



OPERATIONS DIVISION Joint Operations Unit Air Border Sector

Specific Annex 1-10 of the Operational Plan

Joint Operation Alexis I 2015 2015/ABS/06





INDEX

SPECIFIC ANNEX 1 - DESCRIPTION AND ASSESSMENT OF THE SITUATION	3
SPECIFIC ANNEX 2 - OPERATIONAL OBJECTIVES AND INDICATORS	12
SPECIFIC ANNEX 3 - STANDARD OPERATIONAL PROCEDURES (SOP ON THE BASIS OF VEGA HANDBOOK) 14
SPECIFIC ANNEX 4 - OPERATIONAL BRIEFING	24
SPECIFIC ANNEX 5 - COMMAND AND CONTROL SCHEME	25
SPECIFIC ANNEX 6 - JORA	26
SPECIFIC ANNEX 7 - CONTACT DETAILS - FRONTEX	30
SPECIFIC ANNEX 8 - AIRPORT ORGANISATIONAL CONTACT DETAILS	31
SPECIFIC ANNEX 9 - INITIAL DEPLOYMENT LIST	33
SPECIFIC ANNEX 10 - RULES OF ENGAGEMENT (FRANCE)	34



SPECIFIC ANNEX 1 - DESCRIPTION AND ASSESSMENT OF THE SITUATION

1.1 Introduction

Joint Operation Alexis 2015 has been conceived to support Schengen and Schengen Associated Country airports in respect of their own perceived vulnerabilities/needs concerning operational activities

The process by which airports have identified these and the methodology for the selection of common vulnerabilities needs to which Frontex provides the requisite operational support is described in detail in the Operational Plan.

Airports in conjunction with Joint operation Unit Air Border Sector decided to select the following as their vulnerabilities/needs where a joint activity could be launched in participating airports with the provision of appropriate human assets:

- Transit without Visa Abuse
- Document abuse

This briefing document has been created in order to provide an overview of the risks and threats presented at the external air borders of the EU in respect of the above identified vulnerabilities/needs.

The document will assess the general threat and risks as well as the more specific ones associated with the airports which have agreed to participate or are considering their participation in the operation at the time of the drafting of this document.

1.2 Airports in the operational area

The following airports have agreed or are considered as participating in the Joint Operation at the time that this document was created:

•	Amsterdam	(AMS)
•	Barcelona	(BCN)
•	Bucharest	(OTP)
•	Budapest	(BUD)
•	Dusseldorf	(DUS)
•	Geneva	(GVA)
•	Helsinki	(HEL)
•	Lisbon	(LIS)
•	Lyon	(LYS)
•	Madrid	(MAD)
•	Marseille	(MRS)
•	Paris	(ORY)
•	Paris	(CDG)
•	Porto	(OPO)
•	Prague	(PRG)
•	Riga	(RIX)
•	Sofia	(SOF)
•	Stockholm	(ARN)
•	Tallinn	(TLL)
•	Timisoara	(TSR)
•	Varna	(VAR)
•	Vienna	(VIE)
•	Vilnius	(VNO)
•	Warsaw	(WAW)

Zurich

(ZRH)



1.3 Data sources and measurable indicators

The following indicators can be measured by reference to Pulsar Data for all the above airports except Paris Orly (ORY), Marseille (MRS), Lyon (LYS), Varna (VAR) and Timisoara (TSR) which do not currently report in Pulsar.

In addition, Spanish airports, such as Barcelona (BCN) and Madrid, (MAD) do not provide information in Pulsar relating to abused documentation to be analysed for risk analysis.

- Transit without Visa Abuse
 - Is not measured in the collection process, but is effectively a consequence of documents swapping and transit without visa abuse.
- Document Abuse

Pulsar Data is taken for the whole period 01.01.2014 to 12.03.2015

1.4 General overview of the EU's external borders in respect of identified vulnerabilities / needs

Transit without Visa Abuse (TWOV)

Commented [A1]: The blanked out parts contain detailed information regarding vulnerabilities and needs at the EU's external borders. Its disclosure would jeopardize the work of law enforcement officers that relies on such information, and harm the course of future and ongoing operations, thus facilitating 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.



Counter Measures



Document Abuse

The abuse or miss- use of documentation is one of the greatest threats to the air borders.

In 2014, there were **19015 abused or mi-used documents detected**¹. Below is a list of the extent of the abuse:

Abused travel documents at Air Borders in 2014	
AUTHENTIC	3632
AUTH-FRAUD OBT	636
AUTH-IMPOSTOR	2996
COUNTERFEIT	7925
FALSE-COUNTERFEIT	7925
FORGED	4885
FALSE-BIOPAGE	984
FALSE-E-DEVICE	11
FALSE-FORGED	111
FALSE-IMAGE SUB	1613
FALSE-MUTIL	334
FALSE-NEW BIOPAGE	838
FALSE-OTHER	695
FALSE-PAGESUB	299
NO MORE DETAILS	1494
FALSE-NO MORE DETAILS	1494
Other	6
AUTH-FRAUD OBT	2
FALSE-BIOPAGE	1
FALSE-NEW BIOPAGE	1

¹ Frontex European Fraud Document (EDF) data 2014

Commented [A2]: The blanked out parts contain detailed information regarding the measures to be taken by law enforcement officers based on the vulnerabilities and needs at the EU's external borders in the previous section. This would weaken similar current and future operations by depriving them of an element of surprise. This in turn would facilitate irregular migration and therefore affect public security. 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.

