EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

DATA PROTECTION NOTICE

CERT-EU services

The European Union Agency for Fundamental Rights (FRA or Agency) 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 data protection 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.

1. Why do we collect personal data?
2. What kind of personal data does the Agency collect?
3. How do we collect your personal data?
4. Who is responsible for processing your personal data?
5. Which is the legal basis for this processing operation?
6. Who can see your data
7. Do we share your data with other organisations?
8. Do we intend to transfer your personal data to Third Countries/International Organizations
9. When will we start the processing operation?
10. How long do we keep your data?
11. How can you control your data?
    - 11.1. The value of your consent
    - 11.2. Your data protection rights
12. What security measure are taken to safeguard your personal data?
13. What can you do in the event of a problem?
14. How do we update our data protection notice?

1. Why do we collect personal data?

Personal data is collected and processed in relation to the cybersecurity services provided to the Agency by CERT-EU under the Service Level Agreement CERT-EU-005 concluded between the Agency and the Directorate-General for Informatics (DIGIT).

The purpose of processing is to contribute to the security of the ICT infrastructure of the Agency and to enable CERT-EU to carry out its mission. CERT-EU's mission is to contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies by helping to prevent, detect, mitigate and respond to cyber-attacks and by acting as their cyber-security information exchange and incident response coordination hub.

CERT-EU collects, manages, analyses and shares information with the Union institutions, bodies and agencies (the constituents) on threats, vulnerabilities and incidents on unclassified ICT infrastructure. It coordinates responses to incidents at inter-institutional and constituent level, including by providing or coordinating the provision of specialised operational assistance.

In particular, data is processed for specific purposes, such as prevention services, cyber threat intelligence, IDS monitoring, offensive security and incident response.

2. What kind of personal data are collected and further processed?

In order to carry out this processing operation, the following categories of personal data are collected and further processed:

1) Automated processing may involve any personal data flowing or stored on electronic networks of any of the EU institutions, bodies and agencies.
2) Manual processing generally includes the following categories of data:

- Any file (with user-id included) stored in, transmitted from / to a host involved in an incident (as victim, relay or perpetrator),
- Email addresses, phone number, role, name, organisation,
- Name of the owner of assets involved in an incident, user account name (for email, operating system, applications, centralised authentication services, etc),
- Technical protocol data (IP address, MAC address) to which an individual may be associated.

<u>Data is processed for specific purposes in particular:</u>

- Personal data that might be processed for automated cybersecurity procedures (including online media sources, cybersecurity information sharing partnership etc)
- Personal data processed for Cyber Threat Management (first response, analysts and vulnerability assessment teams)
- Personal data processed for Incident response management including backups

3. How is your data collected and further processed?

3a. Information you provide us: This includes data like email addresses, phone number, role, name, organisation

3b. Information we collect about you via:

1. Automatic processing:
   Monitoring of logs and monitoring of intrusion detention sensors are automated this means that only when suspicious activity is identified (through machine-processing), human intervention takes place. Media Monitoring is fully automated. Some of the backup processes (for business continuity purposes) are automated.

2. Manual processing:
   A large variety of software and hardware tools are used to manually process data for cybersecurity purposes including in particular incident response, cyber threat intelligence, constituent data management, vulnerability assessment, and infrastructure management. In addition, manual processing takes place for human resources and other administrative purposes.

4. Who is responsible for 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 Unit Corporate Services is responsible for this processing operation.

The processor is CERT-EU, on the basis of a data processing agreement (annexed to the SLA concluded between FRA and DIGIT) in which the service provider (CERT-EU) acts as processor and the client (the Agency) acts as data controller.

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

Processing is necessary for the management and functioning of the Agency. The described CERT-EU services are necessary in the context of the Cybersecurity regulation and related security regulations, which comprise the specific legal bases[1]. Within this framework, the processor (CERT-EU) collects and processes data to contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies by helping to prevent, detect, mitigate and respond to cyber-attacks and by acting as their cyber-security information exchange and incident response coordination hub.

Therefore, the processing is lawful under Article 5.1.(a) of the Regulation (EU) No 2018/1725.

[1] Inter-institutional Arrangement 2018/C12/01 between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU), OJ C12/1 of 13.1.2018
Directive (EU) 2016/1148 of the European Parliament and of the Council (the 'NIS Directive')

The processor (CERT-EU) does not focus on processing any special categories of data falling under Art. 10(1) or sensitive data falling under Art. 11. However, if this data is involved in a cybersecurity incident handled by CERT-EU, it will be processed manually as part of the incident investigation, including to establish whether a data breach has taken place.

6. Who can see your data?

Within the Agency, your personal data is accessible by the involved Digital Services staff and the Head of Unit Corporate Services and the Director.

To execute its tasks, the processor (CERT-EU) shares personal data with CERT-EU staff, EC Staff, other EUIs Staff, CERT-EU trusted partners (limited personal data related to cyberattacks and security incidents and other malicious actions) via confidential portals and secure channels.

7. Do we share your data with other organisations?

Personal data is processed by the Agency only as the controller and CERT-EU as the data processor. 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 such transfer is foreseen in principle.

