MS, EU neighboring or other third countries
- Unexpected major changes in border management, e.g. introduction of visa obligations, temporary closure of BCPs
- Major incidents related to MS border security (not in relation to activities coordinated by Frontex), e.g. massive arrivals of irregular migrants, traffic accidents at BCP, blockade of BCP
- Border conflict between MS and third countries

---

3/10

---

* Leading to a change on the level of border control, (e.g. introduction of specific border control measures, temporary introduction of border control between Schengen countries, stop for air traffic)
• Civil war/riots and civil commotion in MS, EU neighboring or other third countries
• Armed conflict between EU neighboring and/or other third countries or MS.

Category 2 - Incidents occurring in Frontex activities/joint operations and not related to Frontex staff, or other participants in Frontex activities, such as:

• Incidents in Frontex activities with a high public or political interest (death of persons, high number of arrivals in unexpected regions, unexpected massive arrivals of irregular migrants, capsized or sunk boat)
• Incidents or accidents at the external border with potential effect to the joint operation implementation
• Use of force, and in particular the use of firearms in joint operations
• Incidents with involvement of third countries
• Serious accidents with the involvement of deployed means (e.g. plane crash)
• Dissension between participating MS (Host and Participating) in activities coordinated by Frontex, significant (unexpected) changes in implementation compared with the operational plan
• Unforeseen other incidents with potential effect to the implementation of activities coordinated by Frontex
• Incidents in Frontex activities which could cause public and/or media interest

Category 3 - Incidents involving Frontex staff and participants in Frontex activities, such as:

• Death of Frontex staff/participants
• Severe injury of participants or damage, loss, stealing their and/or Frontex valuable goods/property
• Serious accident involving participants whether on or off duty
• Arrest and/or detention of participants
• Serious illness or contagious diseases effecting Frontex participants
• Impossibility to use Frontex premises or parts of Frontex premises
• Suspected violation of the Frontex Code of Conduct, except for issues related to fundamental rights and the obligations on international protection
• Violation of the Code of Conduct for Frontex Joint Return Operations

Category 4 - Situations of suspected violations of Fundamental Rights or International protection obligations such as:

• Suspected or alleged violations of fundamental rights enshrined in the Charter of Fundamental Rights of the European Union or other relevant International law
• Observed or witnessed potential violations of fundamental rights, in particular against human dignity or other fundamental rights including but not limited to:
  o Right to life
  o Right to the integrity of the person
  o Prohibition of torture and inhuman or degrading treatment or punishment
  o Right to liberty and security
  o Right to asylum
  o Principle of non-refoulement and protection in the event of removal, expulsion or extradition
  o Non-discrimination
- Right to an effective remedy
- Protection of vulnerable persons, such as minors, unaccompanied minors, disabled people, elderly people, pregnant women, single parents with minor children, victims of human trafficking, persons with serious illnesses, persons with mental disorders and persons who have been subjected to torture, rape or other serious forms of psychological, physical or sexual violence.
- Other international protection obligations
- Imminent danger
Commented [A17]: The non-disclosed text contains detailed information related to reporting tools and methods used by law enforcement officials. The text contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied during border control activities which would jeopardize the implementation of future and ongoing operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above the text is not disclosed pursuant to the exception laid down in the first indent of Article 4(1)(a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.
8.12. List of potential fundamental rights violations within Frontex activities

- Asylum
  - Non-access to the asylum procedure:
    - Non-identification
    - Non-registration
    - Non-information and counselling
    - Removal

- Children
  - Best interests of the child
  - Living conditions
  - Unaccompanied minors/Separated children:
    - Legal guardianship and representation
    - Respect for the views of the child, right to participation
    - Family reunification
    - Safeguards regarding age assessment

- Collective expulsion
- Dignity (human dignity)
- Discrimination:
  - Sex
  - Race
  - Colour
  - Ethnic or social origin
  - Genetic features
  - Language
  - Religion or belief
  - Political or any other opinion
  - National origin
  - National minority
  - Property
  - Birth
  - Disability
  - Age
  - Sexual orientation
  - Other grounds

- Effective remedy before a tribunal:
  - Expulsion
  - Extradition

- Family life:
  - Family reunification
- Health care

- Integrity of the person:
  - Physical integrity
  - Mental integrity

- Liberty and security:
  - Deprivation of liberty (arbitrary or unlawful)
  - Guarantees for persons (lawfully) deprived of liberty:
    - Information on the reasons for arrest:
      - Prompt information
      - Information in language understood
      - Information on reasons for arrest
      - Information on charge
    - Examination by a Court (lawfulness of detention):
      - Review of lawfulness of detention
      - Take proceedings
      - Review by a court
      - Speediness of review
      - Procedural guarantees of review
      - Order release

- Property:
  - Deprivation of property

- Reproduction:
  - Risk of torture
  - Risk of other inhuman or degrading treatment or punishment
  - Risk of persecution
  - Risk of death penalty
  - Threat to life
  - Threat to physical integrity
  - Threat to liberty
  - Risk of suffering other serious harm

- Torture and inhuman or degrading treatment or punishment:
  - Torture
  - Inhuman treatment
  - Degrading treatment
  - Effective investigation

- Trafficking in human beings

- Other Vulnerable persons and persons with specific needs:
  - Minors
    - Unaccompanied minors
  - Single parents with minor children
  - Pregnant women
  - Disabled people
  - Elderly people
  - Persons with serious illnesses
  - Persons with mental disorders
  - Victims of human trafficking
  - Victims of torture, rape or other serious forms of psychological, physical or sexual violence.

- Other (specify):
  - ........................................................................
  - ........................................................................
  - ........................................................................

- Personal data
- Private life:
  - Personal and bodily integrity

- Life:
  - Deprivation of life (arbitrary or unlawful)
  - Lives at risk:
    - Expulsion
    - Extradition
  - Use of force, not absolutely necessary:
    - Defence from unlawful violence
    - Effect lawful arrest
    - Prevent escape
    - Quell riot or insurrection
9. ARRANGEMENTS OF DEPLOYED RESOURCES

9.1. Operational Resources Management System (Opera)

https://fs.frontex.europa.eu/opera/

The Operational resources management system (Opera) is an integrated web-based software application custom-designed for the management of the operational resources pooled and deployed in Frontex coordinated activities. Information related to the availability and deployment of the resources is stored in the application and is available for the management of deployments of HR and TE, as well as creating reports.

The main functions of the Opera system are the following:

- To manage contributions to the HR (e.g. EBCG and TM (seconded) and TE Pools: personal data (including deployment history, profiles, photos, personal weapons details, participation in Frontex training, etc.) of officers nominated to the HR Pools is stored in the HR Pools database. MS nominate officers and update the information in real time by using Opera. The content is fully searchable and available for the other functionalities of the application. The same applies to the TE Pool database.

- To manage and allocate resources to joint operations and other activities by:
  - Creating and storing operational details such as duration, location, type of operation, operational needs in terms of HR and TE;
  - Supporting the generation of Frontex requests for availability of resources to the MS;
  - Managing the contributions and allocations of MS resources related to a given Frontex coordinated activity;
  - Managing the Running Expenses of Means templates;
  - Monitoring and registering the deployed resources.

- To issue secure accreditation and participant documents: information on the allocation of HR gives the Operational Team the possibility of easily creating requests for accreditation and participant documents for joint operations. The system is fully automated to ensure the correct type of card is allocated to the recipients.

- To generate reports: Opera gives Frontex and the MS the possibility of generating different types of report in a fully automated way such as: composition and statistics on the Pools, deployment overviews, lists of resources requested and the corresponding replies, the registration for officers, reports on the deployed resources in a given operation, as well as other custom made reports.

Users, according to the Instructions received during the Opera Training and procedures discussed and agreed in the Opera workshops, input information concerning the available/deployed resources, Running Expenses of Means related financial data, and officer registration details (necessary for issuing accreditation/participant’s documents) directly through the Opera dedicated interface.