Commented [A3]: The blanked out parts contain detailed information regarding vulnerabilities and needs at the EU's external borders. Its disclosure would jeopardize the work of law enforcement officials that relies on such information, and harm the course of future and ongoing operations, thus facilitating 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.



FALSE-NO MORE DETAILS	1
FALSE-OTHER	1
OUT OF SCOPE	9
OUT OF SCOPE	9
PSEUDO	11
FALSE-PSEUDO	11
STOLEN BLANK	1053
FALSE-STOLEN BLANK	1053
Grand Total	19015



1.5 Airports



Commented [A4]: The blanked out parts contain detailed analytical findings on the modus operandi of criminal networks and clandestine activities of various individuals per each airport. Their disclosure would be tantamount to releasing pieces of intelligence gathered by law enforcement officials to tackle irregular migration, as well as their follow up actions. The operation would lose its element of surprise. This would weaken similar current and future operations and facilitate irregular migration. 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.





Commented [A5]: The blanked out parts contain detailed analytical findings on the modus operandi of criminal networks and clandestine activities of various individuals per each airport .Their disclosure would be tantamount to releasing pieces of intelligence gathered by law enforcement officials to tackle irregular migration, as well as their follow up actions. The operation would lose its element of surprise. This would weaken similar current and future operations and facilitate irregular migration. 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.

Commented [A6]: The blanked out parts contain detailed analytical findings on the modus operandi of criminal networks and clandestine activities of various individuals per each airport. Their disclosure would be tantamount to releasing pieces of intelligence gathered by law enforcement officials to tackle irregular migration, as well as their follow up actions. The operation would lose its element of surprise. This would weaken similar current and future operations and facilitate irregular migration. 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.

² 12 cases of Syrian migrants in possession of false travel documents were reported in PULSAR over the period from 01-01-2014 to 12-03-2015.

 $^{^{\}rm 3}$ 80 % of the total reported on PULSAR over the period From 01-01-2014 to 12-03-2015



Dusseldorf (DUS) Geneva (GVA)

Commented [A7]: The blanked out parts contain detailed analytical findings on the modus operandi of criminal networks and clandestine activities of various individuals per each airport .Their disclosure would be tantamount to releasing pieces of intelligence gathered by law enforcement officials to tackle irregular migration, as well as their follow up actions. The operation would lose its element of surprise. This would weaken similar current and future operations and facilitate irregular migration. 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.

⁴ From 01-01-2014 to 12-03-2015 (Pulsar data collection)



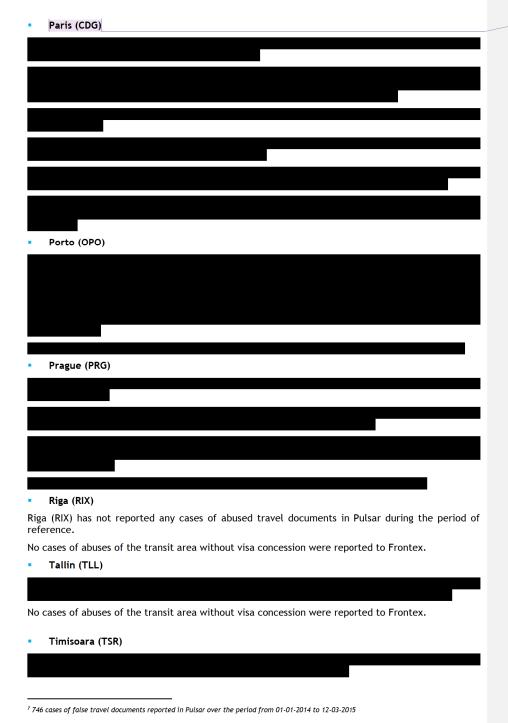
Helsinki (HEL)

 $^{\rm 5}$ From 01-01-2015 to 20-03-2015 (Pulsar data collection)

 $^{\rm 6}$ 6 cases reported in Pulsar over the period from 01-01-2014 to 12-03-2015

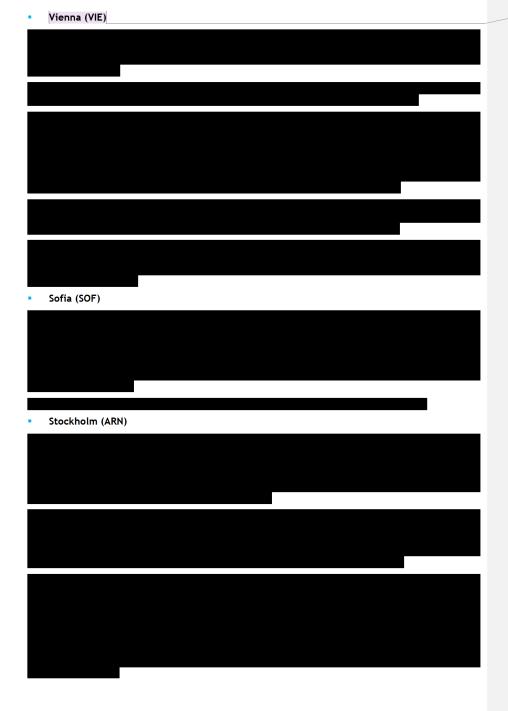
Lisbon (LIS) Lyon (LYS) Lyon airport does not report data in Pulsar. Madrid (MAD) Marseille (MRS) Marseille airport does not report data in Pulsar. Paris Orly (ORY) Paris Orly (ORY) airport does not report data in Pulsar. Commented [A8]: The blanked out parts contain detailed analytical findings on the modus operandi of criminal networks and clandestine activities of various individuals per each airport .Their disclosure would be tantamount to releasing pieces of intelligence gathered by law enforcement officials to tackle irregular migration, as well as their follow up actions. The operation would lose its element of surprise. This would weaken similar current and future operations and facilitate irregular migration. 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.





