

## Decision of the Executive Director

No R-ED-2021-51

### Standard Operating Procedure (SOP) - Serious Incident Reporting

of 19/04/2021

#### THE EXECUTIVE DIRECTOR,

Having regard to the European Border and Coast Guard Regulation<sup>1</sup> (hereinafter “the Regulation”), and in particular Article 106(4) thereof,

Whereas:

- (1) Pursuant to Article 38(3) of the Regulation, the operational plan shall cover all aspects considered necessary for carrying out the joint operation, including in accordance with point (j), detailed provisions on immediate incident reporting by the Agency to the Management Board and to relevant national authorities;
- (2) Pursuant to Article 46(6) of the Regulation regarding the decisions to suspend, terminate or not launch activities, the Executive Director shall take into account relevant information such as reports of serious incidents for decisions referred to in Article 46(4) and (5) of the Regulation;
- (3) Article 5(1)(a) of the Data Protection Regulation<sup>2</sup> in conjunction with Article 87(1)(h) of the Regulation and Article 38(3)(h) of the Regulation provides for the legal basis for processing of personal data in the course of implementation of this reporting mechanism. An effective internal procedure enables a comprehensive and timely response to any serious incident reported within the framework of the activities of the Agency;
- (4) The Standard Operating Procedure (SOP) for Serious Incident Reporting is part of a broader framework regulating the reporting obligations of participants in the activities of the Agency;
- (5) The SOP for Serious Incident Reporting defines the respective steps to be followed for the reporting of serious incidents;
- (6) The SOP for Serious Incident Reporting defines the roles and responsibilities of individual actors concerned in the reporting of serious incidents.

---

<sup>1</sup> Regulation (EU) 2019/1896 of 13 November 2019 on the European Border and Coast Guard (OJ L 295, 14.11.2019, p. 1).

<sup>2</sup> Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39-98).

## HAS DECIDED AS FOLLOWS:

### *Article 1* **Adoption**

Standard Operating Procedure (SOP) - Serious Incident Reporting, as set out in the Annex to this Decision, is hereby adopted.

### *Article 2* **Repeal**

This Decision repeals and replaces the Decision of the Executive Director No 2014/55 of 28 July 2014 on the adoption of the Frontex Standard Operating Procedure on Serious Incident Reporting.

### *Article 3* **Entry into force**

This Decision enters into force on the day following its signature. It shall be applicable from the moment in which all relevant Operational Plans are amended accordingly with the agreement of host Member States and Third Countries.

Done in Warsaw, on 19/04/2021

Fabrice Leggeri  
Executive Director

**Annex:** Standard Operating Procedure (SOP) - Serious Incident Reporting

ANNEX:

# Standard Operating Procedure

**Serious Incident Reporting**

## Contents

<b>1. Introduction</b>	<b>3</b>
<b>2. Definitions</b>	<b>4</b>
2.1. Serious Incident (SI)	4
2.2. Categories of SIs	4
2.3. Serious Incident Report (SIR)	4
<b>3. Roles and Responsibilities</b>	<b>5</b>
3.1. Participants in Frontex activities	5
3.2. Fundamental Rights Monitors (FROMs)	5
3.3. Coordinating staff in Frontex activities	6
3.4. Frontex Situation Centre (FSC)	6
3.5. Fundamental Rights Officer (FRO)	6
3.6. SI-Handler	7
3.7. Senior / Executive Management	8
<b>4. The procedure</b>	<b>8</b>
4.1. General provisions	8
4.2. Steps of reporting serious incidents	9
4.2.1. Initial Information	9
4.2.2. Validation - Assessment - Distribution	9
4.2.3. Final Report	10
4.3. Exceptional reporting - Link to whistleblowing procedure	10
4.4. Reports provided to the FRO by third parties or other sources	11
4.5. Escalation procedure	11
4.6. Link to Crisis Management	11
4.7. Logbook / Storage	11
4.8. Personal Data	11
4.9. Public access to documents	13
<b>List of annexes:</b>	<b>13</b>
<b>ANNEX 1 - Serious Incident Catalogue</b>	<b>14</b>
<b>ANNEX 2 - Serious Incident Reporting Standard Workflow</b>	<b>15</b>
<b>ANNEX 3 - Report Template</b>	<b>16</b>
<b>ANNEX 4 - Distribution of Serious Incident Reports</b>	<b>18</b>
<b>ANNEX 5 - Final SI-Handler Report Template</b>	<b>19</b>
<b>ANNEX 6 - List of potential Fundamental Rights violations within Frontex activities</b>	<b>20</b>
<b>ANNEX 7 - Relevant legal acts and other documents</b>	<b>21</b>

## 1. Introduction

This document defines the procedure to be followed within the European Border and Coast Guard Agency (hereinafter “Frontex”), for the reporting of serious incidents (SIs), in accordance with the European Border and Coast Guard Regulation<sup>1</sup> (hereinafter “the Regulation”). Given the importance of the incidents reported, as well as the urgency to take immediate action within Frontex, it is crucial that participants in Frontex activities are acquainted with the procedural steps set up in this document, and understand the significant impact that Serious Incident Reports (SIRs) could have on Frontex activities, Frontex’s responsibilities, tasks, the possible effect on Frontex professional standards and Fundamental Rights obligations.