9.1.1. Responsibilities

The division of responsibilities between Frontex and the MS in terms of use of Opera are as follows:

Frontex responsibilities:

- To create a given operation;
- To allocate the requests for HR and TE and to send the requests to the MS;
- To confirm the HR made available by MS to the teams, and to confirm the TE made available by MS to the Operation;
- To confirm the HR deployed in the teams, and, after the registration is completed by MS, to issue the accreditation/participant documents;
- To deliver the accreditation/participant documents to the HR deployed in the Operation;
- To collect the accreditation/participant documents at the end of the deployment (supported by the MS).
MS responsibilities:

- To answer the requests for HR and TE sent by Frontex under a particular Operation by making available resources registered in the HR and TE pools;
- To register the HR deployed by filling in all the required registration information, and to complete the registration of the accepted and deployed TE by adding information about the costs of the deployment;
- To support Frontex in collecting the accreditation/participant documents at the end of the deployment.

9.1.2. Registration of Human Resources

Adequate and timely input of all required registration information is a pre-condition to issue accreditation/participant documents which are produced via Opera application using the following input interface:

Under "Travel Details", MS input information concerning the arrival and departure dates (including indication of approximate time of arrival), Flight details if travelling by airplane, Mean of Transportation, Route, Arrival Airport, Entry BCP/Airport and Accommodation. In the event of Accommodation being provided by the host MS and being unknown at the time of registration, MS shall indicate this in the Accommodation box by the text "accommodation provided by Host MS".

The Expiry date of the Accreditation/Participant Document is automatically set as the date of departure from the operational area. In the event of any particular need (e.g. transportation by car, etc.) MS can manually extend the date in order to have the Accreditation/Participant Document valid until the arrival of the officer in his/her MS.
Under "Personal Equipment/Weapons", WS indicate if the officer is travelling to the operational area carrying weapons or not. If yes, WS also register the weapon and indicate the amount and type of ammunition to be carried. This field is mandatory.
Under "Technical Equipment", MS indicate if the deployed officer is linked to a specific item of Technical Equipment requested and deployed through Opera (e.g. helicopter, vessel, etc.), or if he is carrying with him/her any other item of Technical Equipment i.e. night vision goggles etc.

Under Access to FOSS, MS indicate if the officer is to have access to FOSS, and the type of access requested (including duration). More information about FOSS is provided in chapter 5.

Under Additional Information, MS/SAC also indicate the Daily Gross Wage, the Daily Subsistence Allowances, the Return Travel and Daily Accommodation Costs of the deployed officer for that specific operation.
### 9.1.3. Registration of Technical Equipment

In order to register the Technical Equipment made available for deployment in an operation, the IS User should go under the TE Registration and introduce the missing information, such as deployed to, host country and deployment locations, total estimated deployment costs, etc.

<table>
<thead>
<tr>
<th>ENUME</th>
<th>MENTAL</th>
<th>ECTOPIC TIONS</th>
<th>ECTOPIC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Aerial Means</strong></td>
<td>H2L - helicopter (HEL) - more than 2 hours aloft</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Terrestrial Means</strong></td>
<td>T7 - Patrol Car (PC)</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Terrestrial Means</strong></td>
<td>T8 - Vehicle equipped for border surveillance (TV)</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Portable Means</strong></td>
<td>T3 - Thermal Camera</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Portable Means</strong></td>
<td>T2 - Infrared Camera</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Terrestrial Means</strong></td>
<td>T7 - Patrol Car (PC)</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Portable Means</strong></td>
<td>T3 - Thermal Camera</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Portable Means</strong></td>
<td>T2 - Infrared Camera</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Terrestrial Means</strong></td>
<td>T7 - Patrol Car (PC)</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Terrestrial Means</strong></td>
<td>T7 - Patrol Car (PC)</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Terrestrial Means</strong></td>
<td>T7 - Patrol Car (PC)</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Terrestrial Means</strong></td>
<td>T7 - Patrol Car (PC)</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Terrestrial Means</strong></td>
<td>T7 - Patrol Car (PC)</td>
<td></td>
</tr>
<tr>
<td><strong>Incomplete</strong></td>
<td><strong>Terrestrial Means</strong></td>
<td>T3 - Vehicle equipped for border surveillance (TV)</td>
<td></td>
</tr>
</tbody>
</table>
9.2. Technical equipment deployed by Member States

Technical equipment deployed by the MS in the operational areas to foster the border control activities may include Offshore Patrol Vessels (OPV), Coastal Patrol Vessels (CPV), Coastal Patrol Boats (CPB), Helicopters, Fixed Wing Airplanes (FWA), Term Vision Vehicles (TTV), Dog Teams and any other type of equipment preliminary agreed and confirmed by Frontex and the MS.

The technical equipment deployed by the MS can form a part of the overall minimum number of technical equipment (OMNITE) or can be considered as additional technical equipment (beyond OMNITE). The OMNITE is identified by Frontex based on the risk analysis and the operational needs and it is foreseen to ensure sufficient operational response within Frontex coordinated joint operations. The additional technical equipment will supplement OMNITE, in case that any operational needs occur.

9.3. Management of the operational assets\(^6\) deployed by Frontex

PRU and JOU deal with the distribution and retrieval of operational assets in the operational areas, according to the procedures in place. The EBCGT members / representatives of the national authorities receive operational assets based on a pre-conducted needs assessment and are responsible for the maintenance in good conditions of the equipment while in their possession.

\(^6\) Frontex owned assets
The EBCGT members / representatives of the national authorities having received an operational equipment item have the obligation to return the item to the Frontex representative in charge with the distribution / retrieval of the operational assets, according to the conditions laid down in the handover forms.

In case the operational equipment is being damaged / misplaced / stolen while under the responsibility of an EBCGT member / representative of a national authority, the person to whom the equipment was handed over has the obligation to immediately inform the Operational Team about the occurrence.

9.4. Firearms and ammunitions transportation

- The aim of this practical note is to draw the attention to a sensitive issue of transporting weapons and ammunition. The guidelines are given in general and are still subject to more restrictive policy applied by the participating AG, airlines used for the particular legs of the journey and even the airport security authorities of both the departure and transfer airports.

- Basically, the key regulatory requirements to transporting firearms, firearm parts or ammunition by air are:
  1. The acceptance of firearms and ammunition on civil aircrafts is controlled by legislation of the country of origin and of destination (also transfer country in case of connecting flights)
  2. You must declare all firearms and ammunition to the airline during the ticket purchasing and counter check-in process. You should be also able to prove the ownership of the weapon at any time
  3. You may only transport firearms, ammunition and firearm parts in your checked baggage. Firearms, ammunition and firearm parts are prohibited from carry-on baggage. Such firearms shall be unloaded, i.e. free of ammunition, and suitably packed for such carriage
  4. Firearms must be packed separately from ammunition
  5. Firearms and ammunition are mostly transported in the cargo compartment of the airplane, as care by captain procedures are less and less used nowadays
  6. Ammunition must be securely box, for personal use only and may not be carried in quantities exceeding 5 kg (11 lb) per passenger. Any ammunition is to be securely packed in fiber (such as cardboard), wood or metal boxes or other packaging that is specifically designed to carry small amounts of ammunition
  7. The firearm must be packed in a hard-sided container
  8. The container must be locked. A locked container is defined as one that completely secures the firearm from access by anyone other than you. Cases that can be pulled open with little effort do not meet this criterion. The pictures provided here below illustrate the difference between a properly packaged and an improperly packaged firearm
  9. It is recommended that you provide the key or combination to the security officer if he or she needs to open the container. You should remain present during screening to take the key back after the container is cleared. If you are not present and the security officer must open the container, the airline will make a reasonable attempt to contact you. If contact attempt is not successful, the container will not be placed on the plane. Most of the regulations prohibit unlocked gun cases (or cases with broken locks) on aircraft
  10. You can’t use firearm magazines/clips for packing ammunition unless they completely and securely enclose the ammunition (e.g., by securely covering the exposed portions of the magazine or by securely placing the magazine in a pouch, holder, holster or lanyard)
  11. You may carry the ammunition in the same type of hard-sided case as the firearm, as long as you pack it as described above
You can’t bring black powder or percussion caps used with black-powder type firearms in either your carry-on or checked baggage.