Commented [A9]: The blanked out parts contain detailed analytical findings on the modus operandi of criminal networks and clandestine activities of various individuals per each airport .Their disclosure would be tantamount to releasing pieces of intelligence gathered by law enforcement officials to tackle irregular migration, as well as their follow up actions. The operation would lose its element of surprise. This would weaken similar current and future operations and facilitate irregular migration. 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.





Commented [A10]: The blanked out parts contain detailed analytical findings on the modus operandi of criminal networks and clandestine activities of various individuals per each airport .Their disclosure would be tantamount to releasing pieces of intelligence gathered by law enforcement officials to tackle irregular migration, as well as their follow up actions. The operation would lose its element of surprise. This would weaken similar current and future operations and facilitate irregular migration. 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.



Varna (VAR)

Varna airport (VAR) does not report data in Pulsar.

Vilnius (VNO)



No cases of abuses of the transit area without visa concession were reported to Frontex.

Warsaw (WAW)



SPECIFIC ANNEX 2 - OPERATIONAL OBJECTIVES AND INDICATORS

Under the umbrella of the Frontex Programme of Work 2015 this activity contributes to the following corporate goals and prioritized key objectives, as set in the Frontex' Strategy and MAP 2014 - 2017 as well as in concrete in PoW 2015:

- Goal 2: Supporting response, Key Objective nr. 1: Coordinate multipurpose joint activities that sustain the operational presence in areas at the external borders exposed to specific and disproportionate pressure as well as facing significant uncertainties; including consistent action in line with operational reaction mechanism laid down in the EUROSUR Regulation; (str.42)
- Goal 3: Emergency response, Key Objective nr. 1: Develop operational contingency modules in the event of emergency situations by reinforcing/modifying ongoing operational activities or launching new joint operations thus ensuring agility and flexibility and efficient use of resources;

The objectives of the activity are as follows:

- 1. Enhance exchange of knowledge among officers (Frontex, MS/SAC & Third Countries)
- 2. Enhance border security (Frontex, MS & SAC)
- 3. Enhance efficiency of border security (Frontex, MS & SAC)
- 4. Enhance operational cooperation (Frontex, MS/SAC & Third Countries)

 $\textbf{Commented [A11]:} \ \ \textbf{The blanked out parts contain detailed}$ analytical findings on the modus operandi of criminal networks and clandestine activities of various individuals per each airport .Their disclosure would be tantamount to releasing pieces of intelligence gathered by law enforcement officials to tackle irregular migration, as well as their follow up actions. The operation would lose its element of surprise. This would weaken similar current and future operations and facilitate irregular migration. 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.



This activity is expected to deliver the following main benefits:

Tailored operational support and capacity building strengthening MS/SAC operational capabilities on perceived vulnerabilities/needs.

Effective and efficient operational response to perceived vulnerabilities meeting existing threats indications (European Situational Awareness) in order to enhance security of external air borders.

Increased response capacity to emergency situations.

The objectives are meant to be achieved by the following activities:

Objective of the activity	Activity	Indicators of achievement	Expected output
Nr. 1: Enhance exchange of knowledge among officers (Frontex, MS/SAC & Third Countries)	Deployment of guest officers, seconded guest officers and TC observers	Number of MS/SAC and Third Countries participating in the JO Number of man-days deployed during the operation	At least 15 MS/SAC and 3 Third Countries participating in the JO At least 800 GOs man-days deployed in course of the activities At least 90 SGOs man-days deployed in course of the activities At least 60 TC observers mandays deployed in course of the activities
Nr. 2: Enhance border security (Frontex & MS/SAC)	Supporting targeted response focusing on perceived vulnerabilities/n eeds	Number of reinforcing actions (e.g. gate check, doc checks with Ref Man experts or any other action what the particular vulnerability requires)	At least 8.000 reinforcing actions by participating airports in accordance to countermeasures suggested in the Standard Operational Procedures
Nr. 3: Enhance efficiency of border security (Frontex & MS/SAC)	Implementing coordinated operational actions according to the operational plan	Number of airports participating	At least 20 participating airports
Nr. 4: Enhance operational cooperation (Frontex, MS/SAC & Third Countries)	Deployment of officers with specific profile ⁸	Number of man-days of requested specific profile officers deployed during the operation	At least 800 man-days of requested specific profile officers deployed in course of the activities

 $^{^{8}}$ Corresponding to the tackled vulnerabilities and in line with the MB decision nr. 11/2012.



SPECIFIC ANNEX 3 - STANDARD OPERATIONAL PROCEDURES (SOP) ON THE BASIS OF VEGA HANDBOOK

The aim of JO Alexis I 2015 is to enhance document expertise of EU airport border guards, as well as enhancing their capabilities to detect and react on abuses related to transits to/from Third Countries by applying the following Standard Operational Procedures according to need.

Document fraud allows migrants to enter the territory of the Member States illegally and to enjoy free movement in Europe, which also allows freedom of movement to members of criminal networks. Frontex has seen an increase in cases of impersonation in EU/SAC countries. Moreover the detection of counterfeit and forged passports, ID cards and Driving Licenses has also increased more than usual in recent years.

The use of fake or fraudulently obtained breeder documents is growing and makes the detection of the fraudulent issued documents more difficult, mainly ID Cards and Passports. Perspicacity is needed to detect these kinds of forgeries, which are more difficult when we are dealing with EU/SAC Countries documents.

