

Heavy technical equipment

Other technical equipment

Heavy technical equipment

Other technical equipment

Commented [A12]: The non-disclosed parts contain information regarding the technical equipment deployed in the operational area by Frontex and Member States. Disclosing such information would be tantamount to disclosing the exact type and capabilities of the equipment and would enable third parties, e.g. by combining this information with other sources, to draw conclusions regarding usual positions and movement patterns. This would open way for abuse, as numbers and types of equipment used in previous operations are indicative of similar numbers and types for succeeding years. Releasing such information would thus benefit criminal networks, enabling them to change their modus operandi and, consequently, result in hampering the course of ongoing and future operations of a similar nature. This would ultimately obstruct the purpose of such operations: to counter and prevent cross-border crime and unauthorized border crossings. In this light, the disclosure of information regarding the technical equipment deployed would undermine the protection of the public interest as regards public security in the sense of Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

The non-disclosed parts refer to details of the operational area and cannot be released. As ongoing operations tend to cover similar operational areas as the operations conducted in preceding years, disclosing details of previous operational areas would be tantamount to disclosing the current state of play. This would provide smuggling and other criminal networks with intelligence, enabling them to change their modus operandi, which would ultimately put the life of migrants in danger. Consequently, the course of ongoing and future operations of similar nature would be hampered by depriving the operations of any strategy and element of surprise, ultimately defeating their purpose to counter and prevent cross-border crime and unauthorized border crossings. In this light, the disclosure of documents containing such information would undermine the protection of the public interest as regards public security in the sense of Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.



REMARK:

Any changes related to the level of the deployed resources in the course of the RBI do not require the amendment of the Operational Plan. Those deployments will be agreed between Frontex, host and respective participating MS during implementation phase of the RBI.

ANNEX 8 - OPERATIONAL BRIEFING AND DEBRIEFING

Operational briefing

The Operational Briefing is composed of 2 parts:

- General briefing - delivered by Frontex
- National briefing - provided by the respective officers of the host MS

Structure of the Operational briefing:

- Crew members of the assets and officers of the host MS will be briefed at the deployment location during the first day of the deployment.

Standard plan of the General Briefing:

- Legal framework of Frontex (including role, tasks and current structure of Frontex).
- Legal framework of the Rapid Border Intervention.
- Fundamental rights in Frontex activities.
- Frontex Code of Conduct applicable to all persons participating in Frontex Operational Activities.
- Description and assessment of the situation in the area.
- Operational concept, aim and objectives.
- Information on implementation (period, briefing/debriefing, operational areas, participation).
- Main aspects of the Rules on Use of Force.
- Cooperation with third countries, other EU agencies and bodies or international organizations in the operational area.
- The tasks and roles of participants.
- Command and control.
- Communications within JO, FOSS, Press rules.
- Reporting (JORA, incidents, SIR, ██████████ and Frontex).
- Contact details of responsible Frontex staff.
- Organisational arrangements and logistics.
- Evaluation (reports).
- General overview about Frontex Document Alerts.
- Awareness session on THB and Children at Risk.

Operational briefings will be complemented by EASO and EUROPOL representatives by presenting their mandate and tasks within the area where all agencies are operating together.

Standard plan of the National briefing:

- Introduction to the border management, national coast guard/border/police authorities, organizational structure and responsibilities of the respective central and local authorities.
- Contact details of responsible officers (ICC and LCC Coordinators, Central and Local Police Coordinators, Team Leaders, OLO-TE, etc.).
- Introduction to the referral procedures and the responsible national authorities in regard to the vulnerable groups / people seeking international protection.
- National legislation related to the powers and obligations of the Team Members and instructions (supported by a possible demonstration) for use of force including use of weapons.
- Transportation/storage/carry of weapons/special technical equipment.

Commented [A13]: The non-disclosed part contains detailed information related to reporting tools and methods used by law enforcement officials to conduct border control tasks and counter criminal activities. Its disclosure would jeopardize the implementation of ongoing and future operation, and thus facilitate irregular migration and trafficking in human beings as the effectiveness of law enforcement measures would be significantly reduced. As disclosing this information would undermine the protection of the public interest as regards public security, this part is not disclosed pursuant to Article 4(1)a) first indent of Regulation (EC) No 1049/2001.

[REDACTED]

- Presentation of duty plan/working schedule for the deployed crew members.
- Working conditions and facilities in the specific operational area.
- Logistical information on heavy equipment and spare parts delivery (applicable for crews only).