*In line with the Frontex Fundamental Rights Strategy<sup>2</sup>, “Participants in the activities of the Agency are accountable for breaches of their professional conduct rules and are responsible for promoting, respecting, upholding and protecting Fundamental Rights in the context of their participation in a Frontex operational activity, including reporting related to infringements of Fundamental Rights. Any participant in the Agency’s operational activities who has reason to believe that a violation of Fundamental Rights has occurred is required to report it to the Agency via the established reporting channels, such as the Frontex serious incident report system. The Code of Conduct and the Standard Operating Procedure of the Serious Incident Report oblige all participants in the Agency’s operational activities to report any potential violation of Fundamental Rights through a Serious Incident Report (SIR).”*

This procedure is distinct from the reporting under the Supervisory Mechanism (Management Board Decision 7/2021<sup>3</sup>). The Standard Operating Procedure (SOP) on Use of force and Incidents involving the use of force reporting (UFR / IFR)<sup>4</sup> and the Standard Operating Procedure (SOP) on Serious Incident Reporting are reporting mechanisms on incidents that are without prejudice to one another. However, in order to avoid double reporting, incidents involving the use of force identified following the individual reporting obligations set out in SOP UFR/IFR shall be reported and managed according to its provisions.

Alleged Fundamental Rights violations are to be considered Serious Incidents and reported in line with the SOP on SIR unless they involve the use of force by the Standing Corps officers; in which case it is to be reported in line with SOP UFR/IFR.

Should the FSC receive, within the reporting timelines set out in the SOP UFR/IFR, in parallel a SIR and an IFR relating to the same incident, the follow-up procedure described in the SOP UFR/IFR shall take precedence.

The SIR procedure should be applied in accordance with the framework of the applicable mechanisms and relevant legal acts and other documents as set out in Annex 7.

---

<sup>1</sup> Regulation (EU) 2019/1896 of 13 November 2019 on the European Border and Coast Guard (OJ L 295, 14.11.2019, p. 1).

<sup>2</sup> Management Board Decision 12/2021 of 14 February 2021 adopting the Fundamental Rights Strategy.

<sup>3</sup> Management Board Decision 7/2021 of 20 January 2021 establishing a supervisory mechanism to monitor the application of the provisions on the use of force by statutory staff of the European Border and Coast Guard Standing Corps.

<sup>4</sup> Executive Director Decision No R-ED-2021-38 of 6 March 2021 on Standard Operating Procedure (SOP) - Use of force and incidents involving the use of force reporting (UFR / IFR).

## 2. Definitions

### 2.1. Serious Incident (SI)

A Serious Incident (SI) is an event, caused by an action or failure to act by a person, or by force of nature, which directly or indirectly<sup>5</sup> involves Frontex participants<sup>6</sup> or assets and which:

- Entails a potential violation of EU or international law, in particular related to Fundamental Rights and international protection obligations, and/or
- Involves a potential violation of the Frontex Codes of Conduct (CoCs)<sup>7</sup>, and/or
- Has serious actual or potential negative implications on Frontex's tasks or activities<sup>8</sup> and/or has a serious potential life-changing impact on a participant's<sup>9</sup> health.

### 2.2. Categories of SIs

Serious Incidents are clustered into three main categories, illustrated in the SI-Catalogue (Annex 1):

**Category 1** - Situations of potential violations of Fundamental Rights or international protection obligations

**Category 2** - Situations of potential violations of Codes of Conduct<sup>10</sup> provisions

**Category 3** - Situations with serious actual or potential negative implications on Frontex core tasks

Depending on the circumstances and information available concerning a certain event or occurrence, a SI can have more than one category.

### 2.3. Serious Incident Report (SIR)

A Serious Incident Report (SIR) aims to inform as soon as possible primarily the Frontex Executive and Senior Management, the Fundamental Rights Officer (FRO) as well as the Member States<sup>11</sup> and Third Countries (where appropriate and in accordance with the relevant Status Agreement and Operational Plan), the Frontex Management Board (MB) and possible other relevant stakeholders<sup>12</sup>, about the occurrence of a SI. The creation as well as the timely dissemination of a SIR contributes towards enhancing situational awareness, increasing Frontex reaction capabilities and ensuring immediate follow-up to all categories of SIRs. Through the SIR procedure, the conditions and the facts regarding an event are clarified and measures are undertaken by Frontex to respond to the incident and its possible effects. In addition, the SIR process aims at identifying lessons learned, enhancing the procedures

<sup>5</sup> Examples of indirect action include, but are not limited to, the events which are not directly heard or witnessed, not done directly but conducted by an intermediary, deviation from an original route or path, or not directly caused by or resulting directly from an action.

<sup>6</sup> For the purpose of the SOP, participants in Frontex activities refer to all persons taking part in Frontex activities as defined in Article 10 of the Regulation and as per respective operational plans, including but not limited to, Frontex staff, SNEs, Standing Corps (all categories), interpreters, cultural mediators etc.

