

OPERATIONS DIVISION
Joint Operations Unit
LAND BORDERS SECTOR

Handbook to the Operational Plan

Land Border Operations

Approved by

.....
Signature

Berndt Körner
Deputy Executive Director

INDEX

Table of Contents

1. GUIDELINES FOR DEBRIEFING ACTIVITIES	6
1.1. Introduction	6
1.2. Debriefing	6
1.2.1. Tasks of Debriefing Experts	6
1.2.2. Preparation for debriefing	6
1.2.3. Identifying migrants for interview and checking belongings	8
1.2.4. Conducting debriefing sessions	8
1.2.5. Reporting	9
1.3. 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	14
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. FRONTEX ONE-STOP-SHOP (FOSS)	16
4.1. FOSS general information	16
4.2. FOSS access procedures	16
4.2.1. FOSS access authorization	16
4.3. Roles & Responsibilities	18
4.3.1. National FOSS User Coordinator	18
4.3.2. Area of Interest Owner	18
4.3.3. User Administrator's (FSC) - FOSS Service Manager	18
4.4. Navigation in FOSS	18
5. COMMUNICATION WITH THE PRESS	19
5.1. Introduction	19
5.2. Press communication rules	19

5.2.1.	General	19
5.2.2.	Tasks of press offices in the context of Joint Operations	19
5.2.3.	Management of Press Requests	20
5.2.4.	Specific guidelines for participating officers if approached by the media:	20
5.2.5.	Contact details	21
6.	JOINT OPERATIONS REPORTING APPLICATION (JORA)	22
6.1.	JORA General Information	22
6.1.1.	JORA product & service management	22
6.1.2.	JORA Roles and Responsibilities	22
6.2.	JORA Access Request Procedure	24
6.2.1.	Background	24
6.2.2.	Initial Access Request to the JORA System	24
6.2.3.	Access Request to specific operation	27
6.2.4.	Access Request Process	28
6.3.	Contact Details	28
6.4.	JORA Incident Template Attributes' List	29
7.	SERIOUS INCIDENT REPORTING	31
7.1.	Introductory information	31
7.2.	Definition	31
7.2.1.	Serious Incident (SI)	31
7.2.2.	Serious Incident Report (SIR)	31
7.3.	Roles and responsibilities	31
7.3.1.	Participant of Frontex activities in the field	31
7.3.2.	Frontex staff in the operational area (FSO, FOC, etc.)	31
7.3.3.	Operational Manager (OM)	31
7.3.4.	FSC Senior Duty Officer (SDO)	32
7.4.	Content of a SIR	32
7.5.	SIR procedure - Chronology of reporting serious incidents	32
7.5.1.	Initial SIR	32
7.5.2.	Formal SIR	33
7.5.3.	Updated SIR	33
7.5.4.	Final SIR	33
7.6.	Reporting of SI with alleged violation of fundamental rights (FR)	33
7.6.1.	Reporting mechanism	33
7.7.	Frontex internal follow up procedure / SIR-Coordinator	34
7.8.	Personal Data	34
7.9.	Public access	34
7.10.	Serious Incident Catalogue	34
7.10.1.	Serious Incident Categories	34
7.11.	Serious Incident Reporting Mechanism	37
7.12.	List of potential fundamental rights violations within Frontex activities	38
8.	ARRANGEMENTS OF DEPLOYED RESOURCES	39
8.1.	Operational Resources Management System (Opera)	39

8.1.1.	Responsibilities	39
8.1.2.	Registration of Human Resources	40
8.1.3.	Registration of Technical Equipment	43
8.2.	Technical equipment deployed by Member States	44
8.3.	Management of the operational assets deployed by Frontex	44
8.3.1.	Firearms and ammunitions transportation	45
8.4.	Clearance request form for VFR flights at night	48
9.	PROCESSING PERSONAL DATA FOR RISK ANALYSIS (PeDRA) PILOT EXERCISE FOR DEBRIEFING ACTIVITIES	49
9.1.	Aims, objectives and description	49
9.2.	Legal basis	49
9.3.	Scope of personal data	49
9.4.	Interoperability	50
9.5.	Involved actors	Error! Bookmark not defined.
9.6.	Roles and responsibilities	Error! Bookmark not defined.
9.7.	Work flow and responsibilities under the PeDRA Pilot Exercise	51
9.8.	What is personal data?	51
9.9.	Access requests	52
10.	OTHER FRONTEX PRODUCTS AND SERVICES	53
10.1.	Eurosur Fusion Services	53
10.1.1.	Weather Services	53
10.1.2.	Other Services	53
10.2.	Medium Altitude Long Endurance (MALE) Remotely Piloted Aircraft Systems (RPAS) aerial surveillance trial	53
11.	TEMPLATES (EXAMPLES)	54
11.1.	Serious Incident Report Template	54
11.2.	Technical Equipment Mission Report	56
11.3.	PeDRA Interview Template	59
11.4.	Document Alert Template	60
11.5.	User Access Request Form - FOSS	62
11.6.	Intelligence Officer Report	64
	INTERVIEWS	64
	DAILY ANALYSIS / INTELLIGENCE GAPS	64
	FLASH NEWS	64
11.7.	FSO Daily / Flash Report	65
11.8.	Report from Participant	66
11.9.	Final Report from Member State	69
11.10.	Final Report from Third Country	71
11.11.	JORA End-user Feedback Template	72
11.12.	Report on screening, fingerprinting and documents' checks	73
12.	ACRONYMS	75

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 channeled 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.

1.2.1. 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) [REDACTED] 3) debriefing and 4) reporting.

1.2.2. 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.

Commented [A1]: The non-disclosed parts contain detailed information regarding the modus operandi of law enforcement officials when performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing them and the efforts made by the EU and its Member States to counter and prevent cross-border crime and unauthorized border crossings. If this were to happen, public security would 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 (EC) No 1049/2001 relating to the protection of the public interest as regards public security.

In addition, the debriefing expert should be aware of intelligence gaps¹ 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, Members of the Teams 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 [REDACTED]

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 [REDACTED]

If the debriefing [REDACTED]

Prior to the start of the actual debriefing of migrants, [REDACTED]

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 or 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.

Commented [A2]: The non-disclosed parts contain detailed information regarding the modus operandi of law enforcement officials when performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing them and the efforts made by the EU and its Member States to counter and prevent cross-border crime and unauthorized border crossings. If this were to happen, public security would 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 (EC) No 1049/2001 relating to the protection of the public interest as regards public security.

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.

Identifying migrants for interview

Debriefing should

Before meeting

Debriefing experts, with the assistance of interpreters,

During the identification of migrants for interview

The

Therefore, where possible and in accordance with the law of the host MS,

Commented [A3]: The non-disclosed parts contain detailed information regarding the modus operandi of law enforcement officials when performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing them and the efforts made by the EU and its Member States to counter and prevent cross-border crime and unauthorized border crossings. If this were to happen, public security would 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 (EC) No 1049/2001 relating to the protection of the public interest as regards public security.

1.2.4. 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. The potential asylum seekers will be informed of the procedure for launching an asylum application and shall be referred by the debriefing expert to the respective national authority.

Only through gaining the trust of the migrants can the debriefing process produce meaningful results.

The procedure should never be described as an interrogation, which suggests a more forceful and formal line of questioning - it is a voluntary interview.

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/if 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

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 stipulated in the operational plan. Debriefing reports should be sent, stored and treated with confidentiality and should be separated from other reports according to the operational plan. Persons other than the assigned officers from the local authorities, the analyst supporting the operation and the operational manager should not be entitled to receive the interview reports. As a general rule they should be distributed strictly on a need to know and to act basis. Debriefing reports often contain sensitive data and disclosing the information from the interviews may seriously jeopardize the confidential nature of the debriefing activities and impact negatively on the final outcome.

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.

1.3. 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.

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 document. 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 returning the Third Country national to her/his country of origin.

Screening experts will perform screening interviews at the request of the host MS authorities. For the purpose of supporting host MS developing screening activities, 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.

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. 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:

- who is responsible for his/her security
- who from the national authorities is responsible to perform a body/luggage search
- the age and gender of the migrant (special attention should be paid to minors or women from other cultures)
- which claimed nationalities should be screened (in order to prepare the correct screening forms and arrange an interpreter)
- what kind of background info should be available
- what kind of screening forms are needed
- if an interpreter is available on the spot/by phone

2.5. Checking belongings

The screening expert has no mandate to check the belongings of an irregular migrant, however he/she can offer advice to the responsible officer of the national authority based on his/her own experience of locating hidden documents inside belongings.