Operational debriefing

The Operational debriefing for all participants will be performed by FOC/FSO on the spot in close cooperation with the local authorities during the last days of the deployment. In case the Operational debriefing for crewmembers cannot be organized for each deployed asset, it can be limited to the NO within the ICC.

Operational debriefing should consist of at least the following topics:

- Brief feedback on the deployment in operation by the participants on:
 - cooperation with the central/local authorities and Frontex.
 - the assigned tasks' execution within the overall operational concept.
 - information flow among deployed officers - national authorities - Frontex.
- Brief feedback of the performance of the deployed officers by the host MS representative.
- Questions/answers.

[REDACTED] is considered as a part of Operational debriefing.

Commented [A14]: The non-disclosed part contains detailed information related to reporting tools and methods used by law enforcement officials to conduct border control tasks and counter criminal activities. Its disclosure would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and trafficking in human beings as the effectiveness of law enforcement measures would be significantly reduced. As disclosing this information would undermine the protection of the public interest as regards public security, this part is not disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001 .

ANNEX 9 - COOPERATION WITH OTHER UNION BODIES, OFFICES AND AGENCIES OR INTERNATIONAL ORGANISATIONS

Cooperation with EFCA and EMSA

Cooperation between Frontex, the European Fisheries Control Agency (EFCA) and the European Maritime Safety Agency (EMSA) is based on a Tripartite Working Arrangement and includes sharing of maritime information, providing new surveillance and communication services, building capacity, analysing operational challenges and emerging risks in the maritime domain as well as planning and implementing multipurpose operations.

The general operational cooperation between Frontex and EFCA, and Frontex and EMSA is carried out through the operational structures of the RBI and assigned contact points of the respective host MS authorities.

The agencies share, in advance, via established contact points, the basic information on planned patrols of aerial and maritime assets to ensure effective planning and use of resources.

Frontex and EFCA

The cooperation focuses on the exchange of information, namely sightings as regards fisheries control within the operational area of the RBI. In this frame:

- EFCA's template with the minimum requirements for sighting information to be collected is used by participants for all sightings of fishing vessels.
- During EFCA's operations EFCA provides sighting information and position of vessels, which could be of possible interest for Frontex.

In addition, EFCA periodically delivers a tailored briefing package on fisheries control for the National Officials of the aerial and maritime assets deployed in the RBI.

Frontex and EMSA

EMSA periodically delivers a tailored briefing package on pollution control for the National Officials of the aerial and maritime assets deployed in the JO. Frontex can also contribute to EMSA workshops/events with operational experiences in relation to multipurpose maritime activities and deliver tailored briefings for that purpose.

Each time a maritime or aerial asset deployed within the RBI observes a (potential) pollution spill, the Potential Marine Pollution Sighting Form will be filled in and sent to ICC/ EMSA as soon as possible for further analysis and possible action.

EMSA various operational related services to be consumed within multipurpose maritime activities and delivered under umbrella of Eurosur Fusion Services.

Cooperation with Europol

Frontex and the European Union Agency for Law Enforcement Cooperation (Europol) cooperate during the RBI through exchange of information and intelligence.

Both Agencies may contribute to each other Operational briefings, thus maintaining the awareness of the Agencies' mandates and responsibilities to the experts deployed by Frontex and Europol.



Cooperation with EUROJUST

EUROJUST has appointed the contact person in the frame of EURTF.

Cooperation with FRA

The European Union Agency for Fundamental Rights (FRA) can support Frontex in the mainstreaming of fundamental rights in all Frontex activities. Upon request, FRA can provide advice on how to operationalise fundamental rights in Frontex operations. Frontex and FRA also cooperate in the planning and implementation of research at the external EU borders.

FRA also can participate in Readmission activity as an observer.

Coordination with Interpol

Frontex facilitates the coordination between the host MS and International Criminal Police Organization (Interpol) during the RBI through collection of data and intelligence. In particular, the information collected during the RBI, with possible links to criminal activities such as terrorism, trafficking in human beings and smuggling of illicit goods, will be passed to the host authorities, which is a responsible entity to ensure the further dissemination to Interpol, if relevant.

The access to Interpol's global databases enabling comparison of fingerprints, photographs and travel documents to identify internationally wanted persons using false identities may be developed and ensured in the registration locations.