<sup>7</sup> (i) Executive Director's Decision No R-ED-2017/32 of 10 April 2017 on adopting the Code of Conduct applicable to all persons participating in Frontex Operational Activities and (ii) Executive Director's Decision No R-ED-2018/40 of 26 April 2018 on adopting the Code of Conduct for Return Operations and Return Interventions coordinated or organised by Frontex.

<sup>8</sup> Frontex activity means any activity organised or coordinated by Frontex.

<sup>9</sup> Death or serious injury that requires admission in a hospital as an inpatient for at least one overnight stay.

<sup>10</sup> Cf. footnote 8.

<sup>11</sup> For the purpose of the SOP, the term "Member State" includes also the States participating in the relevant development of the Schengen in the meaning of the Treaty on the Functioning of the European Union and its Protocol (No 19) on the Schengen integrated into the framework of the European Union.

<sup>12</sup> The reporting to MB members and possible other stakeholders shall not contain personal data.

and processes in place and reducing the probability of an incident to reoccur including minimising risks of Fundamental Rights violations. The SIR is also a crucial source of information for the FRO to monitor the Agency's compliance with Fundamental Rights, including by conducting investigations.<sup>13</sup>

The SIR should include the following content with respect to each SI:

- SUBJECT containing short description of the SI;
- WHAT happened;
- WHEN did it happen;
- WHERE did it happen;
- WHO/WHAT was involved/affected;
- WHY/HOW did it happen;
- LIKELY/POSSIBLE effects, reactions, consequences;
- SOURCE OF INFORMATION: how was and/or who provided the information and reference to the reliability of the source;
- ACTIONS TAKEN: own actions and actions by MS/others *inter alia*, other countries, EU agencies or international organisations;
- COMMENTS (if anything to add to the facts).

### 3. Roles and Responsibilities<sup>14</sup>

In order to ensure the timely exchange of information and to enable Frontex and all involved stakeholders to take appropriate action, it is crucial that all involved stakeholders understand their role within the SI Reporting procedure (Chapter 4).

#### 3.1. Participants in Frontex activities

Participants in Frontex activities are under the obligation to report any event which could be a SI in case they learn, witness or are directly or indirectly involved in such an event and/or have grounds to believe that such event or occurrence took place, according to the provisions and reporting structure stated in Annex 2.

Frontex shall take reasonable steps to protect anyone creating a SIR against retaliation of any form, whether directly or indirectly, by their supervisor and by persons working for or acting on behalf of the supervisor (see Chapter 4.3).

#### 3.2. Fundamental Rights Monitors (FROMs)

In case of potential Fundamental Rights violations, the FROMs report directly and - in case of imminent Fundamental Rights risks - immediately to the FRO. The FROMs and Frontex Coordinating Officers shall ensure close cooperation on any events in relation to Fundamental Rights.

FROMs are considered as participants in Frontex activities for the purposes of SI category 1 and 2.

---

<sup>13</sup> Article 109(2)(b) of the Regulation.

<sup>14</sup> FRO's access to information and access to operational areas is defined in the Regulation and in Management Board Decision 6/2021 of 20 January 2021 adopting special rules to guarantee the independence of the Fundamental Rights Officer and his or her staff.

### 3.3. Coordinating staff in Frontex activities

Frontex staff with a coordinating role<sup>15</sup> act as the main contact point, responsible for supporting information gathering in relation to the SI and the coordination of the whole process in close cooperation with the FSC and the SI-Handler including the FRO.

Coordinating staff shall ensure the proper and timely transmission of information and continue to monitor the situation in close cooperation with the respective host MS/TC and involved authorities (when applicable). He/she shall subsequently report to the FSC and the SI-Handler.

The appropriate reporting channels are to be followed as specified in the current document (Annex 2), which need to be reflected in the respective Operational Plans and in the respective activity/project documents.

### 3.4. Frontex Situation Centre (FSC)

The FSC is responsible for the compilation of the collected information and the initial assessment of whether an incident should be classified as a category 2 or 3 SI. Cases of potential violations of Fundamental Rights/international protection obligations (category 1 SI) are assessed by the FRO.

In particular, the FSC is responsible for:

- coordinating the initial exchange of information, including with the FRO in order to identify Fundamental Rights relevance of the case (if a potential Fundamental Rights violation is flagged, then responsibility will be moved to the FRO as per chapter 3.5);
- assessing the initial information in cooperation with the relevant stakeholders including the FRO whether the reported case should be assigned and further processed as SI;
- assigning the related SI-Handler;
- distributing without delay the SIR according to the defined recipients list;
- supporting the SI handler in pro-actively monitoring the situation and providing available updates, in close cooperation with the responsible coordinating staff;
- supporting the insertion of a SIR in JORA, in case of need (e.g. when the reporting person has no access to report the SIR in JORA); and
- Inserting all relevant correspondence relating to the SIR in JORA.

### 3.5. Fundamental Rights Officer (FRO)<sup>16</sup>

In addition to the responsibilities outlined under Chapter 3.6 when acting as SI-Handler, the FRO is also responsible for:

- Assessing the initial information for cases involving the potential violation of Fundamental Rights/international obligations, liaising with other Frontex entities when necessary;
- Deciding whether a case related to a potential violation of Fundamental Rights/ international protection obligations should be assigned as a SI or not;

---

<sup>15</sup> Coordinating staff: e.g. Frontex Coordinating Officer for operational activities; Frontex Coordinating Officer for return operations;

<sup>16</sup> All information relevant to the FRO is systematically shared with him or her.



