EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

PRIVACY NOTICE

Monitoring of ICT Systems and E-communications

The European Union Agency for Fundamental Rights (FRA) processes the personal data of a natural person in compliance with Regulation 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

This privacy notice explains FRA's policies and practices regarding its collection and use of your personal data, and sets forth your privacy rights. We recognise that information privacy is an ongoing responsibility, and we will update this notice where necessary.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

PRIVACY NOTICE

1. Why do we collect personal data?

FRA maintains automated machine-based mechanisms, which monitor and log network, email, Internet traffic, Internet activities and incoming/outgoing telephone connections.
FRA`s ICT Systems and E-communications need to be monitored to ensure that they function the way that they should and to allow Administration to take proactive actions to minimize the unavailability of such systems. This includes processing operations which aim to:

- Ensure the security and stability of the systems;
- Detect and prevent attacks (internal and external);
- Ensure the proper functioning of the system;
- Measure usage;

2. What kind of personal data does the Agency collect?

The Agency collects data from the applicants regarding:

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

User email, destination email, destination phone number, incoming phone number, incoming email, date and time.

1b. Firewall Log Files

Source IP, IP destination, date and time;

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.Domain system Monitoring Logs

Username, action, date and time, workstation name.

1e. Proxy server SSL

Source IP, destination IP/DNS, duration, date/time.

1f. Network Security Logs

Source IP, IP destination, date and time, protocol used and Application

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*:

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

PRIVACY NOTICE

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.

3. How do we collect your personal data?

a. Unified Communication (Lync)- Call Monitoring Data

This is a phone-managing tool managed when a user uses the Lync for internally or externally communication, and for recording the logs of all incoming/outgoing telephone connections.

b. Firewall Log Files

When a user is using the ICT infrastructure, FRA operates firewalls or network traffic filters between the Internet and its private internal network in order to create a secure operating environment for FRA`s computers and network resources.

c. Email system log files

When a user is sending/receiving an email, FRA is logging in the traffic of the emails. The content of the email messages may be automatic centrally scanned using lexical analysis techniques. Such method can help in blocking irrelevant or inappropriate messages addressed to Agency staff, such as malicious code, spam email, etc. The central email scanning it is not implemented as a mean of surveillance of user communication activity and no person at this stage could see the content of the email.

d. Domain system Monitoring Logs

This is a tool that monitors the access to domain resources that requires access privileges.

e. Proxy server SSL

When a user is using the Internet, SSL (Secure Sockets Layer) provides a secure channel between all incoming and outgoing web traffic, which is being decrypted in order to ensure the security for FRA systems. After scanning the data, the traffic is encrypted again.

f. Network Security Logs

This tool monitors the ICT Network.

4. Who is responsible for the processing your personal data?

The Agency is the legal entity responsible for the processing of your personal data and determines the objective of this processing activity. The Head of Corporate Services is responsible for this processing operation.

5. Which is the legal basis for this processing operation?

The Agency have in place various ICT Policies including: ICT Policy PO.ICT.001-02, ICT Back Office Policy PO.ICTF.004-01, ICT Security & Data Management Policy PO.ICTF.007-01. Hence, these policies are also the legal basis for this processing operation, which are in accordance with Article 5(a) of the Regulation (EU) No 2018/1725.

Also, the processing is lawful under Article 5(d) of the Regulation (EU) No 2018/1725 because "the data subject has unambiguously given his or her consent".

6. Who can see your data?

Monitoring is done by machine-based mechanisms and the information collected is used for security and capacity management purposes.

In case of technical or security issues, exclusively FRA ICT technical staff might conduct manual processing of this information (internet traffic/email/ICT activities). In exceptional circumstances (i.e. in the framework of Administrative inquiries), only the Director of the Agency can request the manual processing.

Whenever the interests of the service requires urgent access to important information during absence of staff, the Appointing Authority has a right of access to office equipment and professional information handled by staff members and stored on individual PC workstations, central servers and/or in electronic mailboxes.

The Administration may provide anonymous statistics of the using of ICT Services (internet access, telephone and mobile phones) just to the Head of Unit upon request and approval of the Director.

7. Do we share your data with other organisations?

Personal data is processed by the Agency only. In case that we need to share your data with third parties, you will be notified to whom your personal data has been shared with.

8. Do we intend to transfer your personal data to Third Countries/International Organizations

No.

9. When will we start the processing operation?

We will start the processing operation when you are starting to use FRA`s ICT network in anyway.

10. How long do we keep your data?

The Agency will keep your personal data as followed:

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

90 days

b. Firewall Log File

7 days

c. Email system log files

Email system back office: 90 days;

Email system gateway: 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 HRP Department. The data will be kept for 6 month).

d. Domain system Monitoring Logs

Short term 30 days. Long term 12 months

e. Proxy server SSL

Size based: 10 MB daily

f. Network Security Logs

180 days

11. How can you control your data?

You can access, modify or delete your personal data by sending an email request to it.helpdesk@fra.europa.eu . More details are provided below.

11.1. How valuable is your consent for us?

The processing is lawful because "the data subject has unambiguously given his or her consent". Therefore, you have the right to withdraw your consent at any time, and we will delete your data or restrict its processing.

11.2. Your data protection rights

Under data protection law, you have rights we need to make you aware of. The rights available to you depend on the aim of processing of your information. You are not required to pay any charges for exercising your rights.

a) Can you access your data?

You have the right to receive confirmation whether or not we process your personal data. Furthermore, you can have access to such data, as well as obtain copies of your data undergoing processing, at any time and free of charge, by sending an email request to it.helpdesk@fra.europa.eu.

b) Can you modify your data?

Due to the unique characteristics of the data collected and for having to preserve the integrity of the log files, any modification of the data is not possible.

c) Can you restrict us from processing your data?

Limited applicability

d) Can you delete your data?

Limited applicability

e) Can you request the transfer of your data to a third party?

This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another, or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is automated.

f) Do you have the right to object?

Yes, you have the right to object at any time by sending an email request to it.helpdesk@fra.europa.eu when you have legitimate reasons relating to your particular situation. Moreover, you will be informed before your information is disclosed for the first time to third parties, or before it is used on their behalf, for direct marketing purposes.

The Agency will address your requests within 15 working days from the receipt of the request.

g) Do we do automated decision making, including profiling?

No.

12. What security measures are taken to safeguard your personal data?

The Agency has several security controls in place to protect your personal data from unauthorised access, use or disclosure. We keep your data stored on computer systems with limited access to a specified audience only.

13. What can you do in the event of a problem?

a) The first step is to notify the Agency by sending an email to dpo@fra.europa.eu and ask us to take action.

b) At any time you can lodge a complaint with the EDPS at http://www.edps.europa.eu, who will examine your request and adopt the necessary measures.

14. How do we update our privacy notice?

We keep our privacy notice under regular review to make sure it is up to date and accurate.

END OF DOCUMENT