Implementation of the SOP with NATO

Referring to the conclusions of the European Council of 18/19 February 2016, Frontex is coordinating its operational activities under this RBI with the North Atlantic Treaty Organization (NATO) in the Aegean Sea in accordance with the Standard Operating Procedures (SOP).

The Standard Operating Procedures (SOPs) for the cooperation between NATO activity and Frontex coordinated operation in the Aegean Sea is provided in the Annex 13.

[REDACTED]

ANNEX 10 - COORDINATION STRUCTURE

Tasks and Roles of Participants

Member States

International Coordination Centre (ICC)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

ICC Coordinator

[REDACTED]

[REDACTED]

Commented [A15]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[Redacted]

The ICC Coordinator shall:

[Redacted]

Commented [A16]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

Central Police Coordinator (CPC)

[Redacted]

Operational Liaison Officer (OLO)

[Redacted]

Joint Coordinating Board (JCB)

[Redacted]

National Official (NO)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

The NO shall:

[Redacted]

Commented [A17]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

Intelligence Officer (IO)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Team Members and Officers of the host MS

[Redacted]

Commented [A18]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

Commanding Officer (CO)

[Redacted]

Local Coordination Centre (LCC)

[Redacted]

LCC Coordinator

[Redacted]

Local Police Coordinators (LPC)

[Redacted]

¹⁶ In case of maritime and aerial assets.

[Redacted]

Operational Liaison Officer for Technical Equipment (OLO-TE)

[Redacted]

Commented [A19]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[Redacted]

Operational Liaison Officer at the FOCC (OLO-FOCC)

[Redacted]

Frontex

Frontex Coordinating Officer (FCO)

[Redacted]

[Redacted]

The [Redacted]

Operational Manager (OM)

[Redacted]

[Redacted]

[Redacted]

Operational Team (OT)

[Redacted]

Frontex Operational Coordinator (FOC)

[Redacted]

[Redacted]

Frontex Support Officer (FSO)

[Redacted]

Commented [A20]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[Redacted]

[Redacted]

Frontex Support Officer (FSO) for Deployment and Logistics

[Redacted]

[Redacted]

Operational Analyst (OA)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Commented [A21]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[Redacted]

Frontex Operational Coordination Centre (FOCC)

[Redacted]

European Coast Guard Functions Officer (ECGFO)

[Redacted]

[Redacted]

[Redacted]

Frontex Information Management Officer (FIMO) to Greece

[Redacted]

[Redacted]

[Redacted]

Commented [A22]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[Redacted]

Frontex Situation Centre (FSC)

[Redacted] reporting

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Senior Duty Officer (SDO) Service in FSC

[Redacted]

Deployed Frontex Information Management Officers' (FIMO) to FSC

[Redacted]

[Redacted]

Information Fusion Centre (IFC)

[Redacted]

Commented [A23]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[REDACTED]

IFC roles concerning Frontex One Stop Shop (FOSS)

[REDACTED]

IFC roles and responsibilities concerning JORA

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Frontex Liaison Office [REDACTED]

[REDACTED]

European Union Regional Task Force (EURTF)

[REDACTED]

Field Press Coordinator (FPC)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Commented [A24]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

The non-disclosed part contains detailed information related to reporting tools and methods used by law enforcement officials to conduct border control tasks and counter criminal activities. Its disclosure would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and trafficking in human beings as the effectiveness of law enforcement measures would be significantly reduced. As disclosing this information would undermine the protection of the public interest as regards public security, this part is not disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001 .

[REDACTED]

Fundamental Rights Officer (FRO)

During implementation of operational plan, the Frontex Fundamental Rights Officer (FRO) has the task to monitor the compliance with the fundamental rights in the Agency's activities and as such contribute to the mechanism for monitoring fundamental rights, in accordance to Article 109 of the Regulation. FRO also contributes to operational briefings, debriefings and evaluations of the operations, providing recommendations, guidance during its implementation and separate observations to the Frontex Evaluation Reports (FER).

In addition, FRO handles and decides on admissibility of complaints lodged against staff in operational areas for potential breaches of fundamental rights during implementation of operational activities by persons directly affected by them.

