From: [redacted]

To: [redacted]

CC: legal <legal@frontex.europa.eu>

Sent at: 20/01/10 16:38:43

Subject: RE: Frontex, prior check on Joint Return Operations, 2009-0281

Dear [redacted],

Please find attached the two documents you have requested. You will see that in order to ease the drafting should you wish to use these documents that we have used your template (e.g. *Part 1 Proceedings*, etc.) but of course these are working documents.

Your new questions sent before Christmas have also been answered.

In addition, please note that changes have been made to the doc. “further questions” ; as you know, our future operations were still under development when you received our first draft in October 2009.
The Annex (excel) has been also amended.

Inter alia :

- Frontex role : it appears that even in future operations, Frontex will still merely help the Member States who solely decide on the purposes and means (Frontex is not controller or co-controller);
- Frontex will not process medical data, merely one administrative data related to health.

Kind regards

[redacted]
On behalf [redacted]

[redacted]
Legal Adviser
****
Frontex
Rondo ONZ 1, 00-124 Warsaw, Poland
Tel: [redacted]
Fax: +48 22 544 95 01
www.frontex.europa.eu

From: [redacted]
Sent: 11 December 2009 17:13
To: [redacted]
Subject: RE: Frontex, prior check on Joint Return Operations, 2009-0281

Dear [redacted],

there are other pending questions, as folows:

1) Which data is kept for auditing purposes?

2) What is the time limit for blocking or erasure on justified legitimate request from data subejcts?

Thank you very much,

[redacted]
Legal adviser

European Data Protection Supervisor
Contrôleur Européen de la Protection des Données
[redacted]
Tel: [redacted]
Fax: 02/283.19.50
Website: www.edps.europa.eu
Mail address: Rue Wiertz 60 - MO 63
B-1047 Brussels

Office: [redacted]

January 2010

Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) concerning the "Collection of names and certain other relevant data of returnees for joint return operations (JRO)"

Brussels, (Case 2009-0281)

FRONTEX ACTING AS CO-ORGANISER

This reflects the future JRO of Member States, led by an organising Member State, assisted by Frontex acting as a co-organiser.

1. Proceedings

On 17 April 2009, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer of FRONTEX a Notification for prior checking concerning the "Collection of names and certain other relevant data of returnees and Member States (MS)/Schengen Associated Countries (SAC) officials for joint return operations (JRO)".

On 24 April, 6 July and 17 July 2009 the EDPS requested additional information from FRONTEX. The responses were received on 8 June, 16 July and 29 July 2009, respectively. ..., the EDPS sent the draft opinion to the Data Protection Officer for comments which were received on .....

2. Facts

- Purpose of processing

The collection of these data is necessary for the preparation and realization of joint return operations of the Member States, assisted by Frontex under the Frontex Regulation, in order to:
- have exact knowledge of number and identification of persons taking part in JRO;
- to provide airlines with a passenger list;
- to provide third (destination) country with a list of returnees prior to JRO as required by the country concerned;
- to know the risks linked to the returnees and for the security of the JRO;
- to know the health state of returnees in order to secure appropriate medical assistance during the JRO;
- to know if any accompanied minors take part in JRO[1];
The data are gathered by the organising MS/SAC (hereafter, "OMS"). Currently, Frontex Return Operations Sector (ROS) asks participating MS/SAC to send the data only to organising MS/SAC, not to Frontex. However, in view of the expectations and wishes expressed by the MS and EU institutions, ROS needs to gather a strictly limited number of data, in order:

[1] With regard to minors, it can be generally mentioned that their return to the country of origin depends on bilateral agreements between the MS and relevant third countries. The condition to it is existence of a family in the country of origin who will take care of a minor. But no unaccompanied minors are being transferred during JRO. Concerning the accompanied minors, there have been cases of their transfer together with their families within JRO.

1) To better fulfill and further develop the task according to Art. 9 of the Frontex Regulation;
2) To assist an OMS in compiling the aforementioned lists and updating them during the course of the JRO's preparation;
3) To be more pro-active and supportive towards the OMS;
4) To increase the effectiveness and efficiency of Frontex co-organisation of JRO;
5) Forthcoming chartering of aircrafts by Frontex (tender procedure).

- Data subjects

The data subjects concerned are the Returnees.