- Ensuring that the reported case is inserted in JORA by notifying the FSC who shall perform the insertion on behalf of the FRO; and
- Reporting regularly to the Management Board in relation to SIs related to potential Fundamental Rights/international protection obligations violations.

When the FRO handles the SIR, it is the FRO who gathers or verifies information, monitors the situation, investigates and takes any further actions on the case. The FRO might be supported by other business entities as deemed necessary by the FRO.

### 3.6. SI-Handler

A SI-Handler is assigned for every SI due to the serious potential impact and multilateral issues generated by SIRs. The SI-Handler is responsible for management, follow up, coordination and finalisation of the SIR in line with other related Frontex rules as listed in Annex 7.

In particular, the responsibilities of the SI-Handler include:

- Coordinating the collection of information related to the SI and requesting the support of other Frontex entities, when needed;
- Assessing and analysing the available information;
- Ensuring the exchange of information on the case with other Frontex stakeholders, external groups and involved MS/TC;
- Coordinating follow up measures on the SI without jeopardizing any possible administrative inquiry to be conducted for the same event in cooperation with the respective MS/TC authorities and Frontex entities;
- Monitoring and following up the situation related to the incident with a possibility of carrying out on-the-spot visits;
- Creating a timeline for enquiries and keeping track of actions taken;
- Closing the incident with a final report within one month (details under Chapter 4.2.3.), which is distributed to the initial recipients of the SIR and other relevant stakeholders, depending on the case and upon assessment by the SI-Handler (Template in Annex 5); Upon closing the case, the SI-Handler shares the findings and the lessons learned/recommendations; and
- Responding to any related information requests (including to act as a PAD case handler for the SIR).

The SI-Handler is assigned according to the category of the SI as illustrated in the SI-catalogue (Annex 1). Only one SI Handler is assigned to a SIR. If more than one SI category is assigned to a SIR, the entity which was responsible for coordinating and arranging the activity is assigned as SI-Handler, except in cases where there is a possible violation of Fundamental Rights/ international protection obligations when the FRO is always assigned as SI Handler. In case the SI includes a potential violation of Fundamental Rights/international protection obligations, the SI is categorised as Category 1 and FRO is assigned as SI Handler.

Type of SI	SI-Handler
Category 1	Fundamental Rights Officer (FRO)
Category 2	Head of TF Deploy <sup>17</sup> (for Standing Corps (SC) Categories 1-4) Head of Human Resources Unit (for Frontex staff not belonging to the SC, and SNEs) Head of Unit/Entity which organises the activity (for any other participant)
Category 3	Head of Unit/Entity which is responsible for the activity. If the responsible entity cannot be identified, the Head of Unit/Entity responsible for the personnel involved

The SI-Handler may decide to delegate this function to another appropriate representative of his/her entity.

### 3.7. Senior / Executive Management

The Senior / Executive Management is responsible for regularly reporting Serious Incidents and their state-of-play to the Management Board<sup>18</sup> (e.g. number of SI, final report, lessons learned etc.). In addition and upon instructions from Senior/Executive Management, the FSC shall flag immediately specific cases to Management Board Secretariat.

Furthermore, Senior / Executive Management acts upon the cases outlined under Chapter 4.5 and 4.6.

## 4. The procedure

### 4.1. General provisions

The reporting procedures illustrated in this Chapter apply to operational and non-operational activities. Within the SI Reporting mechanism, the FSC reports SIs via a standard taxonomy in the correspondence header:

- **SIR with potential violation of Fundamental Rights/international protection obligations (Category 1)**  
*SDO Log number - SIR FR - Operation/Activity Name - Subject*
- **SIR with potential violation of Frontex Code(s) of Conduct (Category 2)**  
*SDO Log number - SIR CoC - Operation/Activity Name - Subject*
- **SIR with serious actual or potential negative implications on Frontex core tasks (Category 3)**  
*SDO Log number - SIR - Operation/Activity Name - Subject*
- **Or any combination of the above in case more than one Category is assigned**

<sup>17</sup> Or its successor.

<sup>18</sup> Article 38(3)(h) of the Regulation.

## 4.2. Steps of reporting serious incidents

### 4.2.1. Initial Information

The initial information shall be reported by phone, email or directly in JORA (Template in Annex 3). Report by phone must always be followed by email or JORA report, as soon as possible.

- SI Category 1

in case a participant in Frontex activity learns, witnesses, is directly or indirectly involved in such incident and/or has grounds to believe that such an event took place he/she shall immediately report to the FRO who ensures the report is formally inserted in JORA in line with Chapter 3.5. After receiving such knowledge, the FRO shall immediately inform the FSC, Frontex Coordinating Officer, the respective ICC and NFPOC of the involved Member State or Third Country with initial information including a summary of the case at that point of time and serves as preliminary information to obtain immediate knowledge about the incident and conduct the first assessment.