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 should use his knowledge and experience and the tools available such as the screening booklet to acquire the necessary information to complete the screening form to reach a presumed nationality.

The persons alleging a violation of their fundamental rights will be informed of the procedure for reporting such FR violations. The potential 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 groups:

"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 allowed an informal conversation before the interview starts. It is often the case that the interpreter is the first person to engage with the migrant as they share a common language. This informal conversation will help the migrant feel more comfortable to speak with interpreter. For this reason, it is often better to place the interpreter next to the migrant. 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 be verbatim (directly from what is said, using the first person singular 'I', rather than 'he said that'). Where possible the tone and emotion of what is being said should also be conveyed. Interpreters should clarify when they are interjecting their own opinion, or making a personal statement. Generally interpretation should be consecutive, rather than simultaneous (the migrant will speak, and then the interpreter will translate).

During interview the screening expert should speak directly to the migrant. He/she should speak in their normal voice and only for a short time (one longer sentence or three or four short sentences), stopping where there is a natural break to allow the interpreter to translate. Answers should not be interrupted. Complicated sentence structures and changes of direction mid-question should be avoided, as should jargon, idioms, technical words and cultural references that the migrant may not understand. (The interpreter would then have to use explanatory phrases and this may unnecessarily prolong the interview). By communicating clearly and patiently, a good result will be developed and can avoid significant misunderstandings.

The interpreter should not be held responsible for what the migrant does or does not say. The interpreter is the medium, not the source of the information. During interview the screening expert must not say anything that should not be translated, such as 'in jokes' or asides. The migrant could feel marginalized or demeaned, unable to tell whether the conversation is about them. It is also possible that the migrant understands what is being said and their level of comprehension is much better than admitted.

2.7. Working as a team with Interpreters

A qualified interpreter knows his/her role, limitations, and responsibilities. Whilst the screening expert controls the structure of the interview and asks the questions, an experienced interpreter should have limited freedom to clarify specific answers and to guide the screening expert as to any cultural or linguistic factors which may impact on the direction of the questioning. They can establish the truth quickly and accurately, and perceive cultural and emotional subtleties more clearly. Most importantly, they can assist in the determination of the presumed nationality, usually within a very short time.

An important task for the interpreter is to give the screening expert feedback on the reliability of the information received. Their own experience, language expertise and cultural background are valuable assets that can be used to evaluate the credibility and reliability of the information provided by the migrant. When combined with the experience and knowledge of the screening expert, this feedback can deliver high quality information.

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.

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;
- taking restrictive measures to prevent absconding in case migrants refuse fingerprinting, ensuring respect of fundamental rights;
- informing migrants in a timely manner of their rights and obligations and consequences of non-compliance with rules on identification.

3.2. Tasks of experts

Fingerprinting and registration activities shall be carried out according to the host Member State'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 information process it is highly recommended that Host MS prepare relevant number of posters in the registration places.

3.2.2. Use of force

In case counselling does not succeed, and if the host Member States does not consider, where other less coercive alternatives to detention cannot be applied effectively, detaining him/her, the Host Member State 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 Member States 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. 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. 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 for collecting the fingerprinting and the manner in which fingerprints will be processed is of the outmost 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 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. It is suggested that the use of coercion should always be recorded and that 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.

4. FRONTEX ONE-STOP-SHOP (FOSS)

4.1. 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 Member States 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 Member States, 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

4.2. 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 (Members of the Teams, Observers, etc)..

4.2.1. 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 Members of the Teams and other experts.

4.2.1.1. Access authorization procedure for Members of the Teams via OPERA:

When 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) is used the process of requesting and authorizing access to FOSS is fully performed through this system, by completing the section "Access to FOSS", 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 Member of the Teams
- By checking the box "Yes" (in the "Access to FOSS" tab), the NFPOC authorises access to FOSS for the relevant person

- By checking the box “No” (in the “Access to FOSS” tab), the NFPOC does not authorise access to FOSS for the relevant person
- 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. Start and end date can be freely decided, but it is recommended requesting FOSS access before the start of the deployment (for example 15 days in advance). It is also recommended to allow access to operational documents available in FOSS 30 days after the end of the deployment.

The screenshot shows a web interface with a navigation bar at the top containing tabs: "Travel Details", "Personel Equipment/Weapons", "Technical Equipment", "Documents", "Access to FOSS", and "Additional Information". The "Access to FOSS" tab is active and highlighted in blue. Below the navigation bar, there is a section titled "Access to FOSS" with a sub-section containing a radio button for "YES" and a radio button for "NO". Below this, there are three input fields: "Date From", "Date To", and "Type of Access". The "Date From" and "Date To" fields are highlighted with red circles. At the bottom of the form, there are buttons for "Export as Pdf", "Send Notification", "Save Registration", and "Close".

“Type of Access”, by selecting one of the following options:

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

This screenshot is similar to the previous one, showing the "Access to FOSS" form. In this view, the "Type of Access" field is highlighted with a red circle. The "Date From" and "Date To" fields are also visible but not highlighted.

4.2.1.2. Access authorization procedure for Seconded Members of the Teams:

- For Seconded Members of the Teams the same FOSS access procedures as for Frontex staff apply. Unless otherwise requested by the Operational Manager, the Seconded Member of the Teams 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.

4.2.1.3. 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.

4.3. Roles & Responsibilities

4.3.1. National FOSS User Coordinator

This function is assigned to the relevant MS's NFPOC. His/her responsibilities include gathering user data, validating access and providing user data to the "Area of Interest Owner" (Operational Manager).

4.3.2. 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.

4.3.3. 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.

4.4. 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.

5. COMMUNICATION WITH THE PRESS

5.1. Introduction

All Frontex activities are financed from public funds (EU budget) therefore it is Frontex' 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 member states 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.

5.2. Press communication rules

5.2.1. 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.

5.2.2. 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

5.2.3. 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 the 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 in the host MS will process the necessary authorisations, coordinate the flow of national press requests received and inform the 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 in the host MS will process the necessary authorisations for participation of journalists in patrols and visits to restricted operational areas. The press office in the host MS will inform the interested parties and the Frontex Press Office about the decision.
- The press office in 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 member state which deploys the Member of the Teams needs to be informed and approve the press request.

5.2.4. 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 members of the teams prior to the interview about the media, subject of the interview and sensitive topics.

What

[REDACTED]

Commented [A5]: The non-disclosed parts contain detailed information regarding the modus operandi of law enforcement officials when performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing them and the efforts made by the EU and its Member States to counter and prevent cross-border crime and unauthorized border crossings. If this were to happen, public security would 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 (EC) No 1049/2001 relating to the protection of the public interest as regards public security.

[REDACTED]

Please refer journalists to Frontex spokespeople 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).

5.2.5. Contact details

The contact details of the Frontex Press Office members and the press office of the National Authority of the Host MS are indicated in the respective Specific Annex of the Operational Plan "Contact Details".

Commented [A6]: The non-disclosed parts contain detailed information regarding the modus operandi of law enforcement officials when performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing them and the efforts made by the EU and its Member States to counter and prevent cross-border crime and unauthorized border crossings. If this were to happen, public security would 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 (EC) No 1049/2001 relating to the protection of the public interest as regards public security.

6. JOINT OPERATIONS REPORTING APPLICATION (JORA)

6.1. JORA General Information

6.1.1. 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 Owner;
- 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 FOSS.

6.1.2. JORA Roles and Responsibilities

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

6.1.2.1. 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.

6.1.2.2. JORA Frontex Access Manager

- Operational 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;

- Manages the access requests coming from members of the EU Institutions, from Frontex, and from other authorities who take part to the operation;
- Assigns and manages the National Access Managers appointed to the operation in the JORA system;
- Selects delegated Operational Manager(s) in the system when a new operation is created;
- Acts as the Incident Template Verifier;
- Manages users concerning this operation.

6.1.2.3. Delegated JORA Frontex Access Manager

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

6.1.2.4. 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.

6.1.2.5. JORA National Access Manager

National Access Managers are nominated by their Member States / 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.

6.1.2.6. 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.

6.1.2.7. 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.

6.1.2.8. 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.

6.2. JORA Access Request Procedure

6.2.1. Background

The implementation of JORA started in December 2011 with the aim to deliver Frontex and its internal and external stakeholders (Member States, 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 to use JORA, the Microsoft Silverlight should be installed in the user's personal computer or laptop. It is available in the Microsoft official webpage, free of charge:

<http://www.microsoft.com/getsilverlight/Get-Started/Install/Default.aspx>

6.2.2. Initial Access Request to the JORA System

In order to maintain a high level of security of the data, all users requesting access to the JORA are required to comply with the below guidelines when requesting access.