- Categories of data :

- surname, given name
- date of birth
- nationality
- gender
- type and validity of travel document
- returning MS/SAC

- **Security risk assessment:**
It is made by a competent authority of the MS/SAC (not violent, violent, extremely violent, suicidal) not by Frontex.

- **Administrative data related to health**
Frontex processes only a yes / no answer to the question "is this passenger fully healthy?"
An assessment is made by a competent authority of the MS/SAC, whether a person is fully healthy or not; in the latter case a participating MS/SAC should collect medical information about the health case, to be given only to the medical staff present during the JRO, in order to provide the right medical assistance. Medical records or medical arrangements are not disclosed to Frontex. Medical staff are not Frontex staff and do not report to Frontex staff. The Member States are responsible for returnees and have to ensure their physical condition is consistent with a safe return by air.
All the passengers are fit for flight.

- Information to the data subjects

The data subjects are informed by the Member States.

Frontex does not provide the data subjects with the information stipulated by Articles 11 and/ or 12 of Regulation (EC) 45/2001 by FRONTEX.

First, JRO are consequences of public law enforcement activities of the MS/SAC. All returnees are subject of individual removal orders issued by relevant competent national law enforcement authorities or courts of law. Such orders are justified by national security / public security reasons and based on national law (criminal, administrative or similar). Therefore, Article 20(1) (d) applies. Furthermore, it has to be pointed out that illegal stay in a MS/SAC can sometimes constitutes a criminal offence.

Second, when processing the data related to the health of the returnees, Article 20(1)(c) applies, since this is done in order to be able to provide appropriate medical care during the JRO.

It has to be reminded that Frontex does not process any medical data.

Finally, the data related to violent/non violent behaviour of a returnee is processed in order to protect the safety and security of the JRO and of the persons participating in it (i.e. other returnees, the escorts and other individuals). This also justifies the applicability of Article 20(1)(c).

- Procedures to grant rights of data subjects

Rights are granted to data subjects by the Member States.

FRONTEX has not foreseen specific procedures to grant data subjects rights (Articles 13 to 17 of Regulation (EC) 45/2001).

See the reasoning *supra* (Information to the data subjects)

In addition, it has to be emphasized that a potential request of a data subjects to exercise his rights under the Articles 13 to 17 of Regulation (EC) 45/2001 is likely to be deprived of its substance:

1) due to the fact that very few data are processed by Frontex
2) due to the very short length of retention of data by Frontex (see *infra*) i.e. 10 working days. When Frontex will treat the requests sent by the data subject, if any, the personal data may have already been erased, thus rendering the request without object.

- Type of processing (automated and/or manual)

The processing activity conducted is manual.

- Storage media

The storage media is digital. The data might be exceptionally received on paper (e.g. by fax). Then transformed into the digital version (scanned) and the papers would be destroyed.

- Recipient(s) of the Processing

Compiled data and possible updates are sent only to the organiser of the JRO. The data is received from the individual participating MS/SAC, but not disseminated to them mutually. There is no need to enable access to the totality of available data to all participating MS/SAC.

- Retention policy

The data is stored for the following purposes:

- organisation of JRO
- evaluation of JRO (internal within Frontex Return Operations Sector and then also together with MS/SAC)
- internal and external controls, audits.

The length of retention is uniform: the duration will be a few weeks, from the moment of receiving first data related to a concrete JRO to their destruction, depending on the complexity and scale of the JRO. When the JRO is effectively ended, the data will be deleted within 10 working days after the execution of the operation.

Exceptions: when Frontex starts chartering aircrafts, the passenger list will be kept for auditing purposes, and it will be archived for 5 years in a secure area (it means this list would not be easily accessible). The passenger list does not include the risk assessment or the medical assessment.

- Time limit to block/erase data on justified legitimate request from the data subjects

After an operation, Frontex does not need to keep the data except in exceptional circumstances, thus rendering such a request without object.

However, in case Frontex would receive a justified legitimate request from data subjects, it would be forwarded to the relevant MS with a request to answer it.

See also supra, "Procedures to grant rights to data subjects".