- SI Category 2 and 3

in case a participant in Frontex activity learns, witnesses, is directly or indirectly involved in such incident and/or has grounds to believe that such event or occurrence took place he/she shall immediately report to the coordinating structure of the Frontex activity. The coordinating staff should collect any additional information and report the incident, together with an initial assessment, to the FSC with the respective ICC and NFPOC in cc.

### 4.2.2. Validation - Assessment - Distribution

#### Validation - Assessment:

- For cases which are not related to the possible violation of Fundamental Rights or international protection obligations, the FSC performs an assessment, in cooperation with the coordinating staff of the reporting entity when needed.

The assessment consists of the following elements:

- Involvement of Frontex participant/asset
- Negative implications on the Frontex tasks/activities
- Serious and potential life-changing impact on a participant's health
- Violation of Codes of Conduct provisions

It should be underlined that if the final impact level of the incident is considered critical the Crisis Management Policy procedures apply (see Chapter 4.6).

If the FSC considers that despite initial information the circumstances of the case concern a possible violation of Fundamental Rights or international protection obligations, all information is submitted to the FRO for further handling.

If the FSC assesses (and after consultation with the relevant entities, as needed) that according to the initial information, the incident does not qualify to be processed as a SI the SI Reporting procedure is not formally launched and the FSC informs the reporting Unit/staff about this decision. At the FSC level, the decision is taken by the Shift Leader or in his/her absence by the Senior Duty Officer on duty.

- For cases concerning the potential violation of Fundamental Rights/international protection obligations, the FRO performs an assessment of the incident and decides whether the SIR procedure should be launched. In case the FRO decides to launch a SIR, he/she shall inform the FSC which distributes the SIR in line with Annex 4. In case the FRO assesses that according to the initial information, the incident does not qualify to be processed as a SI, the SI Reporting procedure is not formally launched and the FRO informs the reporting Unit/staff about this decision.

#### **Distribution**

After the assessment, the FSC distributes the SIR to the defined recipients (see Annex 4), assigning at the same time the SI-Handler for the case. From that moment on, the handling of the case is transferred to the SI-Handler.

Regular updates on significant developments are shared by the SI Handler with relevant stakeholders (always with the FSC closely informed). In addition, the updated information is inserted in JORA by the SI-Handler or if needed by the FSC, with the aim of ensuring that the JORA Log contains the most complete and up-to-date information.

#### **4.2.3. Final Report**

For every SIR, a final report is drafted by the SI-Handler. The Final Report contains a detailed description of the event, timeline, information collected, entities consulted, follow-up measures, assessment of the case and the final conclusions with proposals, including also lessons learned. The Final Report is submitted to the relevant stakeholders (Frontex entities, MS/TC involved) and the Executive Management for assessment and possible decision making for further action.

The report should be finalised within 1 month from the assignment. If the report cannot be finalised within this time, the SI-Handler submits an intermediate report to the above mentioned relevant stakeholders, with the findings so far gathered, explaining the reasons for not being able to finalise the report within the given time. In this case, the Final Report is submitted as soon as the SI-Handler finalises inquiries.

The SI Reporting procedure is formally closed with the submission of the Final Report by the SI-Handler. As soon as the Final Report is produced and disseminated, the FSC administratively closes the SI report in JORA.

### **4.3. Exceptional reporting - Link to whistleblowing procedure**

Whenever a participant in Frontex activities is involved directly or indirectly witnesses or acquires knowledge about any potential serious irregularity that may have occurred or may be occurring and is a possible Serious Incident Report, the person can directly provide the information to Frontex following by analogy the reporting procedures set out in Management Board Decision 17/2019<sup>19</sup>. In these cases, Frontex shall preserve the protective measures in place (confidentiality of identity, mobility, appraisal and reclassification, anonymity, limits).

In case a Frontex participant is prevented by his/her hierarchy from reporting a SI or has any concerns about the forwarding of his/her report, he/she may either directly address the ED or the FRO for Fundamental Rights

---

<sup>19</sup> Management Board Decision 17/2019 of 18 July 2019 adopting the Frontex Guidelines on Whistleblowing.

concerns. If he/she fears retaliation, he/she may address Frontex Inspection and Control Office with the report by using [whistleblowing@frontex.europa.eu](mailto:whistleblowing@frontex.europa.eu).

#### 4.4. Reports provided to the FRO by third parties or other sources

In line with the Management Board Decision 6/2021 on special rules to guarantee the independence of the FRO and his and her staff, the FRO may receive from third parties or from other sources (international organisations, other EU Agencies, open sources, NGOs etc.) information on potential violations of Fundamental Rights and international obligations. In line with Chapter 3.5 the FRO performs the tasks thereof and decides whether to launch a SI.

#### 4.5. Escalation procedure

If, either due to additional information that has been received or upon request of a Frontex entity or SI-Handler, there is a need for re-assessment of:

- the decision for a case to be processed as SIR or not; or
- the categorisation of the SI; or
- the re-opening of the case;

the case file is submitted by the FSC to DSAM and the Director of the SI-Handler for further discussion and decision making. The file may be further escalated to the respective Deputy Executive Director(s) and the Executive Director who finally decides in consultation with the respective SI Handler. The decision and its justification are documented and logged by the FSC.

