EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

RECORD OF PROCESSING ACTIVITY ACCORDING TO ARTICLE 31 REGULATION 2018/1725[1] NOTIFICATION TO THE DATA PROTECTION OFFICER

NAME OF PROCESSING OPERATION[2]: Monitoring of ICT Systems and E-communications

DPR-2018-026 (to be completed by the DPO)
Creation date of this record: 21/12/2018
Last update of this record: 21/12/2018
Version: 1

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: European Union Agency for Fundamental Rights (FRA)
Organisational unit **responsible**[4] for the processing activity: Corporate Services
Contact person: Constantinos Manolopoulos
Data Protection Officer (DPO): [redacted] dpo@fra.europa.eu)

2) Who is actually conducting the processing? (Article 31.1(a))[5]	
The data is processed by the FRA itself	☒
The data is processed also by a third party (contractor) [mention the third party]	☐

1 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725

2 **Personal data** is any information relating to an identified or identifiable natural person, i.e. someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity. This information may, for example, be the name, date of birth, a telephone number, biometric data, medical data, a picture, professional details, etc.
Processing means any operation or set of operations which is performed on personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3 In case of more than one controller (e.g. joint FRA research), all controllers need to be listed here

4 This is the unit that decides that the processing takes place and why.

5 Is the FRA itself conducting the processing? Or has a provider been contracted?

3) Purpose of the processing (Article 31.1(b))

Why are the personal data being processed? Please provide a very concise description of what you intend to achieve with the processing operation. Specify the rationale and underlying reason for the processing and describe the individual steps used for the processing. If you do this on a specific legal basis, mention it as well (e.g. staff regulations for selection procedures).

This record includes all IT systems that include monitoring features.

1a. Unified Communication (Lync)- Call Monitoring Data

The purpose of recording the logs of the incoming/outgoing telephone connections is to ensure the quality of the service and the system security.

1b. Firewall Log Files

The firewall will filter the Internet traffic in order to mitigate the risks and losses associated with security threats, while maintaining appropriate levels of access for users.

FRA has 2 firewalls as elements of a layered approach to network security:

Firewall 1) - the role of this Firewall is to control the traffic between the outside, inside and DMZ.

Firewall 2) - the role of this Firewall is to control the traffic on the inside network and between the VLANs.

The firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks.
- Block unwanted traffic as determined by the firewall rule set.
- Hide vulnerable internal systems from the Internet.
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet.
- Log traffic to and from the internal network.
- Provide robust authentication.
- Provide virtual private network (VPN) connectivity.

1c. Email system log files

The email traffic is being logged in order to ensure security and stability of the FRA email system, to detect attacks from out and inside and to measure loads. Only information relevant to the transmission of the email is being stored, not the content of the emails. Email may be backed up in order to assure email integrity and availability. Email messages may be archived for future analysis if there is a need to carry out investigation regarding illegal activities.

1d. Proxy server SSL

The purpose of using the Proxy Server SSL is to ensure the security for the ICT systems and to detect attacks from out and inside the network.

1e. Other purposes

Data from incoming or outgoing logs could be used in aggregated format to assist in an ICT system administration task like performance monitoring. In case there is a specific incident that requires the examination of individual log files then the data subject will be

informed in advance providing the necessary information and the purpose of the action, which is to resolve a specific technical issue at hand.

4) Description of the categories of data subjects (Article 31.1(c))

Whose personal data are being processed?

FRA staff	☒
Non-FRA staff (contractors, visitors, conference attendees, etc.)	☒

5) Categories of personal data processed (Article 31.1(c))

Please tick all that apply and give details where appropriate. Include information if automated decision making takes place, evaluation and monitoring

1a. Unified Communication (Lync)- Call Monitoring Data

Date and time, length of the call, from user (email address, phone number, operating systems, MAC address.), to user (email address, phone number, operating system, MAC address.).

1b. Firewall Log Files

Source IP, target Ip and the Protocol used;

1c. Email system log files

Email sender and recipients, sender name, recipient name, subject, send time, SMTP path, date, message-id, bcc, cc and content type.

1d. Proxy server SSL

Source ip, destination ip/dns, duration, date/time, downloaded size. (User ID and IP address, volume of data exchanged, the date and time of access).

1e. Other personal data which could be processed:

• *Active directory:*

The active directory contains the following personal information:

Username, forename, last name, unit, room, telephone number, email address, office address;

• *Windows system logs:*

User name, workstation id, user logon/logoff time.

• *Exchange address book*:

FRA is exchanging its email address book with the EC. Your contact details will be stored within the EC email address book.

The following information is being sent to the EC:

Name, Forename, office email address, office telephone number.

• *ISILOG Inventory tool*:
The Isilog database is containing the following information:
Username, forename, last name.

6) Recipient(s) of the data (Article 31.1 (d))[6]

*Recipients are all parties who have access to the personal data. Who will have access to the data **within** FRA? Who will have access to the data **outside** FRA?*

Designated **FRA** staff members: ☒

FRA ICT technical staff and the Director in some cases

Designated persons **outside** FRA: (please specify) ☐

7) Transfers to third countries or recipients outside the EEA (Article 31.1 (e))[7]

If the personal data are transferred outside the European Economic Area, this needs to be specifically mentioned, since it increases the risks of the processing operation.