- Security and organisational measures

1. The building, premises, offices, rooms in use by Frontex are protected against unauthorized access by: automated access control system, guards at entrances, security checks and controls, alarm system, locks of doors.
2. The areas used by Frontex are kept under constant electronic and human surveillance.
3. All persons entering the premises of Frontex are submitted to security and access checks.
4. All Frontex staff and the Frontex guests have to be announced and registered by the administration of the building in which the Frontex offices are located. The Frontex staff has special access cards allowing them to go through the turnstiles on the ground floor of the administrative building, in order to reach the elevators. The Frontex guests receive ad hoc visitors' cards, from the reception of the building situated on the ground floor, to be used to pass through the turnstiles. All the guests have to be primarily announced by Frontex to the building's administration. The area in front of the elevators is under human surveillance.
5. All offices of the ROS staff are located on the secured floor.
6. The access to this floor is additionally secured by the special entrance door which cannot be unlocked without another special access card with a photo and a name of a holder and Frontex logo. Such a card is only in possession of persons authorised by Frontex and is not being issued for ad hoc visitors. An unauthorized person has to be accompanied by Frontex staff or has to ring the doorbell in order to enter. The door is then opened by a guard and subsequently the person is accompanied by Frontex staff while staying in the area.
7. High security measures requiring iris scan are installed in front of the area of the ROS offices. The access to this highly secured area will be allowed to a limited circle of Frontex staff.
8. The office room doors have to be closed and locked when leaving the office for a longer period (e.g. participation in a meeting, after working hours etc.).
9. The computers of all Frontex staff are secured by personal usernames and passwords. The password must be changed every 74 normal days.
10. All the IT servers are located in the Server Room which is only accessible by a restricted number of Frontex staff. The physical access is protected by a physical access control system with the card reader and the iris scanner. The access to the floor with the Server Room is done through the mantrap door with another card reader and iris scanner.
11. Frontex has a back-up strategy for the IT. The ability to restore data from backups will be tested at least once per month. The offline tapes used for monthly backup will be stored in an adjacent building in a fireproof safe.

12. Deletion of e-mail, delivered to either common ROS e-mail address fjrcc@frontex.europa.eu or personal e-mail addresses of ROS staff, with personal data from the server will be made shortly (1-5 working days) after processing the message
13. Access to ROS files with the processed data in “Frontex-shared\Restricted Area\ Operations Division\Return Operations\Cooperation\Request for Assistance” only by authorised persons.

CONCLUSION:

The data necessary to set up the passenger list and to establish identity, without which it is impossible to organise the JRO, are processed by Frontex. Frontex transfers no data at all to third countries. The necessary data are transferred by the OMS.

In addition Frontex may process in the future the “security risk assessment” and *one* administrative information related to health (see *supra*, “yes/no” answer). These data are not transferred to the destination third country, neither by Frontex nor by the OMS.

January 2010

Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) concerning the "Collection of names and certain other relevant data of returnees for joint return operations (JRO)"

Brussels, (Case 2009-0281)

FRONTEX ACTING AS ASSISTANT

This reflects the 61 JRO of the Member States, already carried out with Frontex support and 26 out of them with Frontex co-financing.

1. Proceedings

On 17 April 2009, the European Data Protection Supervisor (EDPS) received from the Data Protection Officer of FRONTEX a Notification for prior checking concerning the "Collection of names and certain other relevant data of returnees and Member States (MS)/Schengen Associated Countries (SAC) officials for joint return operations (JRO)".

On 24 April, 6 July and 17 July 2009 the EDPS requested additional information from FRONTEX. The responses were received on 8 June, 16 July and 29 July 2009, respectively. ..., the EDPS sent the draft opinion to the Data Protection Officer for comments which were received on .....

2. Facts

- Purpose of processing

The collection of these data is necessary for the preparation and realization of joint return operations assisted by Frontex under the Frontex Regulation in order to:
- have exact knowledge of number and identification of persons taking part in JRO;
- to provide airlines with a passengers list;
- to provide third (destination) country with a list of returnees prior to JRO as required by the country concerned;
- to know the risks linked to the returnees and for the security of the JRO;
- to know the health state of returnees in order to secure appropriate medical assistance during the JRO;
- to know if any accompanied minors take part in JRO[1];

[1] With regard to minors it can be generally mentioned that their return to the country of origin depends on bilateral agreements between the MS and relevant third countries. The condition to it is existence of a family in the country of origin who will take care of a minor. But no unaccompanied minors are being transferred during JRO. Concerning the accompanied minors, there have been cases of their

The data are gathered by the organising MS/SAC. Currently, Frontex Return Operations Sector (ROS) asks participating MS/SAC to send the data only to organising MS/SAC (OMS), not to Frontex.