In case of categorisation of a SIR which the FRO considers to also have an impact on Fundamental Rights, the FRO reserves the right to request the take-over as SI Handler.

#### 4.6. Link to Crisis Management

If the assessment of the initial information is concluding that the impact level of an event is critical, the Frontex Crisis Management Policy<sup>20</sup> procedures should be activated, and the related information and assessments could in turn inform respective Organisational processes (for example risk analysis) and be used for the initiation of operational measures (such as deployment of the SC, Rapid Border Intervention, Joint Operation, etc.).

#### 4.7. Logbook / Storage

During the whole process, from the initial reporting until the final report, the FSC keeps track of the correspondence, the actions taken/decisions made, communications, video footage, satellite imagery or other recordings and all other relevant information regarding the SI. All correspondence related to a SI is stored by the FSC in JORA.

#### 4.8. Personal Data

Processing of personal data by the EU institutions (hereinafter referred to as EUI) is governed by Regulation 2018/1725<sup>21</sup> (hereinafter referred to as EUI DPR).

<sup>20</sup> Executive Director's Decision R-ED-2020-33 of 2 March 2020 on the Crisis Management Policy.

<sup>21</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

Section 3.4 of this SOP establishes the FSC as initial distributor of all SIs unless reported directly to the FRO. Consequently, there are two decision makers upon the processing of personal data contained in a SI. The determination of the means and the purpose of processing is how a Controller is assigned. Under that rationale, it can be established that both the FSC and the FRO are parallel controllers for this processing operation upon personal data.

The Controllers shall ensure that persons involved in or concerned by the processing of personal data in the course of a SI are notified about their personal data being processed. The persons shall be notified via privacy notice published on the Frontex website and/or in the operational plans.

In cases where information is collected from the migrants or returnees, Frontex staff shall inform them about the privacy notice on Frontex website, if not possible via other means on the spot.

#### **4.8.1 Collection and Processing of Personal Data**

The personal data of the following persons shall be collected and processed in the context of the SI:

- Frontex participants;
- other Frontex staff, SNEs and members of Category 2, 3 and 4 of the Standing Corps;

If personal data related to these data subjects is to be contained in the SIR (directly or indirectly identifiable), the corresponding signalling as in the processing of personal data of Annex 3 must be marked.

Only personal data that is strictly necessary for the purpose of the SIR - to enable the Agency to flag the occurrence of an incident that fits within the classification as established in this SOP is to be processed with the aim at conducting follow up actions with the objective of identifying lessons learned towards the Agency.

- Health data, including data of physical injury and medical measures shall be limited to only what is strictly necessary and in minimal amounts possible taking into account the nature of the incident. That data shall be included in the templates in Annex 3 and contain the affirmation that personal data is being processed. Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data such as fingerprints, or data related to a person's sex life or sexual orientation are strictly forbidden to be collected and reported in the SI report. If such a data is accidentally collected (for example in the witness statement), it shall be removed without undue delay.
- Any person involved in the collection, and later processing of personal data shall take reasonable measures to ensure that the data is accurate, and reflects the incident correctly and impartially. If the data is based on opinions and perceptions, this will be highlighted with the expression "personal opinion - unverified".
- All parties involved in the process shall ascertain that the data is accurate. If during the course of the SIR it becomes evident that the data is inaccurate, the data shall be immediately corrected.

#### **4.8.2 Transmission of personal data**

SIRs containing personal data shall only be transmitted to host Third Countries with whom there is an existing Status Agreement. The transmission of personal data shall be in compliance with Chapter V of the Data Protection Regulation, for administrative tasks only. There shall be no other international transfer of personal data in relation to a SIR besides the ones established in this point.

#### 4.8.3 Retention and deletion of Personal data

- All personal data in SIRs shall be deleted one year after the closure of the Joint Operation/Frontex activity where the SI occurred.
- When necessary for reasons of an investigation, internal or otherwise, the personal data is not deleted for the duration of the investigation, those SIRs will be archived in a separate repository with restricted access to persons nominated on a strictly need to know basis.

### 4.9. Public access to documents

SIRs can be subject to public disclosure pursuant to the provisions of 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 Management Board Decision No 25/2016 of 21 September 2016<sup>22</sup>.

#### List of annexes:

- Annex 1 - Serious Incident Catalogue
- Annex 2 - Serious Incident Reporting Standard Workflow
- Annex 3 - Report Template
- Annex 4 - Distribution of Serious Incident Reports
- Annex 5 - Final SI-Handler Report Template
- Annex 6 - List of potential Fundamental Rights violations within Frontex activities
- Annex 7 - Relevant legal acts and other documents

---

<sup>22</sup> Management Board Decision No 25/2016 of 21 September 2016 adopting practical arrangements regarding public access to documents held by Frontex.

## ANNEX 1 - Serious Incident Catalogue

### Serious Incident - Indicative List per category

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

#### **Category 1** - Situations of potential violation of Fundamental Rights or international protection obligations

- Potential violations of Fundamental Rights enshrined in the Charter of Fundamental Rights of the European Union or other relevant international law as described under Annex 6
- Lack of safeguards of Fundamental Rights protection either by action or failure to act (Article 80(1) of the Regulation)
- Witnessed potential violations of Fundamental Rights, in particular against human dignity.

