From: [redacted]

To: [redacted]
<[redacted]

Sent at: 10/08/09 18:32:46

Subject: RE: 2009-0281 prior check

Dear [redacted],

please find attached a draft of the factual part of the Opinion for your consideration. I have added some questions. I would like to ask you not to send the answer until we have had the oportunity to discuss some other aspects on the phone. I will call you for such discussion. Please note that I will be out of the office until 17 August. We can arrange the date of the call according to your availability.

The procedure will be suspended.

Thank you very much.

Best regards,

[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]

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 and Memeber States (MS)/Schengen Associated Countries (SAC) officials for joint return operations (JRO)"

Brussels, (Case 2009-0281)

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 Memeber 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 minors take part in JRO;

The data are primarily 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, not to Frontex. However ROS need to gather the data with regard to the following reasons: 1) To better fulfil and further develop the task according to Art. 9 of the Frontex Regulation; Assistance to an organising MS/SAC in compiling the aforementioned lists and updating them during the course of the JRO's preparation on the basis of information received from participating states; 2) To have a constant overview of which participating MS/SAC have (or have not) provided the required data to the organising state which anyway regularly asks ROS to contact that that state and to provide the data in due time; 3) To increase the effectiveness and

eficienty of Frontex assistance in organising JRO of MS/SAC; 4) Future possible chartering of aircrafts by Frontex.

- Data subjects

The data subjects concerned are the Returnees and officials of MS/SAC, in particular escorts, announced by MS/SAC to take part in a joint return operation.

- Categories of data

The categories of personal data are the following:

* Data related to returnees:
- surname, given name
- date of birth
- nationality
- sex
- type and validity of travel document
- security risk assessment, made by a competent authority of the MS/SAC (not violent, violent, extremely violent, suicidal)
- medical assessment, made by a competent authority of the MS/SAC (whether a person is healthy or not; in the latter case a participating MS/SAC should provide an organising MS/SAC with medical records ; they are not being delivered to Frontex)
- returning MS/SAC

* Data related to MS/SAC' officials:
- name of the relevant MS/SAC
- surname, given name
- date of birth
- nationality
- sex
- function (medical personnel, escort leader, escort, head of operation, interpreter, observer, representative)
- mobile phone

- Information to the data subjects

The data subjects are not provided with the information stipulated by Articles 11 and/ or 12 of Regulation (EC) 45/2001 by FRONTEX.

- Procedures to grant rights of data subjects

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)

The processing activity conducted is automated.

- Storage media

- Recipient(s) of the Processing

Compiled data and possible updates are sent only to the MS organizing the JRO.

- Retention policy

From the moment of receiving first data related to a concrete JRO to their destruction the duration can be as follows, depending on the type of data, 14 – 38 months.

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

COULD YOU GIVE INFORMATION REGARDING THIS POINT?

- 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 the aforementioned special access card. 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. It is planned to install high security measures requiring iris scan 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 system to be implemented in the coming months. 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.

3. Legal aspects

3.1. Prior checking