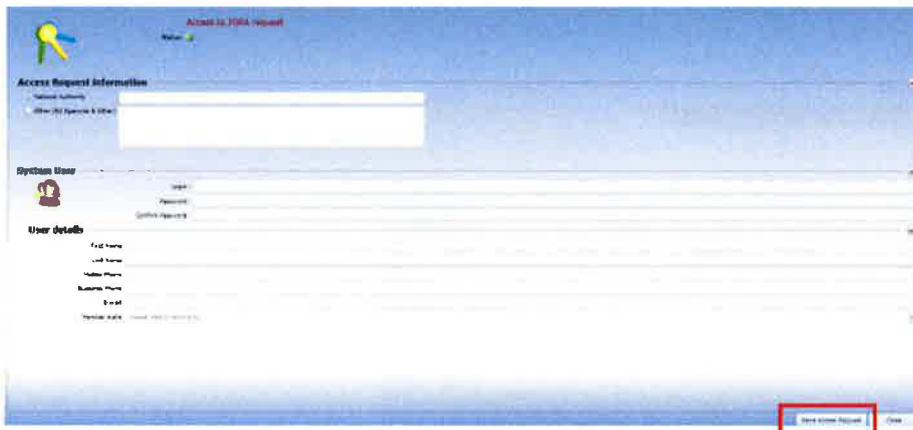
Each user should request access individually by entering the following website:
<https://fis.frontex.europa.eu/jora/>.

After the webpage loads, the access requester should click on Access Request (as shown in the below icon)...



The image shows the login page of the Frontex system. At the top, it says "Type your user name and password." and "FRONTEX" with a logo. There are two input fields: "User name:" and "Password:". Below these is a "Sign In" button. At the bottom left, there is a link "Define Access Request" and a link "AccessRequest" which is highlighted with a red box.

...and fill in the relevant form. Upon completion, users should send the access request by clicking on the bottom-right part of the webpage (Send Access Request).



The image shows the "Access Request Information" form. It has a header "Access Request Information" and a sub-header "National Authority". There is a large text area for "Free text". Below this is a "System User" section with fields for "User name", "Password", and "Confirm Password". At the bottom right, there is a "Send Access Request" button highlighted with a red box.

The Access Request page is divided in several areas, each of which contains specific fields to be filled out by the access requesters. Below you will find a more detailed description of each area:

6.2.2.1. Access Request Information

Two options are available for the user here:

- "National Authority" refers to users coming from Law Enforcement Authorities, Ministries and all similar national entities; and
- "Other (EU Agencies & Other)" refers to users representing EU Institutions or Agencies and all other entities which do not fall in the first category.

After choosing one of the two options, the user fills the "free text" field, which stands next to his/her choice, with the name of his/her Service/Agency/entity.



The image shows a close-up of the "Access Request Information" form. It has a header "Access Request Information" and two radio buttons: "National Authority" (selected) and "Other (EU Agencies & Other)". There is a large text area for "Free text".

6.2.2.2. System User

Each user shall create his/her own user name and password by complying with the criteria described below.

6.2.2.3. Login Requirements

[REDACTED]

6.2.2.4. Password Requirements

[REDACTED]

Commented [A7]: 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.

6.2.2.5. User Details

The user's details should be filled out accordingly. The e-mail provided by the user should be the work e-mail.

After applicants have submitted (on-line) their request, they are required to check their own e-mail (required in the JORA Access Request Form), as an automatic notification is sent by JORA to their e-mail address: it contains a link that should be copied and pasted to the browser (Mozilla, Explorer, etc.). After clicking ENTER, applicants should wait a few seconds before closing the browser.

The relevant National Access Manager shall, then, give applicants the initial access to JORA (this will allow users to be later able to request access to one (or more) specific operation(s), as described below).

Remark: It may take one or more days for users to receive access, depending on the response time of the National Access Manager.

6.2.3. Access Request to specific operation

After the initial access request procedure is completed, and the user receives access to the JORA System, then JORA user should enter (log in) the JORA with his/her credentials (URL: <https://fis.frontex.europa.eu/jora/>), and should define access request under "QUICK TAKS" by clicking on "Define Access Request", as shown below.



After the user fills in the access request form, he/she should send it by clicking the SEND button.



The request now has been submitted and is pending for approval by the National Access manager of the specific operation and/or Frontex Access Manager (FAM) and/ or JORA's Administrator. As soon as, the request is approved, the user may sign in JORA and have access to all requested data.



6.2.4. Access Request Process



* National Access Manager (NAM) of the requestor's Country.

**National Access Manager (NAM) of the MS hosting the joint operation, as listed in the Operational plan. If the NAM is not available, the Frontex Access Manager (FAM) can validate the operational access.

6.3. 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:

Email: [REDACTED]

Commented [AB]: The non-disclosed text contains information on the means of communication used by law enforcement officers within the operation. Its disclosure could lead to possible abusive usage with a view to jeopardize their work and harm the course of future and ongoing operations, ultimately obstructing their purpose to counter and prevent cross-border crime as well as prevent unauthorized border crossings. 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.

6.4. JORA Incident Template Attributes' List

General information

No	Name of attribute	Mandatory ³	Remarks
1	[REDACTED]	[REDACTED]	
2	[REDACTED]		
3	[REDACTED]	<input type="checkbox"/>	
4	[REDACTED]	<input type="checkbox"/>	
5	[REDACTED]		
6	[REDACTED]	[REDACTED]	
7	[REDACTED]	<input type="checkbox"/>	
8	[REDACTED]		
9	[REDACTED]		
10	[REDACTED]	<input type="checkbox"/>	
11	[REDACTED]	<input type="checkbox"/>	
12	[REDACTED]	<input type="checkbox"/>	
13	[REDACTED]	<input type="checkbox"/>	
14	[REDACTED]		
15	[REDACTED]		
16	[REDACTED]	<input type="checkbox"/>	
17	[REDACTED]	<input type="checkbox"/>	
18	[REDACTED]		
19	[REDACTED]	<input type="checkbox"/>	
20	[REDACTED]	<input type="checkbox"/>	
21	[REDACTED]	<input type="checkbox"/>	

Commented [A9]: 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.

³Please 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.

Persons Information

22	[REDACTED]	[REDACTED]	[REDACTED]
23	[REDACTED]	[REDACTED]	[REDACTED]
24	[REDACTED]	[REDACTED]	[REDACTED]
25	[REDACTED]	[REDACTED]	[REDACTED]
26	[REDACTED]	[REDACTED]	[REDACTED]
27	[REDACTED]	[REDACTED]	[REDACTED]
28	[REDACTED]	[REDACTED]	[REDACTED]
29	[REDACTED]	[REDACTED]	[REDACTED]
30	[REDACTED]	[REDACTED]	[REDACTED]
31	[REDACTED]	[REDACTED]	[REDACTED]

Commented [A10]: 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.

Additional Information

32	[REDACTED]	[REDACTED]	[REDACTED]
33	[REDACTED]	[REDACTED]	[REDACTED]
34	[REDACTED]	[REDACTED]	[REDACTED]
35	[REDACTED]	[REDACTED]	[REDACTED]
36	[REDACTED]	[REDACTED]	[REDACTED]
37	[REDACTED]	[REDACTED]	[REDACTED]
38	[REDACTED]	[REDACTED]	[REDACTED]
39	[REDACTED]	[REDACTED]	[REDACTED]
40	[REDACTED]	[REDACTED]	[REDACTED]
41	[REDACTED]	[REDACTED]	[REDACTED]

7. SERIOUS INCIDENT REPORTING

7.1. 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 actors⁴ in Frontex activities⁵ 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.

7.2. Definition

7.2.1. Serious Incident (SI)

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. 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.

7.2.2. Serious Incident Report (SIR)

SIR is a product aimed informing Frontex Senior Management, Member States, 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 ~~Error!~~ Reference source not found.). 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.

7.3. Roles and responsibilities

In order to ensure the immediate information flow after the occurrence of a SI and to enable that Frontex and all involved parties take appropriate action, it is crucial that all actors involved in Frontex activities understand their role within the SIR procedure (Chapter ~~Error!~~ Reference source not found.).

The actors involved in the SIR mechanism are:

7.3.1. Participant of Frontex activities in the field

Every participant related to or involved in Frontex activities is under an obligation to report immediately a SIR to FSC (in line with the reporting structure of the particular joint operation or by using the exceptional reporting), in case he/she receives the knowledge or is directly involved in a SI based on the SI-Catalogue.

7.3.2. Frontex staff in the operational area (FSO, FOC, etc.)

Responsible contact point in the operational area between the involved participants in the field, the host coordination centres (NCC, ICC, RCC, LCC) and FSC.