Photo of a firearm properly packed.

Photo of a firearm and ammunition improperly packed.

- As already mentioned airlines or airports security authorities may have their own additional requirements on the carriage of firearms and variable amount of ammunition that you may have in your checked baggage. Therefore, you should also contact the airline regarding its firearm and ammunition carriage policies. In case of transfer flight to the destination airport you are to be aware also with the airport security policy of the transfer airport.

- In order to avoid any delays and possible seizure of the weapons and ammunition you should organize the shipment of the weapon package (properly documented and secured) according to the security rules and procedures of the transfer airport and also the next airline company. In case the second leg of the flight is scheduled by use of the different airline.

- In case of traveling by car you are kindly invited to set in contact with national responsible authorities (via NFPDC) of transiting MS(s) prior to the travel in order to receive transit permission if such is required.

The respective NFPDC must be informed via e-mail about weapon details (type, brand, serial number), the officers’ personal details (Surname, name) as well as the proper designation between officer and weapon either travelling by plane or car.
The communication to the NFPOC can be conducted either by e-mail or by registering the complete details in Opera platform. In case of registering the officers in Opera platform, the following details are required for issuing the weapon permits: Weapon details (type, brand, serial number), personal details (surname, name), entrance point, exact date of entrance, exact deployment period, route to be followed and the place of deployment.

NOTE: The applicant retains the obligation to get permission from requested airport.

*Clearance request form for VFR flights at night is available on FOSS.*
10. PROCESSING PERSONAL DATA FOR RISK ANALYSIS (PeDRA)
PILOT EXERCISE FOR DEBRIEFING ACTIVITIES

10.1. Aims, objectives and description
PeDRA aims to facilitate the collection of personal data during Frontex Joint Operations, and its transmission to Frontex for processing at the European level. Its objectives are to produce products based on the personal data that will help Frontex, MS and recipient agencies (Europol) to more effectively carry out their respective mandates in the field of cross-border crime.

The first phase of the Pilot exercise was launched in Triton in February 2016 and has successfully met all its objectives, most notably the transmission to Europol of the identities, locations, phone numbers and Facebook profiles of many individuals in Libya involved in people smuggling.

The second phase of the PeDRA Pilot Exercise was launched during JD Indalo, Hera and Minerva 2016 aiming to test data-capture templates, reporting protocols from the operational area and the transmission of personal data to Frontex. Corresponsingly there are several new activities in Frontex aimed at processing the personal data to produce risk analyses, and also cases for transmission to Europol.

As from November 2016 PeDRA was launched in JD Poseidon hosted by Greece.

10.2. Legal basis
According to Article 11c of the Frontex Regulation (1168/2011), Frontex may further process personal data collected by MS during Joint Operations, Pilot Projects and Rapid Interventions.

The Data Protection Regulation EC 45/2001 applies to the processing of personal data by Frontex under PeDRA.

Procedures for processing personal data are set out in Management Board Decision No 58/2015 adopting Implementing Measures for processing personal data collected by MS during Joint operations, Pilot Projects and Rapid interventions.

Information regarding the transfer of personal data to Europol can be found in Article 9 of the Operational Agreement between the Agencies that came into force in December 201515.

10.3. Scope of personal data
- Frontex can only process personal data collected by MS during Frontex Joint Operations, Pilot Projects and Rapid Interventions
- Frontex can only process personal data relating to individuals who are suspected, on reasonable grounds by the competent authorities of the MSs, of involvement in facilitation of illegal migration, human trafficking or other cross-border crimes
- The processing of such personal data shall respect the principles of necessity and proportionality
- Personal data can only be processed by Frontex for two purposes:
  - the transmission of personal data, on a case-by-case basis, to Europol
  - the production of risk analyses, the results of which will be depersonalised
- Personal data will be deleted in Frontex after 90 days

15 Agreement on Operational Cooperation between the European Agency for the Management of Operational Cooperation at the External Borders of the Union ("FRONTEX") and the European Police Office ("EUROPOL") http://www.europa.eu
10.4. Interoperability

The PeDRA has been designed to exploit a data-collection mechanism that has already been in existence in Frontex Joint Operations for several years (debriefing of newly arrived migrants), but with the additional and vital benefit of being able to accommodate the collection and transmission of personal data. To this end, a new and modernized debriefing template specifically designed to capture personal data is to be deployed during the PeDRA. This new online template requires debriefing officers to follow additional instructions for filling in the template and saving it in the correct format, and team leaders also need to know how to access and scrutinise the content of the templates before they are sent to the Intelligence Officer who makes the decision to send to Frontex.

To maintain data security during the PeDRA it is no longer possible for MS representatives to e-mail debriefing templates to frontex because they are expected to contain personal data and this would be a breach of the data protection regulation. The Intelligence Officer is instead requested to send debriefing templates to Frontex via to JORA, which has been recently updated to accommodate the transfer of personal data.

There is also in development a tool which will enable the host MS to extract information from debriefing templates for use and dissemination at the local and national levels.

10.5. Involved actors

The PeDRA only affects officers involved in debriefing activities, and those tasked with the transmission of debriefing templates to Frontex: i.e. debriefers, team leaders, TM (seconded) and Intelligence Officers.

10.6. Roles and responsibilities

- Debriefing experts
- All personal data
- Once the template has been
- Team leaders receive
- The Intelligence Officer will be able to
- Frontex receives templates in JORA.

Commented [A18]: The non-disclosed text contains detailed information regarding the modus operandi of law enforcement officials. It contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied to those activities which would jeopardise the implementation of ongoing and future operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above the text is not disclosed pursuant to the exception laid down in the First indent of Article 41(1)(e) of Regulation No 1049/2009 relating to the protection of the public interest as regards public security.
10.7. Work flow and responsibilities under the PeDRA Pilot Exercise

<table>
<thead>
<tr>
<th>Actors</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debriefers</td>
<td></td>
</tr>
<tr>
<td>Team Leaders</td>
<td></td>
</tr>
<tr>
<td>Intelligence Officer</td>
<td></td>
</tr>
<tr>
<td>Frontex</td>
<td></td>
</tr>
</tbody>
</table>

Commented [A19]: The non-disclosed text contains detailed information regarding the modus operandi of law enforcement officials. It contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied in those activities which would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above the text is not disclosed pursuant to the exception laid down in the first indent of Article 4(1)(a) of Regulation No 1047/2001 relating to the protection of the public interest as regards public security.

10.8. What is personal data?

Data are personal if they relate to an identified or identifiable person, the data subject. A person is identifiable if additional information can be obtained with reasonable effort, allowing the identification of the subject. Data are personal if an Individual, while not identified, is described in the Information in a way which makes it possible to find out who the data subject is by conducting further research.
10.9. Access requests

Commented [A20]: The non-disclosed text contains detailed information related to reporting tasks and methods used by law enforcement officials. The report contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied during border control activities which would jeopardize the implementation of future and ongoing operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above, the text is not disclosed pursuant to the exception laid down in the first indent of Article 41(3)(a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.
11. OTHER FRONTEX PRODUCTS AND SERVICES

11.1. Eurosur Fusion Services

11.1.1. Introductory Information
During 2014 Frontex gradually began to deliver the Initial EUROSUR operational services provided via the Eurosur Fusion Services (EFS). Throughout 2015-2016, their capabilities continue to improve in accordance with the operational needs arising during Frontex-coordinated Joint Operations. Services are delivered on a permanent basis or upon request.