Fraudulent identity and secure documents are often used for the smuggling of migrants, trafficking in persons, terrorist mobility and frauds.

1.1. Definitions for the purpose of JO Alexis I

Categories of documents

Secure documents

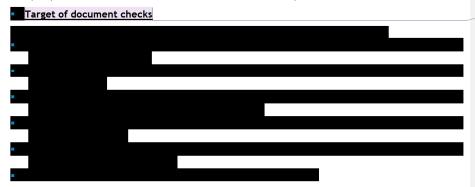
Documents that have incorporated security features to protect their value and prevent fraud abuse. In this regard, many documents such as passports, identity cards, residence permits, travel visas and driving licenses contain security features.

Identity documents

These are documents which may be used to verify aspects of personal identity. Many countries issue identity cards for this reason; however others may accept a driver's license as an effective proof of identity.

Breeder documents

A breeder document is used as a basis to obtain another one such as an identity card, a driving licence or a passport. Most breeder documents do not have the security features of secure documents.



Commented [A12]: The blanked out parts contain detailed information regarding document abuse at Schengen and non-Schengen airports with detailed data on the modus operandi of criminal networks. Its disclosure would jeopardize the work of law enforcement officials 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.

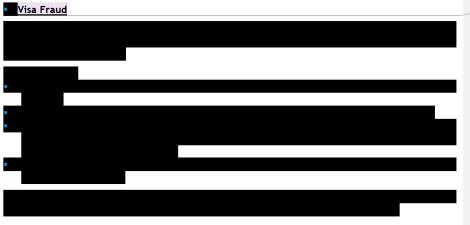




Commented [A13]: The blanked out parts contain detailed information regarding document abuse at Schengen and non-Schengen airports with detailed data on the modus operandi of criminal networks. Its disclosure would jeopardize the work of law enforcement officials and harm the course of future and ongoing 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.

Miss-issued documents

Those travel documents issued by mistake by the issuing authorities. There is not fraudulent activity behind it and they are rarely encountered at border checks, but it is important to detect mistakes made by the issuing authorities in order to inform them or the other Frontex partners as soon as possible.



Commented [A14]: The blanked out parts contain detailed information regarding document abuse at Schengen and non-Schengen airports with detailed data on the modus operandi of criminal networks. Its disclosure would jeopardize the work of law enforcement officials 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.

Improperly Documented passenger

Improperly documented passenger: traveller who does not hold documents specified by the State as required for entry or transit on that State.

Fraudulently documented: traveler using illegal means to circumvent or avoid detection during migration controls.

Impostors (also known as look-a-likes)

A person presenting or using some official travel documents originally issued to another person. Such persons use normally genuine travel documents and are also considered undocumented upon arrival.

Commented [A15]: The blanked out parts contain detailed information regarding document abuse at Schengen and non-Schengen airports with detailed data on the modus operandi of criminal networks. Its disclosure would jeopardize the work of law enforcement officers 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.





Undocumented passengers

Undocumented passenger: except in isolated cases, is a passenger that deliberately disposed of the travel document after passing through the operating carrier's screening process.

Transit Without Visa Abuse - TWOV (first transit and transit on the flights back)

Abuse of the concession given to some nationalities to travel from one Third Country to another Third Country via an EU or Schengen Associated Country airport without a visa.



No Shows

A passenger in transit with a connecting flight on which he/she is recorded that does not take his/her flight. The name given by airlines is "NO SHOW" on his connecting flight.

Swapping in Schengen and in non-Schengen airports

Using a false document is a risk for an irregular passenger. For this reason, the irregular migrant will continue to use his or her genuine document for as long as possible. Therefore, migrants will generally depart with genuine documents.

Commented [A16]: The blanked out parts contain detailed information regarding document abuse at Schengen and non-Schengen airports with detailed data on the modus operandi of criminal networks. Its disclosure would jeopardize the work of law enforcement officers 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.



1.2. Basic Indicators
•
•
•
· · <u> </u>
•
•
•
•
•

Commented [A17]: The blanked out parts contain detailed information regarding criteria to identify migrants' facilitators and traffickers of human beings. Its disclosure would jeopardize the work of law enforcement officers 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.



•		
•		
•		
•		
•		
•		
•		
•		

1.3. Alexis I Standard Operational Procedures (SOP)

Whatever type of border control is carried out, it should be done fully respecting human dignity.

Based on the VEGA handbook (uploaded in FOSS) the following recommended operational procedures and countermeasures enhance capabilities to detect the above listed transit area abuses in the short term period.

Gate checks on Arrivals



Commented [A18]: The blanked out parts contain detailed information on the methods and measures taken by law enforcement officers during border control and specifically regarding gate checks at the air borders. Its disclosure would expose the work of law enforcement officers and harm the course of future and ongoing operations, thus facilitating 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.

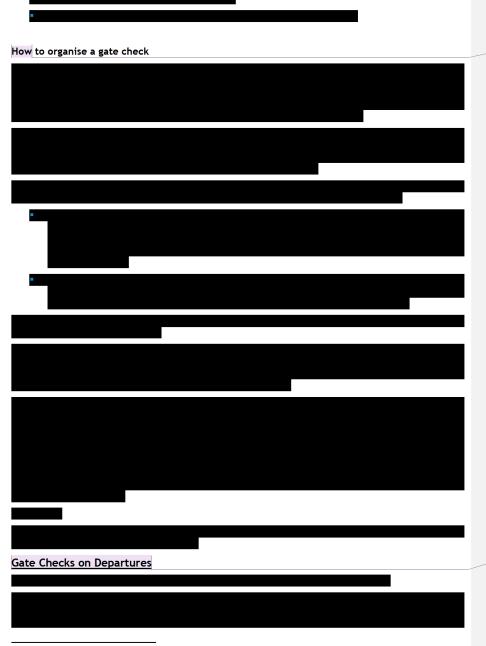
⁹ <u>Legal Basis:</u> Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data. At this stage, it should be highlighted that since the Council Directive required Member States to enact legislation in order to adopt and bring this Directive into force, its implementation may vary from Member State to Member State.