7.3.3. Operational Manager (OM)

Responsible Frontex officer to coordinate further operational information gathering from the actors in the field, if needed, in close cooperation with FSC.

⁴ All persons participating in activities coordinated or led by Frontex

⁵ Frontex activity means any activity coordinated or led by Frontex

7.3.4. FSC Senior Duty Officer (SDO)

Responsible for assessing the SI related to its severity, coordinating the information exchange, processing and distributing the SIR without personal data and further monitoring the situation based on the SI.

7.4. Content of a SIR

The SIR includes among others the following content (whenever possible) with respect to the serious incident occurred:

- HEADER (in the subject line), containing keywords for the serious incident
- WHAT....happened?
- WHEN....did it happen?
- WHERE....did it happen?
- WHO.....was involved/affected?
- WHY.....did it happen?
- HOW.....did it happen?
- MEANS USED: which means were used to carry out the actions leading to the incident? Frontex assets involved?
- SOURCE OF INFORMATION: who provided the information; reliable/not reliable source/information
- ACTIONS TAKEN (Measures): own actions and actions from MS/others
- POSSIBLE CONSEQUENCES (Assessment), EFFECTS, REACTIONS
- COMMENTS (if any)
-

7.5. SIR procedure - Chronology of reporting serious incidents

Every actor involved in Frontex activities is under an obligation to initiate immediately the necessary measures to commence the SIR procedure in case he/she has the knowledge, witnesses or is directly involved in a SI according to the SI-catalogue. The reporting of SI within joint operations coordinated by Frontex must be in line with the reporting structure for the particular joint operation, or alternatively, by using the exceptional reporting according to Chapter **Error! Reference source not found.**.

Please note:

In case of doubts whether the incident fulfils the requirements of a SIR, the FSC may be contacted directly. The FSC Senior Duty Officer provides support on a 24/7 on call service.

7.5.1. Initial SIR

- In order to ensure the immediate information flow to FSC a SI has to be reported through an initial SIR within the first 2 hours after such knowledge has been attained (**Chapter Error! Reference source not found.**).
- The initial SIR contains a summary of the information known at that point of time. This initial SIR serves as preliminary information to obtain immediate knowledge about the incident, and does not need, at this stage, any final confirmation of the incident.
- The initial SIR is not bound by any form and can be reported by using available means of communication.
- The FSC SDO assesses the initial SIR and decides, in line with the SI-Catalogue, if the incident should be further processed as a SIR. In case the incident is not processed as a SIR, the information shall nonetheless be made available immediately to the respective operational team and in case of alleged violations of Fundamental Rights or Frontex Code of Conduct, additionally to the FRO and/or PRU for the further handling.
- The SDO distributes the initial SIR without delay to the Senior Management, and to other Frontex stakeholders, if needed.

7.5.2. Formal SIR

- Frontex actors in the field (FSO, FOC, FCO, etc.) under the coordination of the respective Operational Manager (OM) and in close cooperation with the host authorities or the central operational structures of the host MS in close cooperation with the Frontex actor, are obliged to further monitor the situation and subsequently provide a formal SIR, as soon as possible, and maximum within 48 hours, to FSC.
- For the formal SIR the JORA SIR template is compulsory (example of the template is provided in the chapter 11.1 of this document). The formal SIR should be reported via JORA and email to FSC SDO service, apart from the exceptional reporting according to Chapter Error! Reference source not found..
- The formal SIR should contain a comprehensive overview of the information available, according to Chapter 7.4 (Content of a SIR) and should include possible developments and proposals for the decision making process (if applicable).
- The FSC SDO processes the information received and sends the formal SIR without delay to the Senior Management and to other respective Frontex stakeholders, if applicable.
- In case more information is needed, the FSC SDO shall request that information, in close cooperation with the responsible OM by contacting the appropriate interlocutor (FSO, FOC, etc.) in the operational area.

7.5.3. Updated SIR

- If at a later stage, an actor involved in Frontex activities (involved in or witnessing a particular SI), acquires substantial information, an updated SIR should be provided to FSC, reporting the new information gathered.
- FSC SDO monitors the situation and updates the Frontex Senior Management and relevant stakeholders, if new developments or information are obtained.

7.5.4. Final SIR

- Final SIR is obligatory only if such report is requested by FSC.
- The final SIR shall summarize the main outcome and indicate the closure of the SI.

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

In case of sensitive SI involving allegations on violation of FR, the reporting is a subject to a specific extraordinary procedure as described below.

7.6.1. Reporting mechanism

In case a participant in Frontex activities, witnesses, is involved or has grounds to suspect the occurrence of an incident representing a possible violation of fundamental rights or international protection obligations (category 4 of the SI-catalogue), he/she is obliged to report this case immediately to Frontex using following options:

- Use of the SIR mechanism following the SIR procedure (Chapter Error! Reference source not found.).
- Use of an exceptional reporting via other reporting channels (e.g. personal reporting, shift-, operational-, debriefing reports).

In case the reporting actor has concerns that the disclosure of such sensitive information on alleged violation of fundamental rights via the SIR mechanism could have consequences on his/her or others integrity, reputation or deployment he can make use of the exceptional reporting. After acknowledgement of such information, the OM/FSO/FOC/FCO shall immediately report such incidents to FSC.

7.7. Frontex internal follow up procedure / SIR-Coordinator

Due to the possible dimension and further circumstances of a SI a Frontex internal follow up on the incident may be proposed after SDO's assessment. Therefore, a Frontex internal SIR-coordinator should be proposed by FSC SDO in order to take up the responsibility for further follow up measures related to the respective incident.

7.8. 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 some Land 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 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.

7.9. Public access

SIR can be subject to the public disclosure pursuant to the provisions of the Regulation (EC) No 1049/2001 of 30 May 2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents and the procedure defined by the Frontex Management Board Decision No 3/2014 of 19 February 2014 adopting practical arrangements regarding public access to the documents of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex).

7.10. Serious Incident Catalogue

7.10.1. 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 MS⁶ 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

⁶ Leading to a change on the level of border control. (e.g. introduction of specific border control means, 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 Home) 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:
 - Right to life
 - Right to the integrity of the person
 - Prohibition of torture and inhuman or degrading treatment or punishment
 - Right to liberty and security
 - Right to asylum
 - Principle of non-refoulement and protection in the event of removal, expulsion or extradition
 - Non-discrimination

- o Right to an effective remedy
- o 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.
- o Other international protection obligations
- o Imminent danger

7.11. Serious Incident Reporting Mechanism

Serious INCIDENT REPORTING MECHANISM

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)(a) of Regulation No 1049/2001 relating to the protection of the public interest as regards public security.

7.12. 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
- 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
- Personal data**
- Private life:**
 - Personal and bodily integrity
- Property:**
 - Deprivation of property
- Refoulement:**
 - 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):**
 -
 -
 -
 -
 -

8. ARRANGEMENTS OF DEPLOYED RESOURCES

8.1. Operational Resources Management System (Opera)

<https://fis.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 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.

8.1.1. Responsibilities

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

Frontex responsibilities:

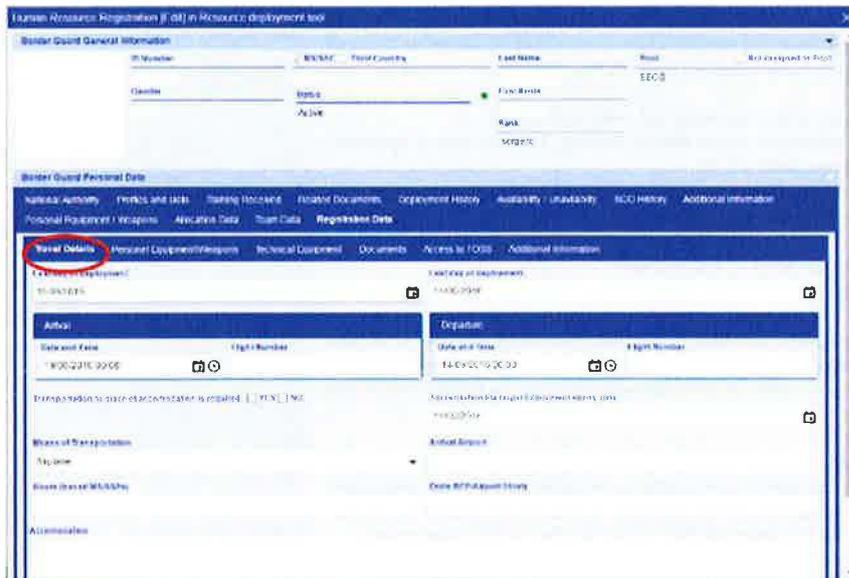
- To create a given operation;
- To create the requests for HR and TE and to send the requests to the MS;
- To allocate the HR made available by MS to the teams, and to confirm the TE made available by MS to the Operation;
- To confirm the HR deployed in the teams, and, after the registration is completed 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).

