(To be filled out in the EDPS' office)
REGISTER NUMBER: 1440

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 28/02/2017

CASE NUMBER: 2017-2045

INSTITUTION: EU-LISA

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001([1])

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER

Luca Zampaglione, eu-LISA Security Officer,

Luca.Zampaglione@eulisa.europa.eu

EU-LISA,
EUROPEAN AGENCY FOR THE OPERATIONAL MANAGEMENT OF LARGE-SCALE IT SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE
EU HOUSE
RÄVALA PST 4
10143 TALLINN, ESTONIA

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

- eu-LISA Security Sector personnel
- G4S personnel (Contractor)
- Security France personnel (Contractor)

[1] OJ L 8, 12.01.2001.

[2] **Please attach all necessary backup documents**

3/ NAME OF THE PROCESSING

Entrance permission and access control system for physical protection at eu-LISA

4/ PURPOSE OR PURPOSES OF THE PROCESSING

eu-LISA uses the data collected through the access control system for the sole purpose of physical security and access control. The access control system helps to control the access to eu-LISA premises in Tallinn and Strasbourg, ensuring the security and the safety of premises, individuals and goods. It complements other physical security system such as the video-surveillance system. It helps to prevent, deter, and if necessary, investigate unauthorised physical access and security incidents in areas under surveillance.

The system is not used for any other purposes than described under the previous point.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

All persons with an application for access to eu-LISA premises in Tallinn and Strasbourg:

- eu-LISA staff
- eu-LISA Seconded National Experts (SNE) and trainees
- eu-LISA contractors
- Visitors

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA *(including, if applicable, special categories of data (Article 10) and/or origin of data).*

- Data contained in the badge: full name of the person who has been given the access token, ID photos, fingerprints template (not the image - only for persons who had access on Strasbourg premises), card serial number.

- Data contained in the system: full name of the person who has been given the access token, badge identification number, access rights of the badge (based on the profiles), access areas on site (with timestamp, readers ID, logged security events (in/out/denied), finishing working date at eu-LISA. For Strasbourg system, fingerprint images are immediately converted into hashes/templates by the software access application and stored inside the card, **with no central database storage.**

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

Data subjects are informed by a privacy statement (see below).

- The privacy statement for visitors will be placed on the board in the entrance building of eu-LISA.
- The privacy statement for eu-LISA staff and contractors will be published on the eu-LISA Intranet page.

The Regulation 45/2001 (hereinafter 'the Regulation') applies to the processing operation of the personal data in the context of the Access Control System at eu-LISA Tallinn and Strasbourg site. According to Articles 11 and 12 of the Regulation, eu-LISA will provide the data subjects with the following information:

The controller is the Head of the Security Unit in eu-LISA. Data are strictly processed within the Security Unit by the Security personnel and by G4S Estonia and Security France personnel (Contractors for managing security guards and reception)

Eu-LISA uses the data collected through the access control system for the sole purpose of physical security and access control. The access control system helps to control the access to eu-LISA premises, ensuring the security and the safety of premises, individuals and goods. It complements other physical security system such as the video-surveillance system. It helps to prevent, deter, and if necessary, investigate unauthorised physical access and security incidents in areas under surveillance.
The system is not used for any other purposes than described under the previous point.

The legal basis of the processing operation is:
-Agency General Information Security Policy
- Commission Decision C(2006) 3602 on security of information systems
- Commission Decision 2015/443 on Security in the Commission
- Commission Decision 2015/444 on the security rules for EUCI

The categories of data which are used in the context of this processing operation are the following:
•Full Name of the person who has been given an access token
• Finishing working date at eu-LISA
•Identification number of the access badge/token
•fingerprint of the person who has been given an access token (only for eu-LISA Strasbourg premises access);
• fingerprint template
• ID-photo

The recipients of personal data related to the access control system logs are:
• eu-LISA security personnel;
• G4S Estonia personnel (eu-LISA contractor for managing security guards and reception at the Agency premises in Tallinn);
• Security France personnel (eu-LISA contractor for managing security guards and reception at the Agency premises in Strasbourg)

Data subjects can exercise their rights of access, rectification, block and erasure of the data at any time by contacting the Head of Security Unit Luca.ZAMPAGLIONE@eulisa.europa.eu.