Commented [A25]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

ANNEX 11 - JORA

JORA Actors

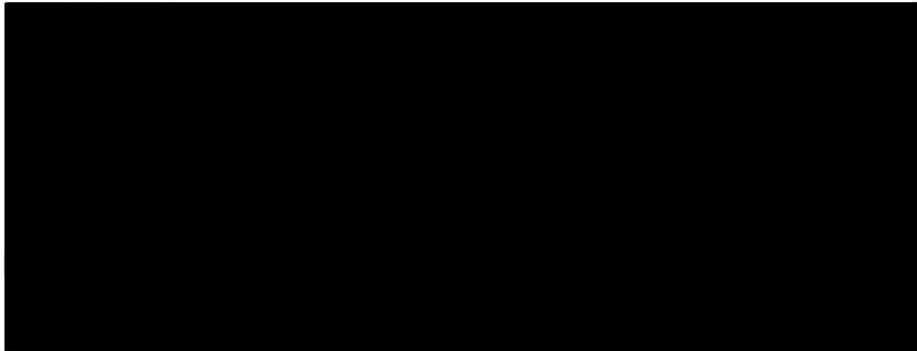
Role	Name	FX/MS	Entity	E-mail	Phone
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Commented [A26]: The blanked out parts contain detailed information related to means of communication used by law enforcement officials. Their disclosure would lead to possible abusive usage and harm the course of future and ongoing operations, and thus facilitate irregular migration. 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.

The blanked out part contains personal data. Its disclosure would affect the privacy and integrity of the individual. Therefore, its disclosure is precluded pursuant to the exception laid down in Article 4(1)(b) of Regulation 1049/2001 regarding public access to European Parliament, Council and Commission Documents.

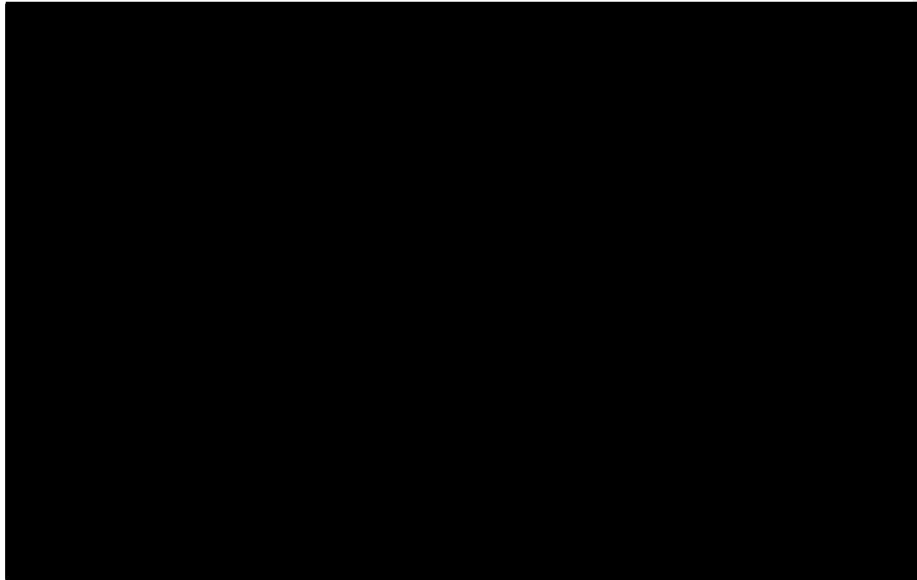


JORA Reporting Structure



Commented [A27]: The non-disclosed part contains detailed information related to reporting tools and methods used by law enforcement officials to conduct border control tasks and counter criminal activities. Its disclosure would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and trafficking in human beings as the effectiveness of law enforcement measures would be significantly reduced. As disclosing this information would undermine the protection of the public interest as regards public security, this part is not disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001 .

JORA Reporting Timeline



ANNEX 12 - STANDARD OPERATING PROCEDURES (SOP) FOR THE COOPERATION BETWEEN NATO ACTIVITY AND FRONTEX COORDINATED OPERATION IN THE AEGEAN SEA

For the purpose of implementing the conclusions of the European Council of 18/19 February 2016, Frontex and MARCOM have agreed on the basis and modalities of the cooperation regarding NATO support to assist with the current migration crisis and Frontex operational activities in the Aegean Sea, as defined in the respective Exchange of Letters. These Standard Operating Procedures (SOP) shall be implemented, in order to ensure the smooth cooperation among the stakeholders taking into consideration that NATO activities in the area are limited to the conduct of reconnaissance, monitoring and surveillance of illegal border crossings within the defined Area of Activity/ Operational Space.