Member States 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.

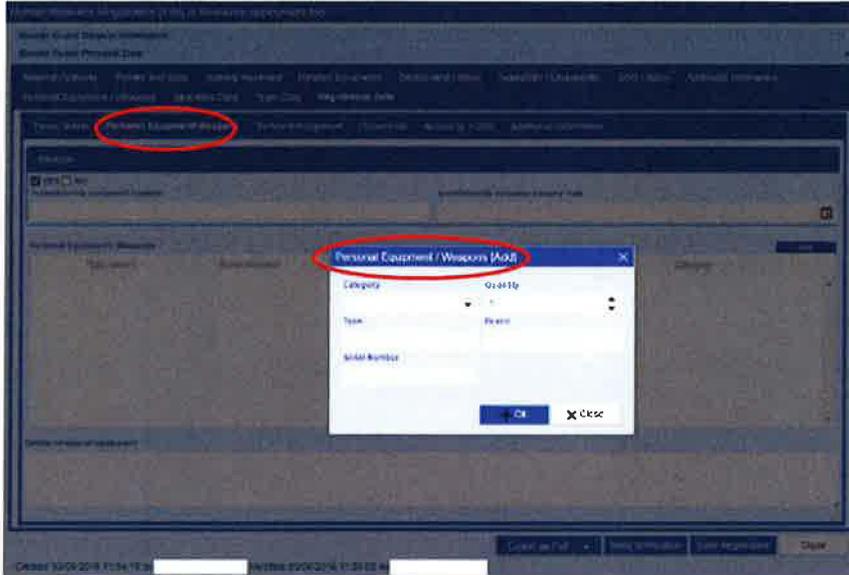
8.1.2. Registration of Human Resources

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:

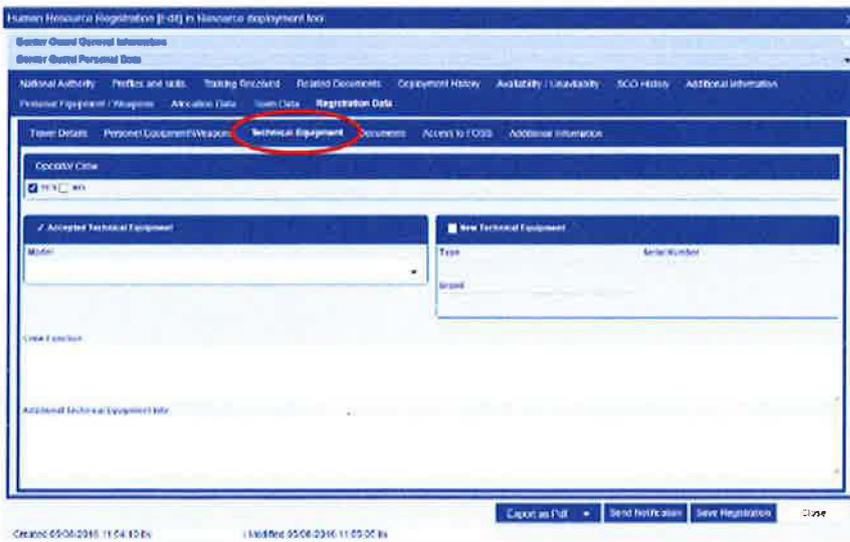


Under "Travel Details", MS input information concerning the arrival and departure dates (including indication of approximate time of arrival), Flight details if travelling by airplane, Mean of Transportation, Route, Arrival Airport, Entry BCP/Airport and Accommodation. In the event of Accommodation being 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".

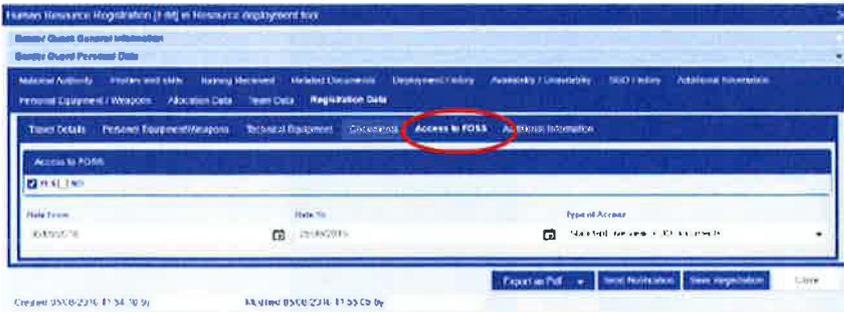
The Expiry date of the Accreditation/Participant Document is automatically set as the date of departure from the operational area. In the event of any particular need (e.g. transportation by car, etc.) MS can manually extend the date in order to have the Accreditation/Participant Document valid until the arrival of the officer in his/her MS.



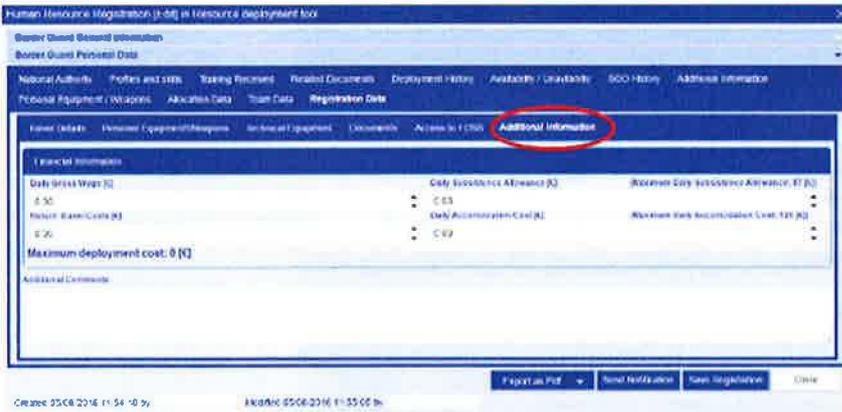
Under "Personal Equipment/Weapons", MS indicate if the officer is travelling to the operational area carrying weapons or not. If yes, MSs also register the weapon and indicate the amount and type of ammunition to be carried. This field is mandatory.



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 4.



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.

Technical Equipment Registration (Edit) in Resource deployment tool

Technical Equipment General Information

MS/SAC Third Country

Brand / Make / Breed:

Deployment Time (in days): 0 Response Time (in days): 20

Model / Name:

Ownership Type: Owner

MsSacOwne:

Serial / Registration / Chip / Tattoo Number:

Type of registration: Civil Status: Active

Standard Description Category:

Standard Description:

Quantity: 1

Purchased with EU co-finance

Fr Notes / Additional Information:

MS/SAC Notes / Additional Information:

Operational Areas Related Documents Deployment History Availability / Unavailability Specification National Authority

OMNTE Additional Requirements Allocation Data **Registration Data**

Quantity	Deployed From	Deployed To	Total Estimated Deployment Cost (€)	Host Country
1	<input type="text"/>	<input type="text"/>	REM	<input type="text"/>

Deployment Locations: TBD

MS/SAC Notes:

Frontex Notes:

Save Registration Close

8.2. Technical equipment deployed by Member States

Technical equipment deployed by the MS in the operational areas to foster the border control activities may Helicopters, Fixed Wing Airplanes (FWA), Thermo Vision Vehicles (TVV), 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 (OMNTE) or can be considered as additional technical equipment (beyond OMNTE). The OMNTE 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 OMNTE, in case that any operational needs occur.

8.3. Management of the operational assets⁷ 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 members of the teams / 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.

⁷ 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.

8.3.1. Firearms and ammunitions transportation

The aim of this practical note is to draw your 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 sending Member State, 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:

- o 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)
- o 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
- o 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
- o Firearms must be packed separately from ammunition
- o Firearms and ammunition are mostly transported in the cargo compartment of the airplanes, as care by captain procedures are less and less used nowadays
- o Ammunition must be securely boxed, 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
- o The firearm must be packed in a hard-sided container
- o 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
- o 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
- o 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)
- o 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
 - o 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 packaged.



- 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 NFPOC) of transiting Member State(s) prior to the travel in order to receive transit permission if such is required.

The Host MS NFPOC 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 by registering the complete details in Opera platform. In case of registering the officers in Opera, 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.