Data subjects have at any time the right of recourse to the EDPS with regard to the processing of their personal information in the context edps@edps.europa.eu
Data subjects may at any time refer to the DPO with regard to the processing of their personal information in the context dpo@eulisa.europa.eu

The data contained in the badge are stored for 1 month after the expiration date of the badge, the data contained in the system are store for 90 days after the recording.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

Data subjects have the rights of access, to rectify, to block, to erase, to object their own personal data by contacting the Head of Security Sector, being the data controller, at this address (Luca.ZAMPAGLIONE@eulisa.europa.eu). Data subjects can also, at any time contact, eu-LISA's DPO with regard to the processing of their personal information by writing to this address (dpo@eulisa.europa.eu). Finally, the right to recourse to the EPDS is also indicated in the privacy statement.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

[*security sensitive info*]

10/ STORAGE MEDIA OF DATA

The evidence of the badge holders is stored electronically on the local HDD of the Security Sector staff and also on the eu-LISA share-drive.
The access event logs are stored electronically on the server of the access control systems and, if the case, some reports/lists of the records could be copied on the eu-LISA internal infrastructure when there a need to perform specific security activities (like investigations, assessments, etc.).

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

Processing operation is necessary for the performance of eu-LISA tasks on the basis of the eu-LISA founding instrument or other legal instrument adopted on the basis thereof or in the legitimate exercise of official authority vested in eu-LISA or in a third party to whom data are disclosed (Regulation (EC) 45/2001, Article 5(a)).

The legal basis of the legitimate exercise of official authority vested in eu-LISA are:
- Agency General Information Security Policy
- Commission Decision C(2006) 3602 on security of information systems
- Commission Decision 2015/443 on Security in the Commission
- Commission Decision 2015/444 on the security rules for EUCI

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

Data will only be disclosed to:
- eu-LISA security personnel;
- G4S Estonia personnel (eu-LISA contractors for managing security guards and reception at the Agency premises in Tallinn);
- Security France personnel (eu-LISA contractor for managing security guards and reception at the Agency premises in Strasbourg);

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

The data contained in the badge is stored for 1 month after the expiration date of the badge. The data contained in the system is stored for 90 days after the recording.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS

The time established to comply with the requests is:
- Right to access data within 3 months;
- Right to rectify personal data according to the previous statement is immediate;
- Right to block, erase, object in a case-by-case analysis within a timeframe of 10 days.

(Please, specify the time limits for every category, if applicable)

14/ HISTORICAL, STATISTICAL OR SCIENTIFIC PURPOSES

If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification.

N/A

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

N/A

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING *(Please describe):*

Article 27(1) of Regulation (EC) No 45/2001 subjects to prior checking by the EDPS "processing operations likely to present specific risks to the rights and freedoms of data subject by virtue of their nature, their scope or their purposes". Article 27(2) of the Regulation contains a list of processing

operations that are likely to present such risks. Regarding the reviewed case, the processing operation presents specific risks since it processes data relating to security measures (Article 27.2 (a)).

Moreover, the nature of biometric data which is highly sensitive, due to the inherent characteristics of this type of data, can in fact represent specific risks to the rights and freedoms of the data subjects. These risks justify the need for the data processing itself to be prior checked by the EDPS in order to verify that rigorous safeguards have been implemented.

AS FORESEEN IN:

Article 27.2.(a)

Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

17/ COMMENTS

The processing operation entrusted to eu-LISA started on the 1st March 2016, this is an ex-post prior checking.

The following **annexes** are included to this notification:

- Presentation of the new eu-LISA badges
- Disclaimer for the Access control system in Tallinn
- Agency General Information Security Policy
- Contractual documentation between eu-LISA and G4S Estonia
- Contractual documentation between eu-LISA and Securitas France
- Printscreen image of the software used to manage the access control system in Tallinn

PLACE AND DATE: 28/02/2017

DATA PROTECTION OFFICER: FERNANDO SILVA

INSTITUTION OR BODY: EU-LISA, LARGE INFORMATION SYSTEM AGENCY