11.1.2. Maritime Services
End to end maritime surveillance services, provided in cooperation with the European Maritime Safety Agency (EMSA) and other providers, are available to operational officers taking part in naval operations. Frontex organized activities are supported with the following services:

- S1 Incident Reporting Service
- S2 Vessel Monitoring and Tracking Service
- S3 Tracking Vessels of Interest
- S4 Vessel Detection Service
- S5 Meteo Service
- S6 Visual Data Discovery Service
- S7 Maritime Simulation Module
- S8 Satellite Imagery Service
- S9 Anomaly Detection Service
- S10 Supporting Information Service
- S11 Coastal Monitoring
- S12 Pre-frontier Monitoring
- S13 Reference Imagery / Mapping

In 2015 the new partnership with the EU SatCen allowed Frontex to provide to the MS new surveillance and analytical services based on Earth Observation (S11-S13).

The important element to assure effectiveness of the delivered services, is the follow up on MS side. Especially in case of Vessel Detection Service (S4) the operational follow up in the framework of the Joint Operation in all possible cases is paramount for the success and efficient use of the information delivered through the service.

Aligned with operational needs, the services are available via the JORA Visualization Module (JVM) and EUROSUR Application.

11.1.3. Vessel Detection Service
The Eurosur Information Services (Geospatial Information, Vessel Monitoring, Vessel Detection and Environmental Information) are available via the Eurosur Fusion Services (EFS) to support decision-making, planning and execution of missions. Aligned with operational needs, these services are accessible via the Eurosur Network and the JORA Visualization Module.

With specific reference to the Vessel Detection Service, it may be activated in support of maritime surveillance activities. For the most efficient implementation and exploitation of the service and in order to take full advantage of it, the Host MS takes all the appropriate actions according to the national legislation and rules of engagement for investigating the VDS detections and coordinating the adequate follow-up
activities. All operational results shall be reported via the reporting structure of the operation. Additional financial resources may be allocated by Frontex to ensure that aerial assets or, if not possible, other assets, are fully employed to investigate the objects of interest detected at sea during VDS-related activities.

**VDS Operational Activities - Actors and Responsibilities (general):**

- **NCC:**
  - Active involvement in the selection procedure of the VDS areas of acquisition with the relevant national competent authority
  - Constant updating on the potential detections, the operational measures taken and the results obtained.

- **ICC:**
  - Identification of the VDS areas of acquisition and execution of the operational activities;
  - Resource (Assets, Manpower) planning and cost-effective utilization;
  - Coordination of the adequate VDS follow-up actions;
  - Collection of operational findings and feedback (Joint Coordination Board), obtained by crews via their National Officers, in a logic of continual service improvement;

- **JOU/Sea Border Sector Operational Team:**
  - Identification and validation of the VDS areas of acquisition, in cooperation with all relevant partners;
  - Monitoring the implementation of the VDS within the framework of the JO and following up each detection with the PSC Service Manager;

- **Frontex Situation Centre:**
  - Financial allocation;
  - Identification and validation of the VDS areas of acquisition, in close cooperation with all stakeholders;
  - Approval of the validated areas of acquisition for further processing with EMSA;
  - Overall coordination and supervision of the acquisitions.

For more information, please send an e-mail to [email protected]

11.1.4. Weather Services

Based on the available state-of-the-art technology, the FSC delivers relevant, timely and accurate information on weather conditions, obtained from observation data and forecast models.

The tailored environmental services, including but not limited to, air temperature, cloud cover, wave height and wind direction and speed can be delivered to decision makers, operational planners and situational centres in order to support their decision-making, planning and execution of mission across the spectrum of Frontex-coordinated joint operations.

11.1.5. Other Services

Aligned with operational needs, these and other services are available via the EUROSUR Application and the JORRA Visualization Module (JVM).

A complete Service Description can be found in the Eurosur Fusion Services Service Catalogue, available on FOSS under the following location: [https://foss.frontex.europa.eu/FusionServices/](https://foss.frontex.europa.eu/FusionServices/)

The Catalogue provides also the details on how to request a service.

For more information, please contact: [email protected]
11.2. Medium Altitude Long Endurance (MALE) Remotely Piloted Aircraft Systems (RPAS) aerial surveillance trial

MALE RPAS offer potential for border surveillance. RPAS’s flexibility, endurance and long range enable them to cover large maritime areas and they can thus contribute to detecting cross-border crime and irregular migration and, most importantly, to support MS in saving human lives at sea. However, the cost-effectiveness and efficiency, together the feasibility of being able to exploit and integrate data in different end-users systems when flying in a Multi-purpose Mission, are two key issues that need to be verified and proofed in a practical way. This activity is going to be implemented in close cooperation between JOU/SIS and C300/RDU.

11.3. Frontex Positioning System

The aim of the Frontex Positioning System (FPS) is to implement reliable encrypted tracking system displaying positions and other data of deployed assets in real time in line with EUROSUR Regulation and to support assets’ financial management by applying automatic update cost calculations.

FPS will be implemented as an essential element in Frontex coordinated maritime joint operations. The system is composed by portable positioning devices installed on board assets participating in operations. The FPS supports the operational centres in reaching full situational awareness. The real time tracking of assets increases the reaction capacity and enhances the security of the crew members on board of participating units. FPS also offers features for Frontex to follow the financial aspects of deployment. The software enables to monitor the level of performed patrolling hours and to follow and update the financial documents according to the operational needs.

The installation of the positioning device on board of an asset needs to be approved by Home and Host MS. As an alternative solution, National Positioning Systems can be integrated into FPS. Home and Host MS shall provide the GPS position of assets joining Frontex operations in a format permitting further automatically processed.

11.4. Frontex Compatible Operational Image

The aim of the Frontex Compatible Operational Image (FCOI) is to implement secured and reliable web based platform with integrated tactical and operational data from variety of sources (geo-location, tracking data, photo imagery, motion pictures, and voice communication) and sharing close to real time data across multiple clients.

To test available MS technical solutions and their capabilities FCOI portable devices will be installed on preselected maritime and terrestrial assets participating in Frontex coordinated joint operations and on assets patrolling in EPN patrolling zones. To test available preselected MS aerial technical solutions participating MS will deliver aerial assets with their own equipment. FCOI will facilitate integration of MS existing equipment to single web based platform.

The FCOI supports the coordination centres in reaching full situational awareness and enhanced command and control function providing close to real time motion picture, two way voice communication, historical record capabilities and real time geo location Information via secured data transmission links.

Based on findings and outcomes achieved by past FCOI activities RDU will carry out a study to assess extended technological solutions to share sensors data and information at local level among different fixed and mobile assets, and to share sensors data/information from the local to higher levels in a reliable and secure way.

11.5. Staff Exchange

The aim of Staff Exchange is to facilitate networking and harmonization of core operational structures by deploying officers of the EU MS to the NCC/ICC/LCC/FP Sea as well as to hotspots/migration reception
centres of MS hosting maritime OP and other operational locations of common interest for national authorities, thus enabling deployed officers to acquire knowledge and specific know-how from experiences and good practices abroad by working with relevant officers in MS others than their own. Under the umbrella of this activity, there are also Common Patrols implemented in maritime surveillance areas of common interest between the EU MS.

The activity involves the specialized staff of the MS authorities, both from host MS and participating MS. In particular, the activity is addressed to operational officers of aforementioned operational structures as well as staff in charge of managing deployments of relevant operational resources, technicians, financial experts and Liaison Officers/crew members. Nevertheless, the list is not exhaustive and it is subject to modification based on MS needs for tailor-made staff exchanges.

11.6. Yellow Pages

Yellow Pages is a web-based and secure information service available 24/7 for authorized users on Frontex One Stop Shop (FOSS) platform.

The purpose is to support planning and performing operational deployments in the respective MS and particular locations of the Frontex coordinated maritime operations as well as to facilitate contacts, information sharing and awareness among the partner authorities.