In case of Greece:

The weapon permits are issued by the competent authorities and received at the points of entry or, in exceptional cases, at the places of deployment (last minute information, etc.). Therefore, the Hellenic NFPoC must be informed at least 5 days before deployment, about the above mentioned details, as well as whether the officers will carry weapons while entering Greece. The above mentioned information is also required in cases of replacement of officers and in these cases the weapon permits are received at the places of deployment and not at the entry points.

Especially in arrival at Athens Airport and following disembarkation from the aircraft, the Members of the Teams will address to the Police Lost and Found office located on the ground floor of the arrivals hall, which is located opposite to the baggage claim area (belt n. 5) and can also be reached on tel: (+30)2103530515. This office will have all weapon permits and will hand them over to the Members of the Teams upon request, on a 24/7 basis.

During departure, the Members of the Teams will have to return this document to the Duty Officer, responsible for extra Schengen Departure, located left to counter n. 54 of the Departure Area (1ST floor) and before the Extra Schengen Area. The telephone of this office is (0030)2103531052.

In case of a need, please contact directly the Hellenic Police headquarters: [REDACTED]

Commented [A12]: The non-disclosed text contains personal data, in particular the name of an individual. Its disclosure would affect the privacy and integrity of the individual and is therefore precluded pursuant to the exception laid down in Article 4(1)(b) of Regulation (EC) No 1049/2001.

8.4. Clearance request form for VFR flights at night

1.	Operator	
2.	Type of aircraft (Alternative A/C)	
3.	Radio Call Sign(s), Registration number	
4.	Purpose of flight	
5.	Diplomatic clearance number	
6.	Pilot in command's surname and rank, number of crew members	
7.	Airport of origin - Last airport before HELLAS/ ETD (UTC) (ICAO aerodrome designator should be added)	
8.	Point of entry into FIR/ date, time (UTC)	
9.	Hellenic airport for landing and ETA (UTC)	
10.	Fuel (Other services requested)	
11.	Date, ETD (UTC) from Hellenic airport	
12.	Route within FIR	
13.	Point of exit from FIR/ date, time (UTC)	
14.	Destination aerodrome and ETA (ICAO aerodrome designator should be added)	
15.	Type, quantity and weight of dangerous goods/ munitions arms (Use UN classification system)	
16.	Fixed armaments, optical, reconnaissance or electric warfare equipment	
17.	Remarks	

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

9. PROCESSING PERSONAL DATA FOR RISK ANALYSIS (PeDRA) PILOT EXERCISE FOR DEBRIEFING ACTIVITIES

9.1. Aims, objectives and description

PeDRA facilitates the collection of information containing 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 enable Frontex, Member States and recipient agencies (currently Europol) to more effectively carry out their respective mandates in the fields of border management and cross-border crime.

A Pilot exercise was first launched in EPN Triton in February 2016 and successfully met all its objectives, most notably the transmission to Europol of the identities, locations, phone numbers and Facebook profiles of several hundred suspects of people smuggling, operating mostly in Libya. Following on from this success, the Pilot Exercise was subsequently also launched in Joint Operations Indalo, Hera, Minerva and Poseidon 2016 aiming to test data-capture templates, reporting protocols from the operational area and the transmission of personal data to Frontex. Correspondingly there were at the time also several new activities in Frontex aimed at processing the information and personal data to produce risk analyses, and also cases for daily transmissions to Europol.

During 2017 PeDRA is foreseen to be launched in all Joint Operations where Joint Debriefing teams are deployed, allowing for a fully European approach to processing information containing personal data collected at the external borders.

9.2. Legal basis

According to Article 47 of the Frontex Regulation (2016/1624), Frontex may further process personal data collected by Member States or by its own staff during Joint Operations, Pilot Projects and Rapid Interventions.

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

Procedures for processing personal data are set out in Frontex Management Board Decision No 58/2015

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 2015⁸.

9.3. Scope of personal data

- Frontex can only process personal data collected by Member States or by its own staff 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 Member States, of involvement in facilitation of illegal migration, human trafficking, terrorism or other cross-border crimes
- The processing of such personal data shall respect the principles of necessity and proportionality
- Under PeDRA personal data shall only be processed by Frontex for:
 - the transmission of personal data to Europol, and back to host Member States
 - the production of risk analyses, the results of which will be depersonalised
- Personal data will be deleted in Frontex after 90 days

⁸ Agreement on Operational Cooperation between the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union ("FRONTEx") and the European Police Office ("EUROPOL") <http://soo.slx.euauth>

9.4. Interoperability

PeDRA represents a modernised approach to the reporting of information containing personal data collected during debriefing activities. To this end, a new and modernized debriefing template specifically designed to capture personal data is deployed during PeDRA. Access to the on-line template is via the Joint Operations Reporting Application (JORA), to which all Debriefers, Team Leaders and Intelligence Officers will need daily access throughout their deployment.

To maintain data security during the PeDRA Pilot Exercise it is no longer possible for Member State representatives to e-mail debriefing templates to Frontex because they are expected to contain personal data and this would be a breach of the security provisions in the data protection regulation.

9.5. Stakeholders

The PeDRA currently only affects officers involved in debriefing activities, and those tasked with the transmission of debriefing templates to Frontex: debriefers, team leaders, and Intelligence Officers.

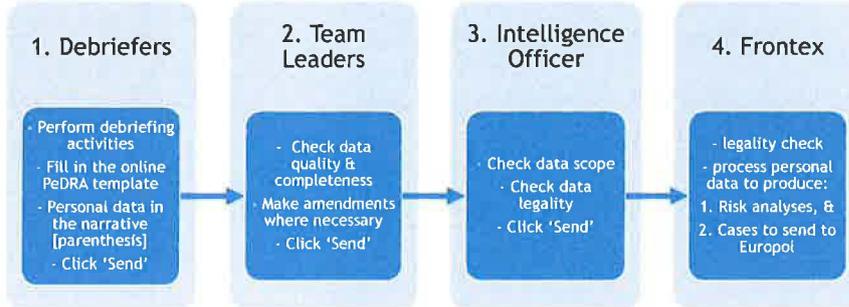
9.6. Roles and responsibilities

- **Debriefing experts** - the work of the debriefing experts' changes very little compared to previous Joint Operations. However under PeDRA, debriefing experts first need to gain access to JORA, and once in JORA they need to gain access to the more secure area for accessing interview templates. After logging in to JORA, debriefing experts can start to fill in the online templates.

All personal data entered into the template should be in the narrative field and should be within [square parentheses]. For example 'The migrant met the facilitator [Muhammad al-Jameel] at the café on George Street'. Once the template has been filled in the debriefer should click on the 'send' button so that the template becomes visible to the local team leader(s).

- **Team leaders** access templates completed by debriefers and inspect them for data quality and completeness, giving feedback where necessary. Then team leaders should then click the 'send' button so that the template becomes visible to the Intelligence Officer(s).
- **The Intelligence Officer** access templates validated by the Team Leaders, and should scrutinise them to ensure that personal data relate to suspects rather than migrants. The Intelligence Officer is then required to export the templates for local storage and then send the templates to Frontex by pressing the 'Send' button.
- **Frontex** receives templates in JORA, where they are first scrutinized for the legality of the personal data. Personal data will then be obscured, and sanitised (depersonalised) versions of templates will be made available to operational analysts in RAU and project managers in JOU who need to read about modus operandi but are not authorised to access personal data. The PeDRA team will then process information containing personal data to produce the two outputs: risk analyses, and cases for onward transmission to Europol.

9.7. Work flow and responsibilities under the PeDRA Pilot Exercise



Actors	Role
Debriefers	Gain access to JORA, and then the PeDRA area of JORA Regular debriefing activities but ask more questions to obtain personal data relating to facilitators and traffickers. Complete the online template in which all personal data should be placed in narrative field within [square parentheses] and photos/maps uploaded.
Team leaders	Check for completeness and quality - give feedback where necessary. No need to obscure personal data. Templates should no longer be sent by e-mail in the daily package.
Intelligence Officers	Check legality of personal data in the narrative field. Ensure that personal data are within [square parentheses]. Export template and save locally. Send template to Frontex. Respond to enquiries from Frontex regarding the legality of the personal data. National access management for access to the templates.
Frontex FSC	Receive uploaded template. Extract data from accepted templates into a PeDRA database. Obscure personal data in JORA for non-authorized users in RAU and JOU.
Frontex RAU	Perform legality check on personal data - contact IO for more information if necessary. Normalise and structure personal data into analytical system. Produce products based on personal data.