¹⁰ Passenger Name Record: databases are owned by airlines and can be accessed by law enforcement authorities upon national legislation. There is no European Union law available on PNR yet.

 $^{^{\}scriptsize \text{II}}$ A person who is refused entry in to, or transit through the Territory of a State by the authorities of that Stat.





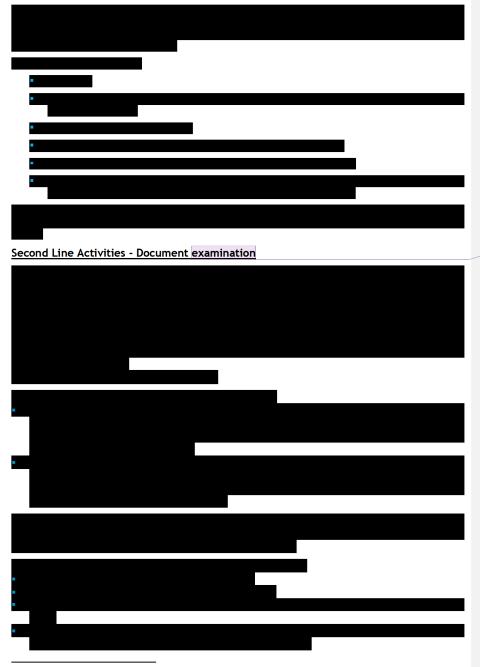


 $^{^{12}}$ Passenger Name Record: databases are owned by airlines and can be accessed by law enforcement authorities upon national legislation. There is no European Union law available on PNR yet.

Commented [A19]: The blanked out parts contain detailed information on the methods and measures taken by law enforcement officers during border control and specifically regarding gate checks at the air borders. Its disclosure would expose the work of law enforcement officers and harm the course of future and ongoing operations, thus facilitating 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.

Commented [A20]: The blanked out parts contain detailed information on the methods and measures taken by law enforcement officers during border control and specifically regarding gate checks at the air borders. Its disclosure would expose the work of law enforcement officers and harm the course of future and ongoing operations, thus facilitating 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.



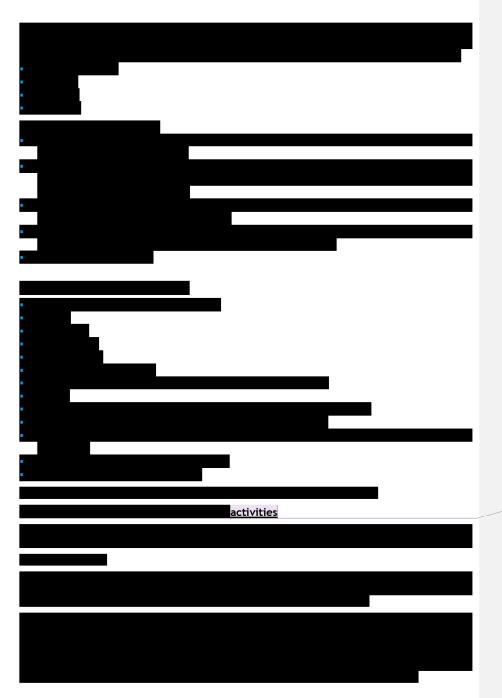


Commented [A21]: The blanked out parts contain detailed information on the methods and measures taken by law enforcement officers during border control and specifically regarding document examination at the air borders. Its disclosure would expose the work of law enforcement officers and harm the course of future and ongoing operations, thus facilitating 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.

 $^{^{13}}$ Passenger Name Record: databases are owned by airlines and can be accessed by law enforcement authorities upon national legislation. There is no European Union law available on PNR yet.

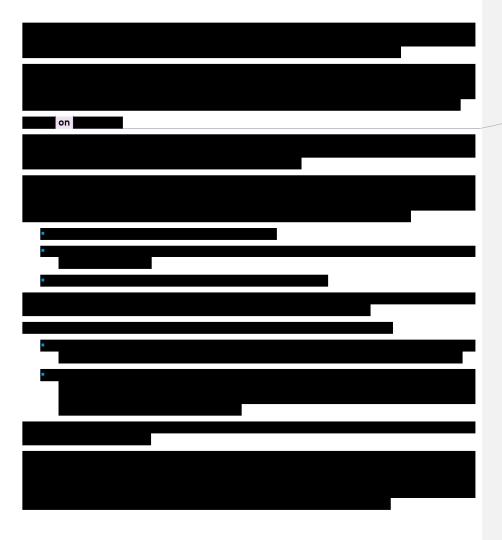
 $^{^{14}}$ Schengen Border Code, Regulation (EC) $\frac{1}{5}$ 62/2006 of the European Parliament and of the Council of 15 March 2006, art. 7(5).





Commented [A22]: The blanked out parts contain detailed information on the modus operandi of facilitators, as well as on the methods and measures taken by law enforcement officers during border control at the air borders. Its disclosure would expose the work of law enforcement officers and harm the course of future and ongoing operations, thus facilitating 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.