Yellow Pages contains useful contact and logistics data in the structured and user-friendly format.

Link (after login/password to FOSS):

Link to the service is also available at Sea Borders front page on FOSS.

Yellow Pages provides specifically:

- logistics details on facilities and working conditions at the deployment locations with a particular highlight given to the Hotspots in Greece and Italy (e.g. airports, seaports, accommodation);
- answers to Frequently Asked Questions and links to other sources of deployments related information;
- contact data to the MS operational structures responsible for coordination of Frontex operations and national patrolling areas (e.g. LCCs, LCCs);
- links to relevant entities in maritime domain (e.g. Maritime Rescue Coordination Centres);
- contact details of Frontex representatives responsible for coordination of the operational activities.

The service is in constant development. Any questions or suggestions for improvement regarding content can be addressed to Yellow Pages team via e-mail.

Commented (A22): The non-disclosed text contains detailed information on the means of communication used by law enforcement officials within the joint operation. Their disclosure could lead to possible abusive usage with a view to jeopardize their work and harm the course of future and ongoing operations and thus facilitating irregular migration and affecting public security. In light of the above, the text is not disclosed pursuant to the exception in the first indent of Article 4(1)(a) of Regulation (EC) No 1049/2001 relating to the protection of the public interest as regards public security.
12. **TEMPLATES (EXAMPLES)**

All actual and tailored templates are published on FOSS on the website of respective Joint Operation. In the course of the preparation phase for the JO, additional templates might be developed. In such cases participating MS will be informed and additional template will be uploaded on FOSS.

12.1. **Serious Incident Report Template**

**Serious Incident Report no.**

<table>
<thead>
<tr>
<th>Reporting date:</th>
<th>Reporting person:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>FSC SIR Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
</tr>
<tr>
<td>Type of SIR</td>
</tr>
<tr>
<td>JORA Incident number (if any)</td>
</tr>
<tr>
<td>Joint Operation</td>
</tr>
<tr>
<td>Frontex SIR Coordinator</td>
</tr>
<tr>
<td>Incident date/time</td>
</tr>
<tr>
<td>Detection date/time</td>
</tr>
<tr>
<td>Original source of the Information</td>
</tr>
<tr>
<td>Location of the Incident</td>
</tr>
<tr>
<td>Is latitude unknown</td>
</tr>
<tr>
<td>Latitude</td>
</tr>
<tr>
<td>Is longitude unknown</td>
</tr>
<tr>
<td>Longitude</td>
</tr>
<tr>
<td>Reference to the operational area</td>
</tr>
<tr>
<td>Frontex resources involved (Human resources / co-financed technical equipment)</td>
</tr>
<tr>
<td>Type of resources / involvement</td>
</tr>
<tr>
<td>Dead persons</td>
</tr>
<tr>
<td>Injured persons</td>
</tr>
<tr>
<td>Missing persons</td>
</tr>
<tr>
<td>Serious Incident Report related to Search and Rescue action</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>SAR activated date/time</td>
</tr>
<tr>
<td>SAR activated by whom</td>
</tr>
<tr>
<td>Boat in distress</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Flag, name, IMO if available</td>
</tr>
<tr>
<td>Detected by</td>
</tr>
<tr>
<td>Detection done by Frontex co-financed asset</td>
</tr>
<tr>
<td>Intercepted by</td>
</tr>
<tr>
<td>Interception done by Frontex co-financed asset</td>
</tr>
<tr>
<td>Estimated people on board</td>
</tr>
<tr>
<td>Planned port of disembarkation</td>
</tr>
<tr>
<td>Departure country</td>
</tr>
<tr>
<td>Involved authorities</td>
</tr>
<tr>
<td>Fact of the case</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Measures</th>
</tr>
</thead>
</table>

| Assessment |
### 2.2. Technical Equipment Mission Report

<table>
<thead>
<tr>
<th>Patrolling asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission Number</td>
</tr>
<tr>
<td>Date</td>
</tr>
<tr>
<td>Responsible ICC/LCC</td>
</tr>
<tr>
<td>Operational Area</td>
</tr>
<tr>
<td>National Official</td>
</tr>
<tr>
<td>Asset location (airport, port)</td>
</tr>
<tr>
<td>Member State</td>
</tr>
<tr>
<td>Authority</td>
</tr>
</tbody>
</table>

### Mission Data Sheet

<table>
<thead>
<tr>
<th>Patrolling asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration/Call Sign</td>
</tr>
<tr>
<td>Commanding Officer</td>
</tr>
<tr>
<td>Communication means (e.g. SAT, HF, VHF, GSM, etc)</td>
</tr>
<tr>
<td>Mission scheduled</td>
</tr>
<tr>
<td>Mission executed</td>
</tr>
<tr>
<td>Brief description in case of deviation</td>
</tr>
<tr>
<td>Engine(s) start up:</td>
</tr>
<tr>
<td>Engine(s) cut off:</td>
</tr>
<tr>
<td>Take off/off berth:</td>
</tr>
<tr>
<td>Landing/on berth:</td>
</tr>
<tr>
<td>On station (ops area):</td>
</tr>
<tr>
<td>Off station:</td>
</tr>
<tr>
<td>Total committed hours according to the SFD (hrs:min):</td>
</tr>
<tr>
<td>Total executed hours so far (hrs:min):</td>
</tr>
</tbody>
</table>
Mission Events

Attach a chart showing the operational area(s) and the entire track flown/sailed while introducing a position mark at least each 1 hrs or occasionally depending on the cruising speed.

Mark and number ALL identified targets detected within the operational area(s) in this chart and describe briefly identified targets according to the number given in a legend (e.g. crafts type, course, speed, activity). Support identified targets with images.

In cases where incidents occurred outside of the operational areas and in cases where incidents occurred on the way towards to the operational area and vice versa applies the same.

Do not delete, filter of cut the footage in case of any incidents. ALL the footage taken in relation to any incidents within Frontex coordinated operations has to be forwarded asap to the designated ICC (preferably using down link capabilities) for further consideration.

Brief description about the mission event(s):
  e.g. migrant activities, SAR events, technical failures, cross-border crime (drugs, pollution, etc.)

Disembarkation in Third Country (if applicable)

Brief description about the incident(s) which requires disembarkation in TC: SAR events, technical failure, etc.
Minimum information to be provided regarding the protection of human rights of the persons taken on board and to be disembarked in TC:

Persons disembarked:
- number
- gender (if possible)
- age (if possible)
- nationalities (if possible)

Medical care provided/ Medical staff on board (Y/N)
<table>
<thead>
<tr>
<th>Language used for communication on board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Place of disembarkation indicated (e.g., pointed out on a map, etc)</td>
</tr>
<tr>
<td>Opportunity was given to each of person taken on board to declare the reasons of non-agreement on disembarkation to the place decided by the CO</td>
</tr>
<tr>
<td>Persons taken on board had an opportunity to consult the Legal advisor</td>
</tr>
</tbody>
</table>

Please note that aforementioned measures taken by the crew shall be conducted in a way that, in all instances, ensures the safety of the persons intercepted or rescued, the safety of the participating units or that of third parties.
12.3. PeDRA Interview Template

Commented [A22]: The non-disclosed text contain detailed information related to reporting tools and methods used by law enforcement officials. The text contains references to the methods applied by law enforcement officers to perform border control tasks in general and to counter illegal activities in particular. Its publicity would expose the working methods applied during border control activities which would jeopardize the implementation of future and ongoing operations, and thus facilitate irregular migration and other cross-border crime such as facilitation of irregular immigration, trafficking in human beings and terrorism. Therefore, public security will be affected. In light of the above the text is not disclosed pursuant to the exception laid down in the First Indent of Article 4(1)(a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.
12.4. Document Alert Template

<table>
<thead>
<tr>
<th>Immigration authority Name</th>
<th>National Immigration authority LOGO</th>
<th>National Flag</th>
</tr>
</thead>
</table>