Information exchange and situation monitoring

MARCOM and Frontex will exchange information classified up to and including “NATO RESTRICTED releasable to Frontex” and “EU RESTRICTED releasable to MARCOM” with a view to effectively achieve the operational objectives in accordance with the following principles:

- Exchange of information from various sources (including information by EU law enforcement bodies upon prior approval of the originator), aiming to gather analyzed information using existing frameworks and platforms. The source(s) and the means by which information has obtained shall not be published.
- Scope of the information exchange includes the sharing of incidents and information relevant for border surveillance, preferably in real time, leading to a common situational picture in the areas of interest.
- Exchange of situational and other relevant reports related to operational activities in the areas of interest.

The information exchange between Frontex and MARCOM will respect the respective coordination structures and the command and control, communication and reporting procedures of the JO Poseidon [REDACTED]

Frontex may share relevant NATO UNCLASSIFIED marked information received with other EU Agencies (e.g. Europol, EASO) participating in the European Regional Task Force (EURTF) set up in Greece, subject to originator's control. Information will be shared within the structure of EURTF and Frontex representative there will request for the originator's control.

FRONTEX will not transfer or release any “NATO RESTRICTED releasable to Frontex” marked information to a third party without the prior written approval of the originator of the information. In case of a need the written approval procedure will be communicated through the Frontex Situation Centre (FSC).

MARCOM may share relevant EU LIMITED (UNCLASSIFIED) information received from Frontex with a third party subject to originator control. The contact point for information sharing and originator control is the FSC.

MARCOM will not transfer or release any EU RESTRICTED information received from Frontex to a third party without the prior written approval of the originator of the information. The contact point for information sharing and originator control is the FSC.

Downgrading and declassification of “NATO RESTRICTED releasable to Frontex” and “EU RESTRICTED releasable to NATO” information remains subject to originator and source subject's control.

Commented [A28]: The non-disclosed part contains detailed information related to reporting tools and methods used by law enforcement officials to conduct border control tasks and counter criminal activities. Its disclosure would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and trafficking in human beings as the effectiveness of law enforcement measures would be significantly reduced. As disclosing this information would undermine the protection of the public interest as regards public security, this part is not disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[REDACTED]

Exchange of liaison officers

MARCOM may designate and deploy a liaison officer to Frontex Liaison Office (FLO)/ EURTF in Piraeus in order to closely cooperate with ICC Piraeus.

Frontex Executive Director may designate a Frontex Liaison Officer (LO) to MARCOM to be deployed in NATO SNMG flagship and/or subordinate commands at the operational and tactical level.

The LO are deployed to facilitate the communications between the respective coordination structures at the operational and tactical level.

Frontex and MARCOM will cover all costs associated with the deployment of their own liaison officers. Further questions related to the status and arrangements applicable to LO will be agreed between Frontex Executive Director and the appropriate level of MARCOM.

Operational planning and deployment

The operational coordination body of the International Coordination Centre (ICC) will make available to Frontex LO to MARCOM:

- [REDACTED] and other relevant data at the beginning of each deployment.

[REDACTED]

Commented [A29]: The non-disclosed part contains detailed information related to reporting tools and methods used by law enforcement officials to conduct border control tasks and counter criminal activities. Its disclosure would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and trafficking in human beings as the effectiveness of law enforcement measures would be significantly reduced. As disclosing this information would undermine the protection of the public interest as regards public security, this part is not disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

MARCOM, will make available to the ICC, either through the MARCOM LO to Frontex or through the Frontex LO to MARCOM:

- [REDACTED] and other relevant data at the beginning of each deployment.

[REDACTED]

The further development of shared awareness and de-confliction arrangements will be the responsibility of the ICC Coordinator after prior consultation within the framework of National Interagency Cooperation. Communications with Frontex as well as with the NATO commander at theatre level will follow in accordance to the relevant Operational Plan.

Liaison officer duties

The LO deployed will perform the following tasks:

[REDACTED]

Commented [A30]: The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

[REDACTED]

Operational communication

The operational communication between JO Poseidon and MARCOM will be ensured via e-mail, JORA File Repository, cell and fixed line phones and videoconferences as well as radio and satellite phones. In order to facilitate the exchange of 'NATO Restricted Releasable to Frontex and EU Restricted information, [REDACTED] these must be individually configured for each Frontex personnel prior to releasing them from MARCOM.