- Data subjects

The data subjects concerned are the Returnees.

- Categories of data processed by the MS, not by Frontex

The categories of personal data related to returnees are as follows:

- surname, given name
- date of birth
- nationality
- gender
- type and validity of travel document
- security risk assessment, made by a competent authority of the MS/SAC (not violent, violent, extremely violent, suicidal)
- returning MS/SAC

An assessment is made by a competent authority of the MS/SAC, whether a person is fully healthy or not; in the latter case a participating MS/SAC should collect medical information about the health case, to be given only to the medical staff present during the JRO, in order to provide the right medical assistance. Medical records or medical arrangements are not disclosed to Frontex. Medical staff are not Frontex staff and do not report to Frontex staff. The Member States are responsible for returnees and have to ensure their physical condition is consistent with a safe return by air.
All the passengers are fit for flight.

-

- Information to the data subjects

The data subjects are informed by the Member States.

As far as Frontex is concerned, acting as an assistant to the JRO without processing personal data, Frontex does not provide the data subjects with the information stipulated by Articles 11 and/or 12 of Regulation (EC) 45/2001 by FRONTEX.

- Procedures to grant rights of data subjects

Rights are granted to data subjects by the Member States.

As far as Frontex is concerned, acting as an assistant to the JRO without processing personal data, Frontex has not foreseen specific procedures to grant data subjects rights (Articles 13 to 17 of Regulation (EC) 45/2001).

- Type of processing (automated and/or manual)

transfer together with their families within JRO.

There is no processing activity from Frontex.

- Storage media

No storage.

- Recipient(s) of the Processing

Compiled data and possible updates have been sent only to the MS organizing the JRO by the individual participating MS/SAC. The OMS does not disseminate all the data to the participating MS/SAC. (there is no need to enable access to the totality of available data to all participating MS/SAC).

- Retention policy

Frontex does not retain any personal data related to a JRO, not even the passengers list.

- Time limit to block/erase data on justified legitimate request from the data subjects

See, *supra*, "Procedures to grant rights to data subjects".

- Security and organisational measures

1. The building, premises, offices, rooms in use by Frontex are protected against unauthorized access by: automated access control system, guards at entrances, security checks and controls, alarm system, locks of doors.
2. The areas used by Frontex are kept under constant electronic and human surveillance.
3. All persons entering the premises of Frontex are submitted to security and access checks.
4. All Frontex staff and the Frontex guests have to be announced and registered by the administration of the building in which the Frontex offices are located. The Frontex staff has special access cards allowing them to go through the turnstiles on the ground floor of the administrative building, in order to reach the elevators. The Frontex guests receive ad hoc visitors' cards, from the reception of the building situated on the ground floor, to be used to pass through the turnstiles. All the guests have to be primarily announced by Frontex to the building's administration. The area in front of the elevators is under human surveillance.
5. All offices of the ROS staff are located on the secured floor.
6. The access to this floor is additionally secured by the special entrance door which cannot be unlocked without another special access card with a photo and a name of a holder and Frontex logo. Such a card is only in possession of persons authorised by Frontex and is not being issued for ad hoc visitors. An unauthorized person has to be accompanied by Frontex staff or has to ring the doorbell in order to enter. The door is then opened by a guard and subsequently the person is accompanied by Frontex staff while staying in the area.
7. High security measures requiring iris scan are installed in front of the area of the ROS offices. The access to this highly secured area will be allowed to a limited circle of Frontex staff.
8. The office room doors have to be closed and locked when leaving the office for a longer period (e.g. participation in a meeting, after working hours etc.).

9. The computers of all Frontex staff are secured by personal usernames and passwords. The password must be changed every 74 normal days.
10. All the IT servers are located in the Server Room which is only accessible by a restricted number of Frontex staff. The physical access is protected by a physical access control system with the card reader and the iris scanner. The access to the floor with the Server Room is done through the mantrap door with another card reader and iris scanner.
11. Frontex has a back-up strategy for the IT. The ability to restore data from backups will be tested at least once per month. The offline tapes used for monthly backup will be stored in an adjacent building in a fireproof safe.
12. Deletion of e-mail, delivered to either common ROS e-mail address fjrcc@frontex.europa.eu or personal e-mail addresses of ROS staff, with personal data from the server will be made shortly (1-5 working days) after processing the message
13. Access to ROS files with the processed data in "Frontex-shared\Restricted Area\ Operations Division\Return Operations\Cooperation\Request for Assistance" only by authorised persons.