Commented [A23]: The blanked out parts contain detailed information on the modus operandi of facilitators, as well as on the methods and measures taken by law enforcement officers during border control at the air borders. Its disclosure would expose the work of law enforcement officers and harm the course of future and ongoing operations, thus facilitating 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.

¹⁵ Passenger Name Record: databases are owned by airlines and can be accessed by law enforcement authorities upon national legislation. There is no European Union law available on PNR yet.



SPECIFIC ANNEX 4 - OPERATIONAL BRIEFING

During the first days of deployment all participants from MS and observers from Third Countries will receive the Operational Briefing delivered by Frontex and national authorities of the host MS.

General briefing delivered by Frontex

The General briefing is a part of Operational briefing carried out by Frontex.

All participants of the joint operation will be briefed by an Air Border Sector team member at the beginning of their deployment. In exceptional cases, if respective participants are not available for the centralized Operational briefing, the briefing will be delivered on the spot.

More detailed information about the General briefing delivered by Frontex during JO Alexis I 2015 are in the Main part of the operational plan (Chapter 5.2).

National briefing delivered by host MS and host TC

The National briefing is a part of Operational briefing carried out by national authorities of host Member State and Third Country (airport representatives) based on the deployment overviews provided by Joint Operations Unit (JOU).

The National briefers (airport representatives) are responsible for carrying out National briefings, based on the Common Briefing Pack, for all participants deployed within JO. The content and the structure of the Common Briefing Pack are provided by Frontex Training Unit. The National briefers should deliver the National briefing at their airport to the guest officers, seconded guest officers and observers from Third Countries during the first day of the deployment National briefer shall:

- Deliver briefings as requested by the deployment overviews.
- Report to the project manager of Frontex Training Unit (Please, see the Specific Annex 5 and 7) and in copy to
 any irregularities regarding briefings carried out.
- Support the development process of training courses, tools and materials, including the implementation process of such activities.
- Prepare Report of National Briefer after each activity and submit it to the project manager (Frontex Training Unit).
- Assist in preparing assessments and evaluations of the operational activities.

A standard plan for operational briefing and debriefing is available in the General Annex of the Operational Plan.

Commented [A24]: The blanked out part contains information related to a means of communication used by law enforcement officers. Its disclosure would lead to possible abusive usage and harm the course of future and ongoing operations, thus facilitating 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.



SPECIFIC ANNEX 5 - COMMAND AND CONTROL SCHEME

Operational Management and Operational team
Area Manager (AM) for joint operations:
Operational Manager (OM):
Operational Team (OT):
Frontex Coordinating Officers (FCO):
Operational Analyst (OA):
Training Unit for Road Shows:
Training Unit for National Briefings:
 Pooled Resources Unit: OPERA team
 Frontex Situation Centre (FSC)
- Senior Duty Officer (SDO)
- Frontex Support Officer (FSO FSC)
- FOSS Service Managers
 JORA Service Managers

Commented [A25]: The non-disclosed text contains the names of actors participating in Frontex activities. The disclosure of such information would undermine the protection of the privacy and the integrity of the individuals, in particular in accordance with EU laws regarding the protection of personal data. In this regard the text is not disclosed pursuant to the exception laid down in Article 4(1)(b) of Regulation (EC) 1049/2001.



SPECIFIC ANNEX 6 - JORA

1. JORA Actors

Role	Name	FX/MS	Entity	E-mail	Phone
JORA Administrator / Service		Frontex	FSC		
Management		Frontex	FSC		
Frontex Access Manager		Frontex	ABS		
Delegated Frontex Access Manager		Frontex	ABS		
Template Creator		Frontex	RAU		
National Access Manager		Austria	MS		
National Access Manager		Bulgaria	MS		
National Access Manager		Czech Republic	MS		
National Access Manager	T	Denmark	MS		
National Access Manager		Estonia	Police and Border Guard Board/NFPOC		
National Access Manager		Finland	MS		
National Access Manager		France	MS		
National Access Manager		France	Marseille		
National Access Manager		France	Lyon		
National Access Manager		Germany	MS		

Commented [A26]: The blanked out parts contain the names and contact details of actors participating in Frontex activities. The disclosure of such information would undermine the protection of the privacy and the integrity of the individuals, in particular in accordance with EU laws regarding the protection of personal data. In this regard those parts are not disclosed pursuant to the exception laid down in Article 4(1)(b) of Regulation (EC) 1049/2001.

The blanked out parts also contain information related to means of communication used by law enforcement officers. 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.

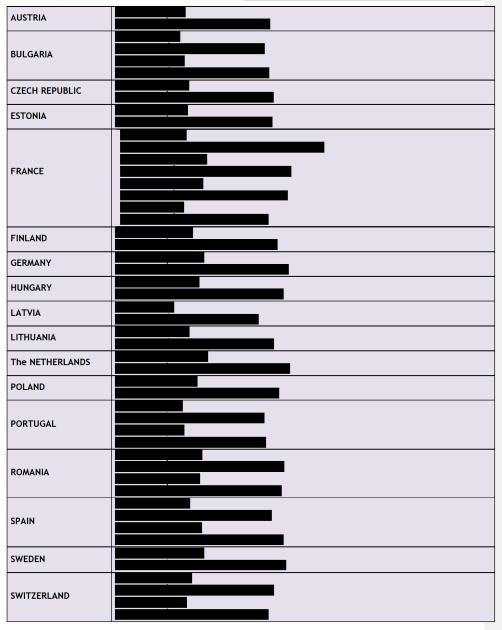


	l	I	I	I	
National Access Manager		Hungary	MS		
National Access Manager		Latvia	MS		
National Access Manager		Lithuania	MS		
National Access Manager		Luxembourg	PGD		
National Access Manager		Netherlands	MS		
National Access Manager		Netherlands	MS		
National Access Manager		Netherlands	MS		
National Access Manager		Norway	MS		
National Access Manager		Poland	MS		
National Access Manager		Portugal	MS		
National Access Manager		Romania	MS		
National Access Manager		Slovenia	MS		
National Access Manager		Slovenia	MS		
National Access Manager		Spain	MS		
National Access Manager		Spain	MS		
National Access Manager		Sweden	MS		
National Access Manager		Switzerland	SAC		
National Access Manager		United Kingdom	NFPOC		