DOCUMENT ALERT

Title

Document Type:  
IS Ref.:  
Fraud Type:  
BCP

(Picture of the falsified/forged document or part of that document)

(Brief description of the bogus document detection including the citizen status route and local of detection.)
DETECTION POINT #1

(Description of the detection point)

DETECTION POINT #2

(Description of the detection point)

Other Pictures and Descriptions:
12.5. User Access Request Form - FOSS

Request for - Please Specify: Select Option

<table>
<thead>
<tr>
<th>First Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name (CAPITAL LETTERS)</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Member</td>
<td></td>
</tr>
<tr>
<td>State/Country/Organisation</td>
<td></td>
</tr>
<tr>
<td>Job Title/Position</td>
<td></td>
</tr>
<tr>
<td>Date and User Signature</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Group(s)</th>
<th>Activity</th>
<th>Specify Duration of FOSS Access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Please specify duration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If OTHER:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Start date</td>
</tr>
<tr>
<td></td>
<td></td>
<td>End date</td>
</tr>
<tr>
<td>Only Basic Access</td>
<td>Library; help;</td>
<td>Select Option</td>
</tr>
<tr>
<td>National Authorities (Overview of all related activities)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Air Border Sector (ABS)</td>
<td>Please specify Joint Operation or Project</td>
<td>Select Option</td>
</tr>
<tr>
<td>Land Border Sector (LBS)</td>
<td>Please specify Joint Operation or Project</td>
<td>Select Option</td>
</tr>
<tr>
<td>Return Operations Sector (ROS)</td>
<td>Please specify Joint Operation or Project</td>
<td>Select Option</td>
</tr>
<tr>
<td>Sea Border Sector (SBS)</td>
<td>Please specify Joint Operation or Project</td>
<td>Select Option</td>
</tr>
<tr>
<td>Other activities/ projects and related content</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Sections</td>
<td>Please specify Section or Activity</td>
<td>Select Option</td>
</tr>
<tr>
<td></td>
<td>Please specify any additional activity or specific page on FOSS:</td>
<td>Select Option</td>
</tr>
<tr>
<td>National Frontex Point of Contact (NFPOC)</td>
<td></td>
<td>Select Option</td>
</tr>
</tbody>
</table>

1. Choose the relevant user group for viewing the information on FOSS.
2. Please note that if any other user group is selected and approved, access to those general FOSS sections is granted by default.
3. This group has access to the majority of FOSS content, excluding a few sections such as some pages related to the EUMUN project. For full access to EUMUN please select it under the OS section.
### Justify the need of access

<table>
<thead>
<tr>
<th>Validation/ Sign-off</th>
<th>Date</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOSS National User Coordinator</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOSS Area of Interest Owner</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Data Protection Statement:** These data are compiled solely for the purpose of access management to FOSS. Data subjects are entitled to have access to their data and to have those data corrected. Service requests should be directed to the FOSS User Administrator. Any concerns can be addressed to the FOSS User Administrator or the Personal Data Protection Officer.

---

13 Provide a short justification on what is your need to have access and what are the activities you are involved in.
14 To be completed only for requests submitted from RE/SC/Third Country National Authorities. Please provide a legitimate name and surname of FOSS National User Coordinator and a signature. If this is not possible, an e-mail may also be accepted if sent from the approved email account of the FOSS National User Coordinator, and with personalised e-mail signature included.
12.6. Intelligence Officer Report

INTELLIGENCE OFFICER DAILY REPORT

[Fields to be filled]

INTERVIEWS

- Information Retrieved from CARA Centres/Place of Deployment

DAILY ANALYSIS / INTELLIGENCE GAPS

1. Summary of Incident
   - Summary Incident 1
   - Summary Incident 2
   - Summary Incident 3
2. Intelligence Point of View
3. Other Relevant Information
4. JITs
5. Profile of Migrants
6. Facilitators
7. EUROPOL Feedback
8. Travel documents
9. Smuggling of drugs
10. Parallel Activities (irregular fishery, pollution, etc)
11. Stolen vehicles
12. Other (Judicial requests / SIS alerts)
13. Weather conditions affecting Experts deployment and JO activities

FLASH NEWS

[Sections for media and open sources]

Flash news
12.7. Team Leader’s Daily Report

<table>
<thead>
<tr>
<th>Dubbing Team:</th>
<th>Place of deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Number:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td>DD/MM/YYYY</td>
</tr>
<tr>
<td>Reporting period:</td>
<td></td>
</tr>
<tr>
<td>Team Leader:</td>
<td>Name/Surname</td>
</tr>
<tr>
<td>Interpreter:</td>
<td>Name/Surname</td>
</tr>
<tr>
<td>Gifts/Gratuity off duty:</td>
<td>Name/Surname</td>
</tr>
</tbody>
</table>

1. INTERVIEWS PERFORMED
(Brief description of the daily activity of the Team)

<table>
<thead>
<tr>
<th>Nationality</th>
<th>Males</th>
<th>Females</th>
<th>Minors</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Add rows if necessary)

<table>
<thead>
<tr>
<th></th>
<th>Total</th>
<th>Total</th>
<th>Total</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(incident)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type of evidence collected:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attach photos of boat/vessel/evidence/etc:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. DEBRIEFING ACTIVITIES

Brief Description of the daily activity of the team other than the interviews

3. ADDITIONAL INFORMATION / REMARKS

Information the team considers being important.

4. PLAN FOR NEXT DAY

Working day for: e.g. activities out of the center, place of interview, etc.
12.8. Team Leaders - Landing Report

Basic Information

Landing Report Reg.
Date and Time of Disembarkation
JORA Number (if available)
Operative Authority Involved
Type of Boat Intercepted
Boat Description
No. Migrants Disembarked: Total number
No. Facilitators Arrested: Total number
Claimed Nationalities
Departure Country
Departure Place
Time of Departure
Place of Disembarkation
State of Health of migrants
Death Cases

(Add rows if necessary)

<table>
<thead>
<tr>
<th>MIGRANTS</th>
<th>TOTAL</th>
<th>Male</th>
<th>Female</th>
<th>Minor Male</th>
<th>Minor Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>Countries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FACILITATORS</th>
<th>TOTAL</th>
<th>Male</th>
<th>Female</th>
<th>Minor Male</th>
<th>Minor Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>Countries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total

Description of the Incident

Brief Description of the event, information taken on the spot (routes, modus operandi, place and time of departure, boat/s, evidences detected inside the boat, health of the migrants, facilitators arrested, etc).

Description of the incident:
About the crew:
About the migrants:
About the sailing boat:

Place Deployment_yyyyymmdd_001_LANDING
Yyyy,mm,dd - 00:00h (24h)
Pictures

To attach pictures taken during the incident or pictures provided by the local authorities.

Name JO

Team Leader:
Debriefing Experts:
Interpreter/OM:
Place:
Date:
12.9. FSO Daily / Flash Report\textsuperscript{17}

Name of the joint operation

Number of the Report

Date of reporting

Reporting period

Reported from

1. Incidents\textsuperscript{18}

Description per Incident

2. Deployed Resources

<table>
<thead>
<tr>
<th>Type of resource</th>
<th>MS</th>
<th>Authority</th>
<th>Period of deployment</th>
<th>Names</th>
</tr>
</thead>
</table>

3. LCC Meeting & Participants

3.1. Participants

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
</tr>
</thead>
</table>

3.2. Outcome of the meeting

<table>
<thead>
<tr>
<th>Issues discussed</th>
<th>Outcome, decisions taken</th>
</tr>
</thead>
</table>

4. Additional Information

Other operational, logistical, practical issues

\textsuperscript{17} Delete which is not applicable
\textsuperscript{18} Flash Report contains only chapter 1
12.10. Report from Participant

All participants of the joint operation are kindly requested to fill in this template and to revert it to Frontex via email account xxxxxxxxxx@frontex.europa.eu within 7 calendar days after termination of the deployment.