#### **Category 2** - Situations of potential violations of Codes of Conduct provisions

Potential violation of the Frontex Codes of Conduct, except for cases which are also related to potential violations of Fundamental Rights and/or the obligations on international protection (Category 1)

#### **Category 3** - Situations with serious actual or potential negative implications on Frontex core tasks

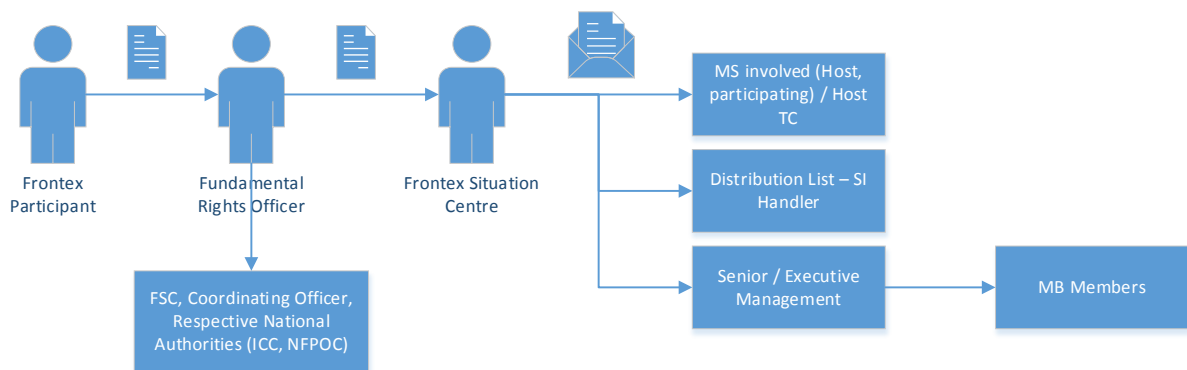
- Serious accidents with the involvement of persons or means during Frontex activities
- Serious/severe contagious disease or severe/life-threatening injury of participants
- Death of Frontex staff/SNEs/other SC member during Frontex activities
- Arrest, detention or criminal proceedings against Frontex staff, SNEs, SC Category 2-4 (except for issues related to Code(s) of Conduct/violation of FR).
- Any other serious incident which does not fall under SI Category 1 and 2



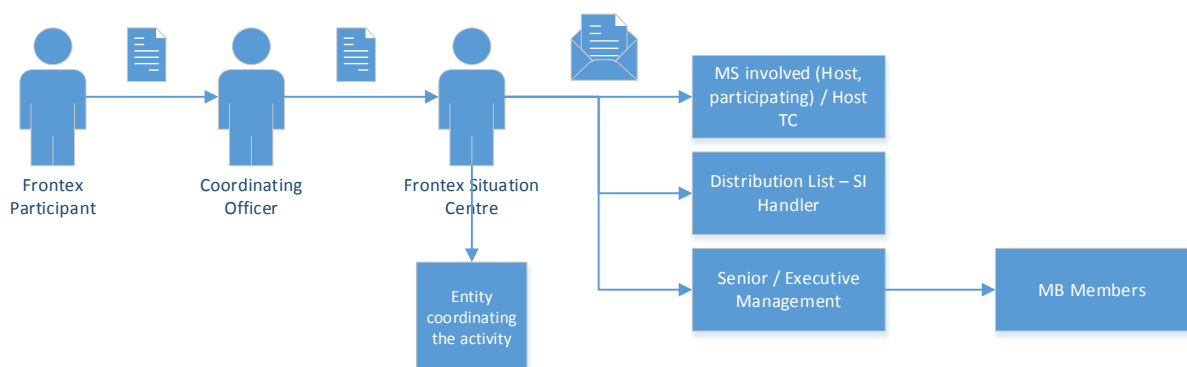
## ANNEX 2 - Serious Incident Reporting Standard Workflow

Cases which could potentially be assigned to SI Category 2 and 3, should be immediately reported to Coordinating Staff (and to the FRO if in doubt as to the exact categorisation or in the event of multiple categorisation of the case). In case a participant in Frontex activities learns, witnesses, is directly or indirectly involved or has grounds to believe that a possible violation of Fundamental Rights/international protection obligations has taken place, he/she is obliged to report the case as soon as possible directly to the FRO. After receiving such knowledge, the FRO needs to inform immediately the FSC, Frontex Coordinating Officer, the respective ICC and NFPOC of the involved Member State or Third Country with initial information including a summary of the case at that point of time and serves as preliminary information to obtain immediate knowledge about the incident and conduct the first assessment if the case should be escalated as SI.