However, your personal data could be transferred to the recipients in a third country or to an international organisation in accordance with Regulation (EU) 2018/1725. Please refer to the latest version of the CERT-EU Privacy Statement. Currently, these organisations are the NATO NCIRC (NATO Cybersecurity Incident Response Center), and the UN OICT (Office of Information and Communications Technology)

The legal bases for such transfers are stipulated in detail in the aforementioned Privacy Statement.

9. When we will start the processing operation?

We will start the processing operation from the signature of the amended SLA between the two parties.

10. How long do we keep your data?

The data are kept for as long as it is necessary to perform the services under the SLA. The duration of processing of personal data by the service provider (CERT-EU) per type of processing activity will not exceed the duration of the SLA.

The processor (CERT-EU) only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, namely for the below mentioned periods:

A) Personal data that might be processed for automated cybersecurity procedures:

- Data will be kept for up to 3 years. For online content as long as the data remain publicly available

B) Personal data processed for Cyber Threat Management:

- For reports: 5 years and an additional 5 year period for archiving
- For all other data: up to 10 years and an additional 10 year period for archiving

C) For Personal data processed for Incident response management:

Data is kept for up to 2 years.

Regarding the processing of personal data stemming for administrative tasks the period is ten years starting from the payment of the balance of the last fee due under the Amendment 3 of the SLA.
Upon expiry of this period, the service provider shall, at the choice of the client, return, without any undue delay and in a commonly agreed format, all personal data processed on behalf of the client and the copies thereof, or shall effectively delete all personal data unless Union law requires a longer storage of those personal data.

The service provider shall keep the personal data in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

11. How can you control your data?

Under Regulation 2018/1725, you have rights we need to make you aware of. The rights available to you depend on our reason for processing your information. You are not required to pay any charges for exercising your rights except in cases were the requests are manifestly unfounded or excessive, in particular because of their repetitive character.

We will reply to your request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

You can exercise your rights described below by sending an email request to it.helpdesk@fra.europa.eu

11.1. The value of your consent

Since the performance of this particular processing operation is mandatory in accordance with the applicable legal framework (please refer to Section 5 of this Notice concerning the legal basis), you are not required to provide your consent.

11.2. Your data protection rights

a. Can you access your data?

You have the right to receive information on whether we process your personal data or not, the purposes of the processing, the categories of personal data concerned, any recipients to whom the personal data have been disclosed and their storage period. Furthermore, you can have access to such data, as well as obtain copies of your data undergoing processing.

b. Can you modify your data?

You have the right to ask us to rectify your data you think is inaccurate or incomplete at any time.

c. Can you restrict us from processing your data?

You have the right to restrict the processing of your personal data. If you do, we can no longer process them, but we can still store them. In some exceptional cases, we will still be able to use them (e.g. with your consent or for legal claims). You have this right in a few different situations: when you contest the accuracy of your personal data, when the Agency no longer needs the data for completing its tasks, when the processing activity is unlawful, and finally, when you have exercised your right to object. Restrictions may apply on a case-by-case basis.

d. Can you delete your data?

You have the right to ask us to delete your data when the personal data are no longer necessary for the purposes for which they were collected, when you have withdrawn your consent or when the processing activity is unlawful. In certain occasions we will have to erase your data in order to comply with a legal obligation to which we are subject.

We will notify to each recipient to whom your personal data have been disclosed of any rectification or erasure of personal data or restriction of processing carried out in accordance with the above rights unless this proves impossible or involves disproportionate effort from our side.

e. Are you entitled to data portability?

Data portability is a right guaranteed under Regulation 1725/2018 and consists in the right to have your personal data transmitted to you or directly to another controller of your choice. Restrictions may apply on a case-by-case basis.

f. Do you have the right to object?

When the legal base of the processing is "*necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body*" which is the case in most of our processing operations, you have the right to object to the processing. In case you object, we have to stop the processing of your personal data, unless we demonstrate a compelling reason that can override your objection. Restrictions may apply on a case-by-case basis.

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

Not applicable

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 our internal servers with limited access to a specified audience only.

The service provider shall adopt appropriate technical and organisational security measures relating to the provided services[2]. Both types of measures shall give due regard to the risks inherent in the processing and to the nature, scope, context and purposes of processing, in order to:

a. ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

b. restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

c. ensure a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

d. ensure measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The service provider shall maintain a record of all data processing operations carried out on behalf of the client, transfers of personal data, security breaches, responses to requests for exercising rights of people whose personal data is processed and requests for access to personal data by third parties.
For a more concrete stipulation of the security measures implemented by the processor (CERT-EU), please refer to its specific Record and Privacy Statement.

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 it.helpdesk@fra.europa.eu and ask us to take action.

b) The second step, if you obtain no reply from us or if you are not satisfied with it, contact our Data Protection Officer (DPO) at dpo@fra.europa.eu.

c) 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 data protection notice?

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

END OF DOCUMENT

[2] These organisational measures include the appropriate use of the service and its functionalities