Returnees **from** **Annex to our ref. no:**

[1] According to the Council Decision of 29 April 2004 on the organisation of joint flights for removals from the territory of two or more Member States, of third-country nationals who are subjects of individual removal orders (2004/573/EC), Annex - Common Guidelines on Security Provisions for Joint Removals by Air, No. 1.1.2.

Medical records will be provided just to the organising Member State. They will not be disclosed to Frontex.

No.	Surname	Given Name	Date of Birth (dd/mm/yy)	Nationality	Sex (F/M)	Type of Document	Validity (dd/mm/yy)	Security risk assessment:	Health status: Is the returnee healthy?
1									☐ yes ☐ no If no, medical records will be provided in time[1].
2									☐ yes ☐ no If no, medical records will be provided in time[1].
3									☐ yes ☐ no If no, medical records will be provided in time[1].
4									☐ yes ☐ no If no, medical records will be provided in time[1].
5									☐ yes ☐ no If no, medical records will be provided in time[1].
6									☐ yes ☐ no If no, medical records will be provided in time[1].
7									☐ yes ☐ no If no, medical records will be provided in time[1].
8									☐ yes ☐ no If no, medical records will be provided in time[1].

Returnees **from** **Annex to our ref. no:**

[1] According to the Council Decision of 29 April 2004 on the organisation of joint flights for removals from the territory of two or more Member States, of third-country nationals who are subjects of individual removal orders (2004/573/EC), Annex - Common Guidelines on Security Provisions for Joint Removals by Air, No. 1.1.2.

Medical records will be provided just to the organising Member State. They will not be disclosed to Frontex.

No.	Surname	Given Name	Date of Birth (dd/mm/yy)	Nationality	Sex (F/M)	Type of Document	Validity (dd/mm/yy)	Security risk assessment:	Health status: Is the returnee healthy?
9									☐ yes ☐ no If no, medical records will be provided in time[1].
10									☐ yes ☐ no If no, medical records will be provided in time[1].
11									☐ yes ☐ no If no, medical records will be provided in time[1].
12									☐ yes ☐ no If no, medical records will be provided in time[1].
13									☐ yes ☐ no If no, medical records will be provided in time[1].
14									☐ yes ☐ no If no, medical records will be provided in time[1].
15									☐ yes ☐ no If no, medical records will be provided in time[1].
16									☐ yes ☐ no If no, medical records will be provided in time[1].

Returnees **from** **Annex to our ref. no:**

[1] According to the Council Decision of 29 April 2004 on the organisation of joint flights for removals from the territory of two or more Member States, of third-country nationals who are subjects of individual removal orders (2004/573/EC), Annex - Common Guidelines on Security Provisions for Joint Removals by Air, No. 1.1.2.

Medical records will be provided just to the organising Member State. They will not be disclosed to Frontex.

No.	Surname	Given Name	Date of Birth (dd/mm/yy)	Nationality	Sex (F/M)	Type of Document	Validity (dd/mm/yy)	Security risk assessment:	Health status: Is the returnee healthy?
17									☐ yes ☐ no If no, medical records will be provided in time[1].
18									☐ yes ☐ no If no, medical records will be provided in time[1].
19									☐ yes ☐ no If no, medical records will be provided in time[1].
20									☐ yes ☐ no If no, medical records will be provided in time[1].
21									☐ yes ☐ no If no, medical records will be provided in time[1].
22									☐ yes ☐ no If no, medical records will be provided in time[1].
23									☐ yes ☐ no If no, medical records will be provided in time[1].
24									☐ yes ☐ no If no, medical records will be provided in time[1].

Official Representatives							
No.	**Surname**	**Given Name**	**Date of Birth** (dd/mm/yy)	**Nationality**	**Sex**	**Function**	**Mobile phone**
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							

Official Representatives							
No.	**Surname**	**Given Name**	**Date of Birth** (dd/mm/yy)	**Nationality**	**Sex**	**Function**	**Mobile phone**
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							

150110 JRO_-_further_questions_3.doc

No Preview Could Be Created

The OpenDocument library function "OOoConverter::OOoConnect" returned an error (Conv_ESERVICEMANAGER).