NOTE: Detailed roles and responsibilities of the different actors are described in the JORA Policy and Process business documentation



2. JORA Incidents Reporting Structure



Commented [A27]: The blanked out parts contain information regarding the reporting mechanisms of law enforcement engaged in the operation. Its disclosure would expose elements of their work and harm the course of future and ongoing operations, thus facilitating irregular migration and criminal activities. 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.



3. JORA INCIDENT TEMPLATE ATTRIBUTES' LIST

JORA Attribute	Required	Description
[Incident Number]	(*)	Data set by the JORA
[Reporting Unit]	(*)	Information set by the JORA
[Date of Reporting]	(*)	Date set by the JORA
Guest Officer involved		yes/not
1.Arrivals gates: number of gate checks implemented in line with SOP		amount
2.Departure gates: number of gate checks implemented in line with SOP		amount
3. Second line: number of document checks implemented in line with SOP		amount
4.Transit area: number of targeted and non-targeted activities implemented in line with SOP		amount
5.Deployed officers: number of times they participated in the aforementioned activities		amount
6.Modus operandi		Free text
7. Comments		Free text



SPECIFIC ANNEX 7 - CONTACT DETAILS - FRONTEX

1. General

Authority	Address	Email address
Frontex (HQ)	Plac Europejski 6, 00-844 Warsaw, Poland	frontex@frontex.europa.eu
Frontex Situation Centre	Plac Europejski 6, 00-844 Warsaw, Poland	
Alexis Operational Team	Plac Europejski 6, 00-844 Warsaw, Poland	
OPERA team	Plac Europejski 6, 00-844 Warsaw, Poland	
JORA team	Plac Europejski 6, 00-844 Warsaw, Poland	
FOSS team	Plac Europejski 6, 00-844 Warsaw, Poland	

Commented [A28]: The blanked out parts contain detailed information related to means of communication used by law enforcement officers. Their disclosure would lead to possible abusive usage and harm the course of future and ongoing operations, thus facilitating 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.

2. Frontex

Role	Name	Phone number	Email address	
Area Manager for joint operations				
Operational Manager				
Operational Team Member				
Frontex Coordinating Officers				
Operational Analyst				
Frontex Training Unit				
Frontex Training Unit				
Spokesperson	Izabella Cooper	+48 667 667 292	izabella.cooper@frontex.europa.eu	
Press Officer	Ewa Moncure	+48 785 001 374	ewa.moncure@frontex.europa.eu	

Commented [A29]: The blanked out parts contain the names and contact details of actors participating in Frontex activities. The disclosure of such information would undermine the protection of the privacy and the integrity of the individuals, in particular in accordance with EU laws regarding the protection of personal data. In this regard those parts are not disclosed pursuant to the exception laid down in Article 4(1)(b) of Regulation (EC) 1049/2001.

REMARK:

Any changes related to the contact details of the participants in the course of the joint operation do not require the amendment of the Operational Plan. The updated contact details will be available and shared with the participants during implementation phase on a need to know basis.



SPECIFIC ANNEX 8 - AIRPORT ORGANISATIONAL CONTACT DETAILS

Country	Airport	Airport Contact Person	Email	Telephone	Mobile
Austria	Vienna (VIE)				
Austria	Vienna (VIE)				I
Austria	Vienna (VIE)				
Bulgaria	Sofia (SOF)				
Bulgaria	Varna (VAR)				
Czech	Prague				
Republic	(PRG)				
Czech	Prague				
Republic	(PRG)				
Estonia	Tallinn				
	(TLL)				
Estonia	Tallinn				
Finland	(TLL) Helsinki				
FIIIIaliu	(HEL)				
Finland	Helsinki				
Tilland	(HEL)				
Finland	Helsinki				
	(HEL)	_			
Finland	Helsinki				
	(HEL)				
France	Marseille				
France	(MRS) Marseille				
rrance	(MRS)				
France	Paris				
	(CDG)				
France	Paris				
	(CDG)				
France	Paris (ORY)				
France	Paris (ORY)				
France	Lyon (LYS)				
France	Lyon (LYS)				
Germany	Dusseldorf				
	(DUS)				
Germany	Dusseldorf				
,	(DUS)				
Hungary	Budapest				
	(BUD)				

Commented [A30]: The blanked out parts contain the names and contact details of actors participating in Frontex activities. The disclosure of such information would undermine the protection of the privacy and the integrity of the individuals, in particular in accordance with EU laws regarding the protection of personal data. In this regard those parts are not disclosed pursuant to the exception laid down in Article 4(1)(b) of Regulation (EC) 1049/2001.