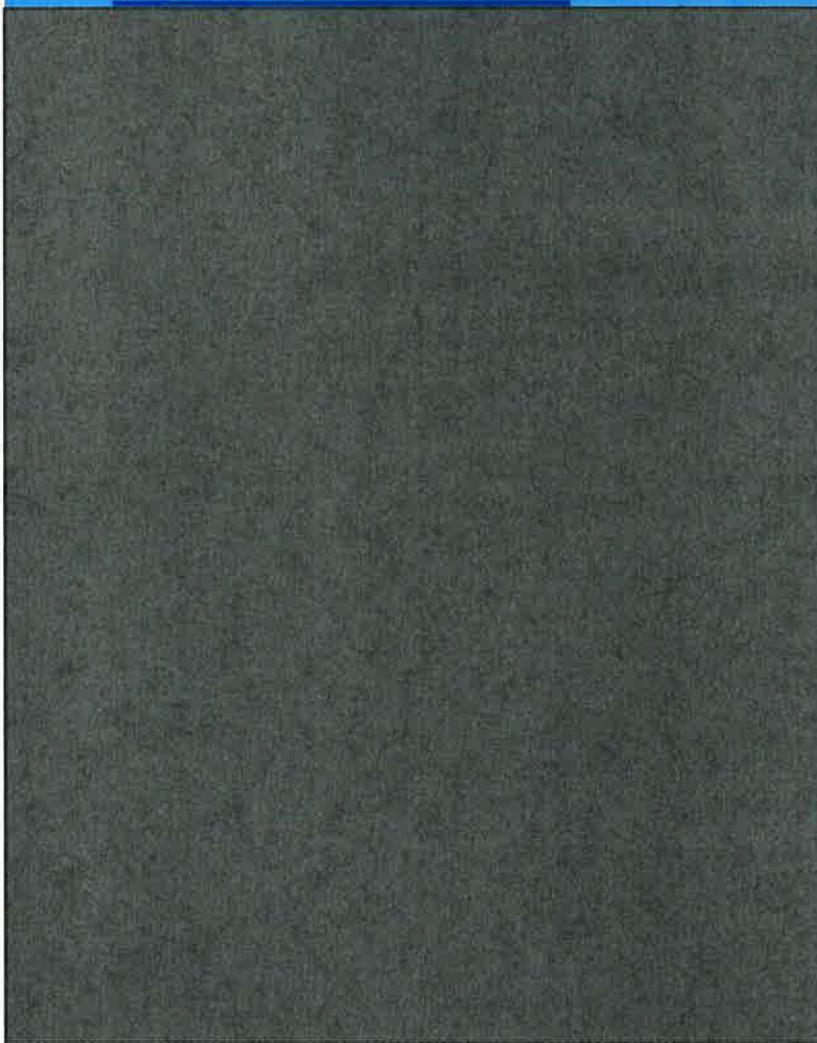
9.8. What is personal data?

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.

9.9. Access requests



INTERVIEW ACCESS REQUEST



Commented [A13]: 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.

10. OTHER FRONTEX PRODUCTS AND SERVICES

10.1. Eurosur Fusion Services

10.1.1. 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.

10.1.2. Other Services

Aligned with operational needs, these and other services are available via the EUROSUR Application and the JORA 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/>

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

For more information, please contact: [REDACTED]

10.2. 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 areas and they can thus contribute to detecting cross-border crime and irregular migration. 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 Multipurpose 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/LBS and CBD/RDU.

Commented [A14]: The non-disclosed text contains information on the means of communication used by law enforcement officers within the operation. Its disclosure could lead to possible abusive usage with a view to jeopardize their work and harm the course of future and ongoing operations, ultimately obstructing their purpose to counter and prevent cross-border crime as well as prevent unauthorized border crossings. 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.

11. 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.

11.1. Serious Incident Report Template

Serious Incident Report no.

Reporting date:

Reporting person:

FSC SIR Category	
Subject	
Type of SIR	
JORA Incident number (if any)	
Joint Operation	
Frontex SIR Coordinator	
Incident date/time	
Detection date/time	
Original source of the information	
Location of the incident	
Is latitude unknown	
Latitude	
Is longitude unknown	
Longitude	
Reference to the operational area	
Frontex resources involved (Human resources / co-financed technical equipment)	
Type of resources / involvement	
Dead persons	
Injured persons	
Missing persons	
Fact of the case	

Measures
Assessment

11.2. Technical Equipment Mission Report

Patrolling asset

Mission Number

Date

Responsible ICC/LCC

Operational Area

National Official

Asset location (airport, port)

Member State

Authority

Mission Data Sheet

Patrolling asset

Registration/Call Sign

Commanding Officer

Communication means (e.g. SAT, HF, VHF, GSM, etc)

Mission scheduled

total hrs:

Mission executed

total hrs:

Brief description in case of deviation

Engine(s) start up:

Engine(s) cut off:

Take off/off berth:

Landing/on berth:

On station (ops area):

Off station:

Total committed hours according to the SFD

(hrs:min):

Total executed hours so far

(hrs:min):

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 the operational area and vice versa applies the same

Do not delete, filter or 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

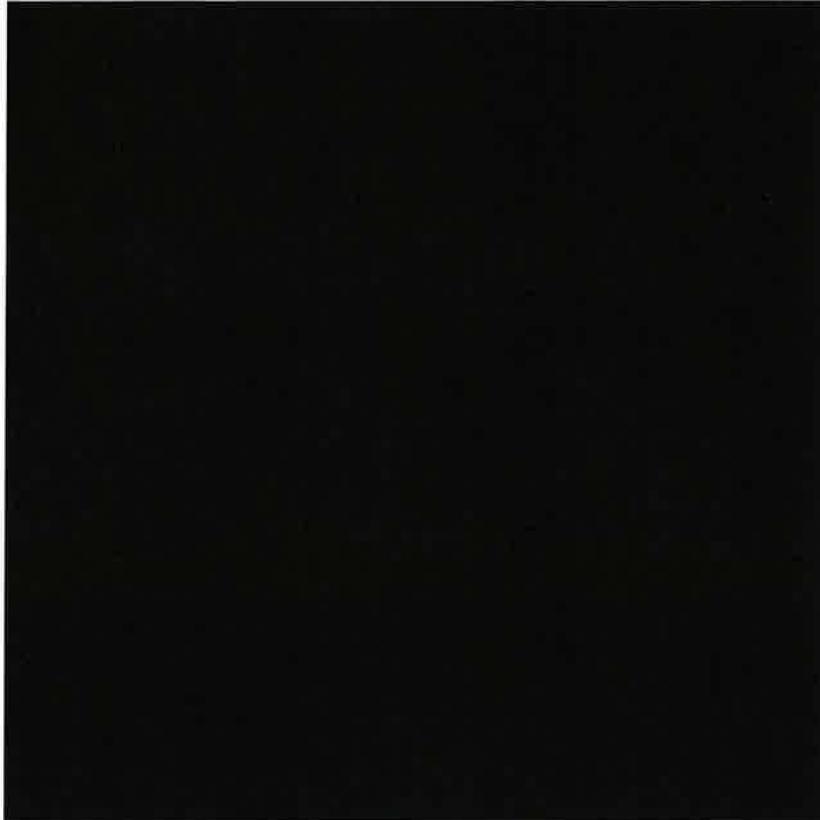
Minimum information to be provided regarding the protection of human rights of the persons taken on board and to be disembarked in TC:

Persons disembarked : <input type="checkbox"/> number <input type="checkbox"/> gender (if possible) <input type="checkbox"/> age (if possible) <input type="checkbox"/> nationalities (if possible)	
Medical care provided/ Medical staff on board (Y/N)	

Language used for communication on board	
Place of disembarkation indicated (e.g., pointed out on a map, etc)	
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	
Persons taken on board had an opportunity to consult the Legal advisor	

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.

11.3. PeDRA Interview Template



Commented [A15]: 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.

11.4. Document Alert Template

Place, date

Immigration authority Name	National immigration authority LOGO	National Flag
-------------------------------	-------------------------------------------	---------------

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:

11.5. User Access Request Form - FOSS

Request for - Please Specify: Select Option

First Name				
Last Name (CAPITAL LETTERS)				
Email				
Member State/Country/Organisation				
Job Title/Position				
Date and User Signature				
User Group(s) ⁹	Activity	Specify Duration of FOSS Access		
		<u>Please specify duration</u>	If OTHER:	
			Start date	End date
Only Basic Access (Library; Help; Contacts; Media Monitoring) ¹⁰	<input type="checkbox"/>	Select Option		
National Authorities (Overview of all related activities)	Air Border Sector (ABS) Please specify Joint Operation or Project	Select Option		
	Land Border Sector (LBS) Please specify Joint Operation or Project	Select Option		
	Return Operations Sector (ROS) Please specify Joint Operation or Project	Select Option		
	Sea Border Sector (SBS) Please specify Joint Operation or Project	Select Option		
	Please specify any other activity:	Select Option		
Other activities/ projects and related content	Other Sections Please specify Section or Activity	Select Option		
	Please specify any additional activity or specific page on FOSS:	Select Option		
National Frontex Point of Contact (NFPOC) ¹¹	<input type="checkbox"/>	Select Option		
Justify the need of access ¹²				

⁹ Choose the relevant user group for viewing the information on FOSS.