The aim of the report is to gather feedback from the participants in order to support improvements for future operational activities.

<table>
<thead>
<tr>
<th>Data about deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the joint operation</td>
</tr>
<tr>
<td>Name of the participant</td>
</tr>
<tr>
<td>Member State / Authority</td>
</tr>
<tr>
<td>Period of deployment</td>
</tr>
<tr>
<td>Location of deployment</td>
</tr>
</tbody>
</table>

1. Did you receive and acknowledge OPLAN of the JO and if yes, was it in time and who provided it to you?

To be filled in by the participant

2. Did you receive enough information about JO from Frontex during General Briefing?

To be filled in by the participant

3. Did you receive enough information about JO from Host MS during the National Briefing?

To be filled in by the participant
4. Have you been satisfied with the organization and timelines of the Joint Operation (JO) and if not, why?
To be filled in by the participant

5. Was communication with Frontex and local authorities regular and sufficient for effective co-operation? Have you had sufficient feedback during the course of implementation of the JO?
To be filled in by the participant

6. Did you have the opportunity to generate ideas and contribute to the JO during the implementation phase?
To be filled in by the participant

7. What in your opinion were the strong and weak points of the JO?
To be filled in by the participant

8. If you had a power what would you change in this JO in order to achieve bigger added value for the EU?
To be filled in by the participant

9. Have you participated in any of the specific EBTG Profile training (Screening, Debriefer, Expert, Advanced-Level Document Officer training, etc) organized by the Frontex Training Unit?
To be filled in by the participant
10. What kind of training subjects you would like to propose / should be covered to improve your job performance during Frontex coordinated activity in future?

To be filled in by the participant

11. Did you observe any procedure or practice that raises concerns about fundamental rights compliance during JO?

To be filled in by the participant

12. Are you satisfied with your performance during the JO?

(Please make a self-assessment and describe in few words the pros and cons of your participation)

To be filled in by the participant

13. Would you like to participate again in Frontex coordinated JO and if yes, why?

To be filled in by the participant

14. Are there any comments/suggestions you would like to add?

To be filled in by the participant
12.11. Final Report from Member State

Each MS hosting and contributing to the JO and claiming for the final payment are requested to elaborate the Final Report and to revert it to the Frontex via email account XXXXXXXXX@frontex.europa.eu within 7 calendar days after termination of the deployment. (The report can be produced by each participating authority separately).

The template of the Final Report provides the minimum requirements for the report. The MS authorities are encouraged to include any additional information considered to be important to report.

<table>
<thead>
<tr>
<th>Data about deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the joint operation</td>
</tr>
<tr>
<td>Member State</td>
</tr>
<tr>
<td>Authority</td>
</tr>
<tr>
<td>Period of deployment</td>
</tr>
<tr>
<td>Location of deployment</td>
</tr>
</tbody>
</table>

1. Coordination and cooperation

Assessment of the coordination structure established during the JO: performance of Frontex (FX) and the hosting MS (KCC/LLC, Focal Points Sea, Police Stations, Detention Centers, BCPs, etc)
Level of cooperation between FX, host and participating MS during the JO Interagency cooperation (EMSA, E/CA, Europol, etc)

To be filled in by MS

2. Information flow

Assessment of the information flow between all actors involved in the JO (FX/KCC/KO/experts/assets/MS/MO/MS/FX feedback to the MS about ongoing JO and etc)
JORDA, FOSI usage

To be filled in by MS

3. Deployed resources

Participating authorities
Technical equipment: total number, type, periods of deployment, operational areas covered, patrolling hrs performed, etc
Experts: total number, periods, locations of deployment, activity performed by of different profiles' experts, etc
4. Operational results

Results achieved by the human and technical resources during the deployment period, e.g.:
- the number of migrants detected, prevented, intercepted, rescued, landed, identified, detained, repatriated;
- the number of migrants boats detected, prevented or intercepted;
- the number of facilitators identified/arrested;
- cross-border crimes identified;
- etc

5. Practical arrangements and logistics

Positive and negative aspects identified prior and during the implementation of JO OPERA

6. Additional information

Any additional information MS considers to be reported, including concerns related to fundamental rights during JO

7. Recommendations

From MS point of view

To be filled in by MS

Each Third Country participating as Observer in the joint operation and claiming for the final payment are requested to elaborate the Final Report and to revert it to Frontex via email account xxxxx@frontex.europa.eu within 7 days after termination of the deployment.

This report is not dedicated to evaluate host MS.

<table>
<thead>
<tr>
<th>Data about deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name of the joint operation</strong></td>
</tr>
<tr>
<td><strong>Third Country</strong></td>
</tr>
<tr>
<td><strong>Authority</strong></td>
</tr>
<tr>
<td><strong>Period of deployment</strong></td>
</tr>
<tr>
<td><strong>Location of deployment</strong></td>
</tr>
</tbody>
</table>

**Observations**

To be filled in Third Country (free text)
12.13. JORA End-user Feedback Template

To report an issue, proposal a suggestion or provide any recommendation, please fill in the following template and send it to the JORA Product and Service Management by e-mail [blank]

If you are reporting an error message that appeared while you were logged on to JORA, please save the relevant log and send it to us as an attachment along with this form. Thank you.

<table>
<thead>
<tr>
<th>Name of the JORA user</th>
<th>Frontex Unit / Sector</th>
<th>(If applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Members State</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Duty station</td>
<td></td>
</tr>
<tr>
<td>&quot;Name of the operation&quot;</td>
<td>Frontex Access Manager</td>
<td>Frontex Template Creator</td>
</tr>
<tr>
<td></td>
<td>National Access manager</td>
<td>BCP/BCU Incident reporter</td>
</tr>
<tr>
<td></td>
<td>LCC incident verifier</td>
<td>ICC incident verifier</td>
</tr>
<tr>
<td></td>
<td>FSC incident approver</td>
<td>No specific role in the system</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reported Issue</th>
<th>Login problem</th>
<th>Error message</th>
<th>Attribute</th>
<th>Drop-down list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Input</td>
<td>Validation Process</td>
<td>Data Modification</td>
<td>Data Loss</td>
</tr>
<tr>
<td></td>
<td>Export Function</td>
<td>Attachments</td>
<td>Dashboard</td>
<td>Development</td>
</tr>
<tr>
<td></td>
<td>User Friendliness</td>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Please describe the situation in detail on the reported issue. In case an error message appeared, please describe the sequence of actions taken before it appeared].

* As defined in the JORA system
* Please mark the box according to your role
* If an error message appears in JORA, please save the log and send it as an attachment.
* Attribute: it is the field shown in the Incident Template that contains a drop-down menu or its category (i.e.: Type of Incident + category; Irregular Border Crossing + one value of the drop-down menu).