Hungary	Budapest (BUD)		I
Latvia	Riga (RIX)		
Latvia	Riga (RIX)		
Lithuania	Vilnius (VNO)		
Lithuania	Vilnius (VNO)		
Netherlands	Amsterdam (AMS)		
Poland	Warsaw (WAW)		
Portugal	Lisbon (LIS)		
Portugal	Porto (OPO)		
Portugal	Porto (OPO)		
Romania	Bucharest (OTP)		
Romania	Bucharest (OTP)		
Romania	Timisoara (TSR)		
Romania	Timisoara (TSR)		
Spain	Barcelona (BCN)		
Spain	Madrid (MAD)		
Sweden	Stockholm (ARN)		
Switzerland	Zurich (ZRH)		
Switzerland	Geneva (GVA)		
Switzerland	Geneva		



SPECIFIC ANNEX 9 - INITIAL DEPLOYMENT LIST

Available on a separate sheet.



SPECIFIC ANNEX 10 - RULES OF ENGAGEMENT (FRANCE)

Following the terrorist attacks faced by France at beginning of January 2015 and due to the continuously high terror threat in public places, at the beginning of March 2015 France recommend that guest officers deployed at French airports are deployed with service weapons and bullets proof vests.

<u>Description of the tasks and special instructions for the members of the EBGT¹⁶</u>

1) Use of force/weapons

(a) Define the principles on the use of force

When using force, members of the EBGTs shall not exceed the minimum degree that is necessary, proportional and reasonable in the circumstances. When deployed in France, members of the EBGTs may apply direct coercion (i.e. physical force, special equipment) only in legitimate self-defense and in legitimate defence of other persons.

To act within the context of self-defense or defence of the others:

- 1. Aggression shall to be:
- -Actual: the danger is imminent
- -Illegal: the aggression is illegal (riposte to police forces during a demonstration cannot be considered as self-defense)
- -Real: the aggression should not be reputed imaginary or thought to be possible
 - 2. Defence shall to be:
- -Necessary: there is no other means to escape the danger
- -Concomitant: the reaction must be immediate, for example: we do not have to act out of revenge or with the aim of stopping the runaway aggressor
- -Proportionate to the aggression : the reaction must not be excessive
 - (b) Define the principles on the use of weapons

Weapon and bullets shall not be carried off duty must be stored in the police safe foreseen for it at the end of each shift.

The use of firearms, as it may affect the life or health of persons is the last resource of the actions of guest officials. Firearms may only be used in case of legitimate self-defense and in legitimate defence of other persons.

To use of firearms within the context of self-defense or defence of the others:

- 1. Aggression shall to be:
- -Actual: the danger is imminent
- -Illegal: the aggression is illegal (riposte to police forces during a demonstration cannot be considered as self-defense)
- -Real: the aggression should not be reputed imaginary or thought to be possible
 - 2. Defence (the use of the weapon) shall to be:

 $^{^{16}}$ Pursuant to the provision of Article 3a(d) of the Frontex Regulation



-Necessary: there is no other means to escape the danger

-Concomitant: the reaction must be immediate, for example: we do not have to act out of revenge or with the aim of stopping the runaway aggressor

-Proportionate to the aggression : the reaction must not be excessive

(c) Define the type of equipment/weapons permissible

Members of the EBGTs from a competent authority of another Member State that is involved in police or customs activity under an international agreement or a legislative act of the European Union may carry firearms (handguns), cut-and-thrust weapons (batons and telescopic batons). Gas weapons or pneumatic weapons cannot be carried by members of the EBGTs deployed in France.

- (d) Define the conditions to use coercive measures/weapons (warnings, targets, etc.)
- Handcuffs: Handcuffs might be carried by the GO as it might be useful in case of use of force. However,
 Nobody can be handcuffed unless he is considered dangerous to himself or others [...] (Art.803 Criminal Procedure Code),

The usefulness of handcuffing is under the responsibility of the French police officer accompanying the GO. Handcuff should be wisely and applies the principle of proportionality depending of the person: age, health, seriousness of the offense. Do respect the dignity. Handcuffing is prohibited for minors under thirteen years old. (DGPN Instructions $n^{\circ}04$ -10464 du 13/09/2004)

- cut-and-thrust weapons (batons and telescopic batons): The use of force including use of cut-andthrust weapons (batons and telescopic batons) is only allowed within the context of self-defense or defence of the others:
 - (i) Aggression shall to be:

-Actual: the danger is imminent

-Illegal: the aggression is illegal (riposte to police forces during a demonstration cannot be considered as self-defense)

-Real: the aggression should not be reputed imaginary or thought to be possible

(ii) Defence (the use of the weapon) shall to be:

-Necessary: there is no other means to escape the danger

-Concomitant: the reaction must be immediate, for example: we do not have to act out of revenge or with the aim of stopping the runaway aggressor

 $\hbox{-} \textbf{\textit{Proportionate}} \ to \ the \ aggression: the \ reaction \ must \ not \ be \ excessive$

- (e) Define the immediate measures to be taken following the use of coercive measure/weapons
- The health of those involved in a use of force case is the priority as soon as the assault ended. In this
 context medical examinations of all persons involved are highly recommended.
- In accordance with the Article 10c COUNCIL REGULATION (EC) No 2007/2004 « Criminal liability »,
 guest officers are treated in the same way as officials of France with regard to any criminal offences
 that might be committed against them or by them.

RELEVANT APPLICABLE LAW:



- Self-defense or defence of the others : Articles 122-4, 112-5, 122-7 Penal Code
- Use of force: Article 113-4 de l'arrêté du 6 juin 2006 portant règlement général d'emploi de la police nationale (NOR: INTC0600544A)
- Handcuff: DGPN Instructions n°04-10464 du 13/09/2004