¹⁰ Please note that if any other user group is selected and approved, access to these general FOSS sections is granted by default.

¹¹ This group has access to the majority of FOSS content, excluding a few sections such as some pages related to the EURINT project. For full access to EURINT please select it under the ROS section.

¹² Provide a short justification on what is your need to have access and what are the activities you are involved in.

Validation/ Sign-off	Date	Signature
<i>FOSS National User Coordinator</i> ¹³		
<i>FOSS Area of Interest Owner</i>		

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 concern can be addressed to the FOSS User Administrator or the Frontex Data Protection Officer.

¹³ To be completed only for requests submitted from MS/SAC/Third Country National Authorities. Please provide a legible name and surname of FOSS National User Coordinator and a signature. If this is not feasible, an e-mail may also be accepted if sent from the approved e-mail account of the FOSS National User Coordinator, and with personalized e-mail signature included.

11.6. Intelligence Officer Report

INTELLIGENCE OFFICER DAILY REPORT

Ref. No:	Click here to enter text.			
Date:	Click here to enter a date.			
Period covered:	FROM	Click here to enter a date.	TO	Click here to enter a date.
Joint Operation:	Choose an item.			
Intelligence Officer:	Click here to enter text.			

A. INTELLIGENCE

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. JDTs
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

Media and Open Sources
Flash news

11.7. FSO Daily / Flash Report¹⁴

Name of the joint operation _____

Number of the Report _____

Date of reporting _____

Reporting period _____

Reported from _____

1. Incidents¹⁵

Description per incident

2. Deployed Resources

Type of resource	MS	Authority	Period of deployment	Names

3. LCC Meeting & Participants

3.1. Participants

Name	Role

3.2. Outcome of the meeting

Issues discussed	Outcome, decisions taken

4. Additional Information

Other operational, logistical, practical issues

¹⁴ Delete which is not applicable

¹⁵ Flash Report contains only chapter 1

11.8. 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 xxxxxxxxx@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.

Data about deployment

Name of the joint operation

Name of the participant

Member State / Authority

Period of deployment

Location of deployment

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 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 have a power what would you change in this JO in order to achieve bigger added value for EU?

To be filled in by the participant

9. Have you participated in any of the specific EBGT Profile training (Screening, Debriefing experts, Advanced-Level Document Officer training, etc) organized by 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

11.9. 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 xxxxx@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.

Data about deployment

Name of the joint operation

Member State

Authority

Period of deployment

Location of deployment

1. Coordination and cooperation

Assessment of the coordination structure established during the JO: performance of Frontex (FX) and the hosting MS (ICC/LCC, Focal Points, Police Stations, Detention Centers, BCPs, etc)

*Level of cooperation between FX, host and home MS during the JO
Interagency cooperation (EASO, Europol, etc)*

To be filled in by MS

2. Information flow

Assessment of the information flow between all actors involved in the JO (FX/ICC/IO/experts/assets/NO/MS/FX feedback to the MS about ongoing JO and etc)

JORA, FOSS 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

To be filled in by MS

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*

To be filled in by MS

5. Practical arrangements and logistics

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

To be filled in by MS

6. Additional information

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

To be filled in by MS

7. Recommendations

From MS point of view

To be filled in by MS

11.10. Final Report from Third Country

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.

Data about deployment

Name of the joint operation

Third Country

Authority

Period of deployment

Location of deployment

Observations

To be filled in Third Country (free text)

11.11. 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 ([REDACTED]).

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.

Name of the JORA user	
Frontex Unit / Sector	(if applicable)
Members State	
Duty station	
¹⁶Name of the operation	
¹⁷User role (in JORA)	Frontex Access Manager <input type="checkbox"/> Frontex Template Creator <input type="checkbox"/> National Access manager <input type="checkbox"/> BCP/BCU Incident reporter <input type="checkbox"/> LCC incident verifier <input type="checkbox"/> ICC incident verifier <input type="checkbox"/> FSC incident approver <input type="checkbox"/> No specific role in the system <input type="checkbox"/>

Commented [A16]: The non-disclosed text contains information on the means of communication used by law enforcement officers within the operation. Its disclosure could lead to possible abusive usage with a view to jeopardize their work and harm the course of future and ongoing operations, ultimately obstructing their purpose to counter and prevent cross-border crime as well as prevent unauthorized border crossings. 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.

Reported Issue			
Login problem <input type="checkbox"/>	¹⁸ Error message <input type="checkbox"/>	Attribute ¹⁹ <input type="checkbox"/>	Drop-down list <input type="checkbox"/>
Data Input <input type="checkbox"/>	Validation Process <input type="checkbox"/>	Data Modification <input type="checkbox"/>	Data Loss <input type="checkbox"/>
Export Function <input type="checkbox"/>	Attachments <input type="checkbox"/>	Dashboard <input type="checkbox"/>	Development <input type="checkbox"/>
User Friendliness <input type="checkbox"/>	Other <input type="checkbox"/>		

[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].

¹⁶ As defined in the JORA system

¹⁷ Please mark the box according to your role

¹⁸ If an error message appears in JORA, please save the log and send it as an attachment.

¹⁹ 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).

ADDITIONAL INFORMATION / REMARKS:

Document checks:

Advanced-Level Document Of
 Advanced-Level Document Of
 Advanced-Level Document Of

Documents checked/issued by	Forged documents
Total:	

ADDITIONAL INFORMATION / REMARKS:

12. ACRONYMS

Abbreviation	Spelling
B	
BCP	Border Crossing Point
BCU	Border Crossing Unit
C	
CFPOC	Central Frontex Point of Contact
CO	Commanding Officer
CPB	Coastal Patrol Boat
CPV	Coastal Patrol Vessel
D	
DSR	Daily Situation Report
E	
EASO	European Asylum Support Office
EBCGT	European Border and Coast Guard Teams
EU	European Union
EUROSUR	European External Border Surveillance System
EFS	Eurosur Fusion Service
F	
FAM	Frontex Access Manager
FASS	Frontex Aerial Surveillance Services
FCO	Frontex Coordinating Officer
FER	Frontex Evaluation Report
FOC	Frontex Operational Coordinator
FOSS	Frontex-One-Stop-Shop
FP	Focal Point

FSC	Frontex Situation Centre
FSO	Frontex Support Officer
FRO	Fundamental Rights Officer
Frontex	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
FWA	Fixed Wing Airplane
G	
GIS	Geographic Information System
GSM	Global System for Mobile Communications
H	
HF	High frequency
HQ	Headquarters
HR	Human Resources
I	
IBM	Integrated Border Management
ICC	International Coordination Centre
ICT	Information and Communications Technology
IO	Intelligence Officer
J	
JCB	Joint Coordinating Board
JDT	Joint Debriefing Team
JO	Joint Operation
JORA	Joint Operations Reporting Application
JOU	Joint Operations Unit
JRCC	Joint Rescue Coordination Centre
JRO	Joint Return Operation
L	

LCC	Local Coordination Centre
LO	Liaison Officer
LO Piraeus	Liaison Office (Piraeus)
LO-TE	Liaison Officer - Technical Equipment
M	
MRCC	Maritime Rescue Coordination Centre
MRSC	Maritime Rescue Sub-Centre
MS	Member State
N	
NAM	National Access Manager
NCC	National Coordination Centre
NPC	National Point of Contact
NO	National Official
O	
OA	Operational Analyst
OM	Operational Manager
Opera	Operational Resources Management System
OPLAN	Operational Plan
OPV	Offshore Patrol Vessel
OT	Operational Team
P	
PeDRA	Personal Data for Risk Analysis
POB	People on board
PRU	Pooled Resources Unit
R	
RAU	Risk Analysis Unit
RCC	Regional Coordination Centre

RDU	Research and Development Unit
RoE	Rules of Engagement
S	
SAC	Schengen Associated Countries
SAR	Search and Rescue
SBS	Sea Borders Sector
SDO	Senior Duty Officer
SI	Serious Incident
SIR	Serious Incident Report
T	
TE	Technical Equipment
TL	Team Leader
TRU	Training Unit
TVV	Term Vision Vehicle
V	
VHF	Very high frequency
W	
WAR	Weekly Analytical Report
WAU	Weekly Analytical Update