SIR – Standard Workflow for Category 1



SIR – Standard Workflow for Category 2 and 3



## ANNEX 3 - Report Template



Reporting Date and time (UTC)				
Reporting person				
Subject				
Frontex activity/ Joint Operation				
Proposed SI Category				
JORA Incident number (if any)				
Original source of information				
Frontex resources involved				
Type of resources involved (Human resources / technical equipment)				
Incident date/time				
Location of the incident				
Latitude				
Longitude				
Location Details				
Reference to the operational area (for operational activities)				
Dead/Missing/Injured persons				
Link to Use of Force reporting	YES		NO	
Personal Data contained	YES		NO	

<b>Information/Allegations</b>

Assessment
Potential violation of EU or international law, in particular related to Fundamental Rights and international protection obligations and/or
Potential violation of the Frontex Code of Conduct (CoC) and/or
Direct or indirect Involvement of Frontex participants or deployed assets:
Negative Implications on Frontex tasks/activities:
Serious or life-changing impact on participant's health:

Measures/Actions Taken

## ANNEX 4 - Distribution of Serious Incident Reports

The FSC is the unit primarily responsible for the distribution of the SIRs and for managing/documenting the correspondence connected with each case. In this respect, SI-Handler and involved stakeholders shall provide to the FSC all the related correspondence.

After the assignment of a case as SI, the FSC informs the defined distribution list, the SI Handler who is allocated for this case and also the host MS and TC<sup>23</sup> and concerned/involved MSs about the initiation of the SIR procedure. Any subsequent communication with internal or external stakeholders on the SI and its status is decided and managed by the SI-Handler. Other external partners (e.g. EU Institutions, Agencies, etc.) can be included in SI-related correspondence on a need to know basis, depending on the case and after the assessment by the SI-Handler.

### SIR Distribution list

<b>Serious Incident Report with possible violation of FR</b> <b>(Category 1)</b>	<b>Serious Incident Report with possible violation of CoC</b> <b>(Category 2)</b>	<b>Serious Incident - General category</b> <b>(Category 3)</b>
Personal and functional mailboxes of: - Executive Director - DEDs - HoCAB - HoOMPR - DODs - HoUFSC - HoULPU - HoOICO - HoOFRO - Head of TF Deploy <sup>24</sup>		
Additionally: - FSC Shift Leaders - SI Handler per case - HoU of the entity organising the activity (if not the same as SI Handler)		

*The predefined distribution list applies. The respective list of recipients can be extended on a need to know basis, in consultation with the SI-Handler.*

<sup>23</sup> National Frontex Points of Contact (NFPoC).

<sup>24</sup> Or its successor.

## ANNEX 5 - Final SI-Handler Report Template



Warsaw, .....

### FINAL SIR REPORT

Log Number: ..... /YYYY - SIR - .....

SI-Handler: .....

<b>Key Points</b>
<ul style="list-style-type: none"><li>•</li><li>•</li><li>•</li></ul>
Description of the event - Timeline
Information collected - Contributors/Entities consulted - Follow-up
Assessment
Final conclusion - Proposals - Lessons learned

## ANNEX 6 - List of potential Fundamental Rights violations within Frontex activities

(non-exhaustive list)

- Asylum**
  - Non-access to the asylum procedure:
    - Non-Identification
    - Non-Registration
    - Non-Information and counselling
    - Removal without guarantees
- Children**
  - Best interests of the child
  - Living conditions (unsuitable/degrading)
  - 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**
- 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/Right to good administration**
  - 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 (proportionality):
    - Excessive use of force
    - 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
  - No individual assessment
- 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):**
  - .....
  - .....
  - .....
  - .....
  - .....

## ANNEX 7 - Relevant legal acts and other documents

- Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard;
- Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data;
- Management Board Decision 12/2021 of 14 February 2021 adopting the Fundamental Rights Strategy.
- Management Board Decision 7/2021 of 20 January 2021 establishing a supervisory mechanism to monitor the application of the provisions on the use of force by statutory staff of the European Border and Coast Guard Standing Corps;
- Management Board Decision 6/2021 of 20 January 2021 adopting special rules to guarantee the independence of the Fundamental Rights Officer and his or her staff;
- Management Board Decision 17/2019 of 18 July 2019 adopting the Frontex Guidelines on Whistleblowing;
- Executive Director Decision No R-ED-2017-32 of 10 April 2017 adopting the Code of Conduct applicable to all persons participating in Frontex Operational Activities;
- Executive Director Decision No R-ED-2018-40 of 26 April 2018 adopting the Code of Conduct for Return Operations and Return Interventions coordinated or organised by Frontex;
- Executive Director Decision No 2014/08 of 3 February 2014 on the adoption of the Frontex Standard Operating Procedure for handling alleged violations of the Frontex Code of Conduct for all persons participating in Frontex activities (Frontex CoC) and Frontex Code of Conduct for Joint Return Operations coordinated by Frontex (Frontex CoC for JROs)<sup>25</sup>;
- Executive Director Decision No 2012/87 of 19 July 2012 on the adoption of the Frontex Standard Operating Procedure to ensure respect of Fundamental Rights in Frontex joint operations and pilot projects;
- Executive Director Decision No R-ED-2018-159 of 31 December 2018 on Frontex Internal Structure and Rules of Procedure (“FISRoP”);
- Executive Director Decision No R-ED-2020/33 of 2 March 2020 Frontex Crisis Management Policy;
- Executive Director Decision No R-ED-2021-38 of 6 March 2021 on Standard Operating Procedure (SOP) - Use of force and incidents involving the use of force reporting (UFR / IFR).

---

<sup>25</sup> A revision of Executive Director’s Decision 2014/08 will be initiated by Pooled Resources Unit, based on the revised SOP for Serious Incident Reporting.