Communication between Frontex deployed assets and MARCOM units will be in accordance to International Radio Communication Procedures. Furthermore, any other available tool enabling the communication among all participants and coordinating structures will be used.

Commented [A31]: The non-disclosed part contains detailed information on the means of communication used by law enforcement officials. The disclosure of this information would put law enforcement officials' work in jeopardy and harm the course of future and ongoing operations aimed at curtailing the activities of organized criminal networks involved in the smuggling and migrants and trafficking in human beings. As the disclosure of such pieces of information would undermine the protection of the public interest as regards public security, it must therefore be refused as laid down in Article 4(1)(a) first indent of Regulation (EC) No 1049/2001 .

ANNEX 13 - DATA PROTECTION REQUIREMENTS FOR THE RAPID BORDER INTERVENTION

1. Data Processing conditions

The conditions agreed with MSs in the Management Board Implementing Rules of 2015 and with the EDPS in two different opinions are as follows:

- Only personal data related to persons about whom there are grounds they may have committed a cross border crime are to be processed by the agency.
- The personal data shall be transmitted by the host MS to the Agency via the Intelligence officer.
- Personal data of that nature shall only be transmitted via JORA.
- The controller of the personal data is the host MS.
- MSs may set specific conditions for the transmission of the personal data to the Agency.
- The sources of the personal data are debriefing activities and other actions foreseen in the Operational Plan.
- The types of entities to be transmitted to the Agency and the types of data categories related to suspects of cross border crime.

2. Data protection requirements

The data protection requirements for this RBI are linked to the fulfilment of the data protection principles. Only the personal data referred to in this Annex will be allowed to be processed within the context of this RBI. Any processing activity taking place that is not covered under this Annex will be deemed unlawful and will not be processed by the parties (host MS and Frontex).

2.1 Lawfulness, fairness and transparency

The personal data to be processed under this Annex will be processed under the legal regimes applicable to each party. Personal data processed in relation of migrants shall be processed by the host MS and under the General Data Protection Regulation and national provisions, if applicable, developing the General Data Protection Regulation.

The host MS undertakes the obligation to ensure that transparency is provided vis-à-vis the data subjects.

Personal data related to individuals under which there are serious grounds to believe they may have been involved in the commission of cross border crime will be processed by both the host MS and the Agency. For the processing activities related to this data subject, the host MSs will be subjected to the transposed national provisions of the Law Enforcement Directive.

Frontex may receive, upon agreement of the respective authority of the Host MS, operational personal data related to suspects of cross border crime from the host MS and the processing activities will be subjected to Chapter IX of the European Union Institutions Data Protection Regulation and the specific provisions governing the processing of personal data contained in the EBCG Regulation. The Agency undertakes the obligation to ensure transparency via the appropriate notice and record.

2.2 Purpose limitation

Personal data will be collected only for the achievement of specific purposes for which the RBI has been opened. In particular, for this RBI, the purpose of processing personal data is for controlling illegal immigration and tackling cross-border crime, while facilitating legitimate border crossings. Processing of personal data is limited to the operational activities defined below.

The purpose for the processing of operational personal data limited to suspects is threefold:

- to identify, based on reasonable grounds, suspects of cross-border crime by the host Member State.
- to facilitate the transmission of operational personal data to Europol.
- to use the collected operational personal data for the performance of risk analysis.



2.3 Data minimisation

Only the following types of data subjects will be allowed to be processed within the framework of this RBI:

Persons who cross the external border without authorization
Persons about whom there are reasonable grounds to suspect are involved in cross border crime (Suspects)
Personal data of the personnel involved in the RBI (Officers)

Only the minimum amount of data will be processed for the following activities:

Operational activity

Border checks	Not applicable
Border surveillance at sea	
Border surveillance at land	Not applicable
Preventing and detecting cross-border crime	
Supporting screening of migrants' nationality	Not applicable
Supporting fingerprinting and registration of migrants	Not applicable
Supporting documents checks of migrants at reception centres and in hotspot areas	Not applicable
Reporting relevant document and identity fraud cases (Frontex Document Alerts)	Not applicable
Collection of information through the debriefing activities	Not applicable
Information gathering through the second-line interviews at the airports	Not applicable
Supporting the implementation of the Readmission activity	Not applicable
EUROSUR FUSION SERVICES - Vessel Monitoring & Tracking Service	

2.4 Accuracy

Both parties undertake the obligation to ensure that the data processed within this RBI will be accurate and will develop mechanisms to ensure the accuracy of the data. In the processing of operational personal data, the host MS will strive to communicate to the Agency those cases where data may not have been accurate. In particular, the host MS will communicate to the Agency when there are no longer reasonable grounds to suspect that an individual has been involved in cross border crime. In those cases, the Agency will delete the data immediately.