Data are transferred to third country recipients:

Yes ☐

No ☒

If yes, specify to which country:

If yes, specify under which safeguards:

Adequacy Decision of the European Commission ☐

Standard Contractual Clauses ☐

Binding Corporate Rules ☐

Memorandum of Understanding between public authorities ☐

[6] No need to mention entities that may have access in the course of a particular investigation (e.g. OLAF, EO, EDPS).

[7] **Processor** in a third country using standard contractual clauses, a third-country public authority you cooperate with based on a treaty. If needed, consult your DPO for more information on how to ensure safeguards.

8) Retention time (Article 4(e))

How long will the data be retained and what is the justification for the retention period? Please indicate the starting point and differentiate between categories of persons or data where needed (e.g. in selection procedures candidates who made it onto the reserve list vs. those who didn`t). Are the data limited according to the adage "as long as necessary, as short as possible"?

1a. Unified Communication (Lync)- Call Monitoring Data

90 days

1b. Firewall Log Files

180 days

1c. Email system log files

180 days (After a staff member has left FRA due to the end of his/her contract, his/her email data and his/her data found on his/her private folder and professional email account will be exported from the ICT systems to an separate storage area with limited access upon a notification of the CS unit. The data will be kept for 6 month).

1d. Proxy server SSL

180 days

1e. Windows Log files

90 days

9) Technical and organisational security measures (Article 31.1(g))

Please specify where/how the data are stored during and after the processing; please describe the security measures taken by FRA or by the contractor

How is the data stored?

FRA network shared drive	☒
Outlook Folder(s)	☐
CRM	☐
Hardcopy file	☐
Cloud (give details, *e.g. cloud provider*)	☐
Servers of external provider	☐

Other (please specify): *E.g. The data is stored in the EU and no transferred outside EU; the system cannot track the IP; cookies are enabled just for keeping the session active and deleted after the session expires; the data transmission takes places via https://; you need to check the security incident procedure of the contractor and the data breach procedure*

10) Lawfulness of the processing (Article 5(a)–(d))[8]: Processing necessary for: *Mention the legal basis which justifies the processing*	
(a) a task carried out in the public interest or in the exercise of official authority vested in the FRA (including management and functioning of the institution) (Examples of legal basis: FRA Founding Regulation (EC) No. 168/2007 establishing the European Union Agency for Fundamental Rights Articles 4.1 a) and 4.1 c);); FRA legal acts (Conditions of Employment, Staff Rules, Administrative Circular etc.)	☒
(b) compliance with a legal obligation to which the FRA is subject	☐
(c) necessary for the performance of a contract with the data subject or to prepare such a contract	☐
(d) Data subject has given consent (ex ante, explicit, informed) Describe how consent will be collected and where the relevant proof of consent will be stored	☒
(e) necessary in order to protect the vital interests of the data subjects or of another natural person	☐

11) Data Minimisation(Article 4(c)) *Do you really need all data items you plan to collect? Are there any you could do without?*
The processed personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed i.e. monitoring of ICT systems to secure proper and secure use.

[8] Tick (at least) one and explain why the processing is necessary for it. Examples:

(a) a task attributed to your EUI by legislation, e.g. procedures under the staff regulations or tasks assigned by an Agency's founding regulation. Please mention the specific legal basis (e.g. "Staff Regulations Article X, as implemented by EUI IR Article Y", instead of just "Staff Regulations")

(a2) not all processing operations required for the functioning of the EUIs are explicitly mandated by legislation; recital 17 explains that they are nonetheless covered here, e.g. internal staff directory, access control.

(b) a specific legal obligation to process personal data, e.g. obligation to publish declarations of interest in an EU agency's founding regulation.

(c) this is rarely used by the EUIs.

(d) if persons have given free and informed consent, e.g. a photo booth on EU open day, optional publication of photos in internal directory;
(e) e.g. processing of health information by first responders after an accident when the person cannot consent.

12) Transparency (Article 14)

How do you inform people about the processing operation?

The data subjects are informed via the ICT Security & Data Management Policy, ICT Policy and ICT Back Office Policy. Moreover, a Privacy Notice informing the data subjects about all the processing operations is available on the FRA Intranet;

13) Exercising the rights of the data subject (Article 14 (2))

How can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? How will you react?

Data subject rights:

Right to have access	☒ Anytime [or specify the timeframe]
Right to rectify	☒ Anytime [or specify the timeframe]
Right to erase ("right to be forgotten)	☒ Anytime [or specify the timeframe]
Right to restrict of processing	☒ Anytime [or specify the timeframe]
Right to data portability	☐ Anytime [or specify the timeframe]
Right to object	☒ Anytime [or specify the timeframe]
Right to obtain notifications to 3rd parties	☒ Anytime [or specify the timeframe]
Right to have recourse	☒ Anytime [or specify the timeframe]
Right to withdraw consent at any time	☒ Anytime [or specify the timeframe]

14) High risk identification

Does this process involve any of the following?

- ☐ *data relating to health, (suspected) criminal offences or otherwise considered sensitive ('special data categories');*
- ☐ *evaluation, automated decision-making or profiling;*
- ☐ *monitoring data subjects;*
- ☐ *new technologies that may be considered intrusive.*

If yes provide details

Not applicable. The processing operations do not monitor the data subjects. Processing is required to ensure proper functiing of the ICT systems.

14) Other linked documentation *Please provide links to other documentation of this process (consent form, privacy notice, project documentation, security related policies /measures etc.)*
Privacy Notice

Responsible	Signature	Date
Head of Corporate Services Unit C. Manolopoulos		