## GENERAL OVERVIEW

<table>
<thead>
<tr>
<th>PLAN_UID</th>
<th>GEI</th>
<th>Asset</th>
<th>AREA</th>
<th>TYPE</th>
<th>RS</th>
<th>Authority</th>
<th>Location</th>
<th>Start of Mission</th>
<th>End of Mission</th>
<th>Dog</th>
<th>INITIALLY PLANNED PATROLLING TIME</th>
<th>Total Patrolling Time</th>
<th>% OF Fulfillment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan 14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: The table continues with more plans and details, not shown in the image.
12.15. Weekly Advanced-Level Document Officer report

<table>
<thead>
<tr>
<th>Reporting exports names:</th>
<th>XX / XXXX (starting with 01 for each export deployment)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of reporting:</td>
<td>XX / XX / XXXX</td>
</tr>
<tr>
<td>Place of deployment:</td>
<td>XXXX</td>
</tr>
</tbody>
</table>

### WEEKLY STATISTICS

<table>
<thead>
<tr>
<th>Nationality claimed by the holder</th>
<th>Weekly number of documents checked</th>
<th>Weekly number of document forgeries identified</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### WEEKLY HIGHLIGHTS

Please describe below the most significant findings from the reporting week:

**EXAMPLES:**
- Main nationality and type of forged/counterfeit travel documents checked
- Main forgery types identified
- Quality of forgeries
- Known prices paid for forged/documents
- Other notes if available
WEEKLY HIGHLIGHTS

Please copy anonymized examples of documents identified with some descriptions/explanations

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
12.16. Daily screening report

Available on FOSS in excel format.
13. ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Spelling</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
<td></td>
</tr>
<tr>
<td>ALDO</td>
<td>Advanced-Level Document Officer</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td></td>
</tr>
<tr>
<td>BCP</td>
<td>Border Crossing Point</td>
</tr>
<tr>
<td>BCU</td>
<td>Border Crossing Unit</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td></td>
</tr>
<tr>
<td>CFPOC</td>
<td>Central Frontex Point of Contact</td>
</tr>
<tr>
<td>CO</td>
<td>Commanding Officer</td>
</tr>
<tr>
<td>CM</td>
<td>Cultural Mediator</td>
</tr>
<tr>
<td>CPB</td>
<td>Coastal Patrol Boat</td>
</tr>
<tr>
<td>CPC</td>
<td>Central Police Coordinator</td>
</tr>
<tr>
<td>CPV</td>
<td>Coastal Patrol Vessel</td>
</tr>
<tr>
<td><strong>D</strong></td>
<td></td>
</tr>
<tr>
<td>DSR</td>
<td>Daily Situation Report</td>
</tr>
<tr>
<td><strong>E</strong></td>
<td></td>
</tr>
<tr>
<td>EASO</td>
<td>European Asylum Support Office</td>
</tr>
<tr>
<td>ERBGT</td>
<td>European Border and Coast Guard Teams</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EUROSUR</td>
<td>European External Border Surveillance System</td>
</tr>
<tr>
<td>EURTF</td>
<td>European Union Regional Task Force</td>
</tr>
<tr>
<td>EFS</td>
<td>Eurosur Fusion Service</td>
</tr>
<tr>
<td><strong>F</strong></td>
<td></td>
</tr>
<tr>
<td>FAM</td>
<td>Frontex Access Manager</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>FASS</td>
<td>Frontex Aerial Surveillance Services</td>
</tr>
<tr>
<td>FCO</td>
<td>Frontex Coordinating Officer</td>
</tr>
<tr>
<td>FER</td>
<td>Frontex Evaluation Report</td>
</tr>
<tr>
<td>FLO</td>
<td>Frontex Liaison Office</td>
</tr>
<tr>
<td>FOC</td>
<td>Frontex Operational Coordinator</td>
</tr>
<tr>
<td>FOSS</td>
<td>Frontex-One-Stop-Shop</td>
</tr>
<tr>
<td>FP</td>
<td>Focal Point</td>
</tr>
<tr>
<td>FSC</td>
<td>Frontex Situation Centre</td>
</tr>
<tr>
<td>FSO</td>
<td>Frontex Support Officer</td>
</tr>
<tr>
<td>FRO</td>
<td>Fundamental Rights Officer</td>
</tr>
<tr>
<td>FrenEx</td>
<td>European Border and Coast Guard Agency</td>
</tr>
<tr>
<td>FWA</td>
<td>Fixed Wing Airplane</td>
</tr>
<tr>
<td>GIS</td>
<td>Geographic Information System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>HF</td>
<td>High frequency</td>
</tr>
<tr>
<td>HQ</td>
<td>Headquarters</td>
</tr>
<tr>
<td>HR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>IEBM</td>
<td>Integrated Border Management</td>
</tr>
<tr>
<td>ICC</td>
<td>International Coordination Centre</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>IO</td>
<td>Intelligence Officer</td>
</tr>
<tr>
<td>JCB</td>
<td>Joint Coordinating Board</td>
</tr>
<tr>
<td>JDT</td>
<td>Joint Debriefing Team</td>
</tr>
<tr>
<td>JO</td>
<td>Joint Operation</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>JORA</td>
<td>Joint Operations Reporting Application</td>
</tr>
<tr>
<td>JOU</td>
<td>Joint Operations Unit</td>
</tr>
<tr>
<td>JRCC</td>
<td>Joint Rescue Coordination Centre</td>
</tr>
<tr>
<td>JRO</td>
<td>Joint Return Operation</td>
</tr>
<tr>
<td>LCC</td>
<td>Local Coordination Centre</td>
</tr>
<tr>
<td>LO</td>
<td>Liaison Officer</td>
</tr>
<tr>
<td>LO-TE</td>
<td>Liaison Officer - Technical Equipment</td>
</tr>
<tr>
<td>LPC</td>
<td>Local Police Coordinator</td>
</tr>
<tr>
<td>MRCC</td>
<td>Maritime Rescue Coordination Centre</td>
</tr>
<tr>
<td>MRSC</td>
<td>Maritime Rescue Sub-Centre</td>
</tr>
<tr>
<td>MS</td>
<td>Member State</td>
</tr>
<tr>
<td>NAM</td>
<td>National Access Manager</td>
</tr>
<tr>
<td>NCC</td>
<td>National Coordination Centre</td>
</tr>
<tr>
<td>NCP</td>
<td>National Contact Point</td>
</tr>
<tr>
<td>NFPOC</td>
<td>National Frontex Point of Contact</td>
</tr>
<tr>
<td>NO</td>
<td>National Official</td>
</tr>
<tr>
<td>OA</td>
<td>Operational Analyst</td>
</tr>
<tr>
<td>OM</td>
<td>Operational Manager</td>
</tr>
<tr>
<td>Opera</td>
<td>Operational Resources Management System</td>
</tr>
<tr>
<td>OPLAN</td>
<td>Operational Plan</td>
</tr>
<tr>
<td>OPV</td>
<td>Offshore Patrol Vessel</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Team</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>PeDRA</td>
<td>Personal Data for Risk Analysis</td>
</tr>
<tr>
<td>POB</td>
<td>People on board</td>
</tr>
<tr>
<td>PRU</td>
<td>Pooled Resources Unit</td>
</tr>
<tr>
<td>RAU</td>
<td>Risk Analysis Unit</td>
</tr>
<tr>
<td>RCC</td>
<td>Regional Coordination Centre</td>
</tr>
<tr>
<td>RDU</td>
<td>Research and Development Unit</td>
</tr>
<tr>
<td>RoE</td>
<td>Rules of Engagement</td>
</tr>
<tr>
<td>SAC</td>
<td>Schengen Associated Countries</td>
</tr>
<tr>
<td>SAR</td>
<td>Search and Rescue</td>
</tr>
<tr>
<td>SBS</td>
<td>Sea Borders Sector</td>
</tr>
<tr>
<td>SDO</td>
<td>Senior Duty Officer</td>
</tr>
<tr>
<td>SI</td>
<td>Serious Incident</td>
</tr>
<tr>
<td>SIR</td>
<td>Serious Incident Reporting</td>
</tr>
<tr>
<td>TE</td>
<td>Technical Equipment</td>
</tr>
<tr>
<td>TL</td>
<td>Team Leader</td>
</tr>
<tr>
<td>TM</td>
<td>Team Members</td>
</tr>
<tr>
<td>TM (seconded)</td>
<td>Teams Members seconded to the Agency</td>
</tr>
<tr>
<td>TRU</td>
<td>Training Unit</td>
</tr>
<tr>
<td>TVV</td>
<td>Term Vision Vehicle</td>
</tr>
<tr>
<td>VHF</td>
<td>Very high frequency</td>
</tr>
<tr>
<td>W</td>
<td>Weekly Analytical Report</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------</td>
</tr>
<tr>
<td>WAU</td>
<td>Weekly Analytical Update</td>
</tr>
</tbody>
</table>

Handbook to the Operational Plans of Joint Maritime Operations