2.5 Storage limitation

Personal data related to persons who cross the external border without authorization will be stored by the host MS for a period determined according to their national procedures.

Personal data related to suspects will be processed by the host MS for a period determined according to their national procedures. When the same data is processed by the Agency, the data shall be deleted or rendered anonymous after 90 days.



2.6 Integrity and confidentiality

The host MSs shall ensure appropriate technical and organizational measures for all the personal data processed within a RBI. In case of a personal data breach, the host MS will notify the occurrence of such breach to their national data protection supervisor and communicate the breach to the Agency. In relation to the operational personal data allowed to be processed by the Agency, Frontex shall notify possible data breaches to the European Data Protection Supervisor and communicate those to the host MS.

2.7 Accountability

For the following processing activities upon personal data, the Data Protection responsibility is allocated as indicated in the table below. The Controller is bound to demonstrate the compliance with the applicable legal framework.

When one of the parties is nominated as Controller, that party determines on its own the purposes for which the processing of personal data is taking place as well as the means for the processing of personal data. The other party shall not be able to challenge or intervene in that decision making process.

When the Agency is processing personal data on behalf of a host MS who acts as Controller, the Agency shall only do so on written instructions from the Controller. For those cases where a Controller is the host MS and the Agency is a processor, both parties undertake the obligation to arrange a legally binding document with the following minimum requirements:

- Frontex shall only process personal data on behalf of a host MS following documented instructions.
- Only specific persons shall be authorized to process personal data on behalf of the host MS and these persons shall commit themselves to confidentiality.
- Frontex shall follow the security and organizational measures indicated by the host MS.
- A procedure shall be included in the text in relation to the position of Frontex when data subjects may wish to exercise their rights.
- A procedure shall be included in the text with regards to security of personal data and personal data breaches.
- Frontex shall make available to the Controller host MS all information available necessary to demonstrate compliance with data protection obligations in accordance with Regulation (EU) 1725/2018.

Operational activity	Personal data processing activities	Data Protection Responsibility
Border surveillance at sea	<ul style="list-style-type: none"> The crew members of maritime and aerial assets must properly document by taking photos and/or videos all actions (detection, tracking and interception) for information and evidence collection purposes. Collected/collated information (pictures and/or videos) related to sightings of fishing vessels or gear from participating assets during patrolling activities TVV and aerial assets observation includes taking photos and/or videos. 	MS as Controller FX as Processor on behalf of the Controller
Preventing and detecting cross-border crime	<ul style="list-style-type: none"> Officers deployed can report information and operational personal data related to suspects of cross-border crime, including terrorism, collected during their operational activities 	MS and FX as Joint Controllers
EUROSUR FUSION SERVICES	<ul style="list-style-type: none"> Search, identification and tracking of vessels of interest using IMO and MMSI numbers and others pertaining to commercial and fishing vessels fleets available at EMSA database. The processing activities upon this database and with specific software are conducted by FX and MSs. 	FX and MS in parallel controllership FX as controller

Commented [A32]: The non-disclosed part contains detailed information related to reporting tools and methods used by law enforcement officials to conduct border control tasks and counter criminal activities. Its disclosure would jeopardize the implementation of ongoing and future operations, and thus facilitate irregular migration and trafficking in human beings as the effectiveness of law enforcement measures would be significantly reduced. As disclosing this information would undermine the protection of the public interest as regards public security, this part is not disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.

The non-disclosed part contains detailed information regarding the modus operandi of law enforcement officials performing border control and/or coast guard duties. Disclosing such information would expose the working methods applied in ongoing and future operations, thus obstructing their effectiveness in prevention of cross-border crime and unauthorized border crossings. In consequence, it would undermine the protection of the public interest as regards public security and thus, cannot be disclosed pursuant to Article 4(1)(a) first indent of Regulation (EC) No 1049/2001.



For those cases where there is a Joint Controllership, both the host MS and the Agency shall draw an arrangement with the minimum following conditions:

- Responsibilities with their respective data protection obligations.
- Specification of procedures for data subjects rights.
- Roles of the parties.