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]: CERT-EU services

Reference number: DPR-2022-148
Creation date of this record: 11/02/2022
Last update of this record:
Version: 1

Part 1 (Publicly available)

1) Controller(s)[3] of data processing operation (Article 31.1(a))
Controller: European Union Agency for Fundamental Rights (FRA)
Schwarzenbergplatz 11, A-1040 Vienna, Austria
Telephone: +43 1 580 30
Email: contact@fra.europa.eu
Organisational unit **responsible**[4] for the processing activity: Corporate Services
Contact details: it.helpdesk@fra.europa.eu
Data Protection Officer (DPO): 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):	☒
The processor is CERT-EU, on the basis of a data processing agreement (annexed to the Service Level Agreement concluded between FRA and DIGIT)	

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?

in which the service provider (CERT-EU) acts as processor and the client (the Agency) acts as data controller.

Contact point at external third party (e.g. Privacy/Data Protection Officer – use functional mailboxes, not personal ones, as far as possible):
The contact point for all requests is the Agency who will contact the corresponding CERT-EU contact. This is specified in the SLA Annex.

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).

The purpose of processing is to contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies 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 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.

Mode of processing

- Automatic processing (Article 24)
    - Computer/machine
        - Any other:

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.

- Manual processing
    - Word documents
    - Excel sheet
    - Any other:

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.

Data is processed for specific purposes in particular:

- Prevention services
- Cyber threat intelligence
- IDS monitoring
- Offensive security
- Incident response

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

Whose personal data are being processed?

FRA staff ☒

Non-FRA staff) ☒

CERT-EU's automated cybersecurity operations can involve processing of any personal data of any of the EU institutions, bodies and agencies. Manual cybersecurity processing includes data subjects involved in any of CERT-EU's cybersecurity activities (either as victims of a cyberattack or as malicious actors).

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

Please tick all that apply and give details where appropriate

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.

Data is processed for specific purposes in particular:

- 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

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

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

Designated **FRA** staff members ☒

The assigned Digital Services staff, Head of Unit CS and Director

Recipients **outside** FRA ☒

EUIBAs (EU institutions, bodies and agencies) Staff, CERT-EU trusted partners (limited personal data related to cyberattacks and security incidents and other malicious actions)

7) Transfers to third countries or international organisations (Article 31.1 (e))[6]

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

Transfer outside of the EU or EEA

Yes ☐

No ☒

If yes, specify to which country:

Transfer to international organisation(s)

Yes ☒

[6] **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.

No ☐

If yes specify to which organisation:

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)

Legal base for the data transfer

☐ Transfer on the basis of the European Commission's adequacy decision (Article 47)

☐ Transfer subject to appropriate safeguards (Article 48.2 and .3), specify:

a) ☐ A legally binding and enforceable instrument between public authorities or bodies.
Standard data protection clauses, adopted by
b) ☐ the Commission, or
c) ☐ the European Data Protection Supervisor and approved by the Commission, pursuant to the examination procedure referred to in Article 96(2) .
d) ☐Binding corporate rules, ☐ Codes of conduct , ☐ Certification mechanism pursuant to points (b), (e) and (f) of Article 46(2) of Regulation (EU) 2016/679, where the processor is not a Union institution or body.

Subject to the authorisation from the European Data Protection Supervisor:
☐ Contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation.

☐ Administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

☐ Transfer based on an international agreement (Article 49), specify:

Derogations for specific situations (Article 50.1 (a) –(g))

☐ N /A
☒ Yes, derogation(s) for specific situations in accordance with article 50.1 (a) –(g) apply
In the absence of an adequacy decision, or of appropriate safeguards, transfer of personal data to a third country or an international organisation is based on the following condition(s):

☐ (a) The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards
☐ (b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
☐ (c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
☒ (d) The transfer is necessary for important reasons of public interest
The specific legal bases are stipulated in detail in the CERT-EU Privacy Statement

☐ (e) The transfer is necessary for the establishment, exercise or defense of legal claims
☐ (f) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
☐ (g) The transfer is made from a register which, according to Union law, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union law for consultation are fulfilled in the particular case

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"?

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 per type of processing activity will not exceed the period referred to in the beginning of attached SLA Annex (duration of the agreement).

The processor (CERT-EU) only keeps the 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.
For more details see here: CERT-EU Privacy Statement

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?

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

Other (please specify):
As described in the provided Annex:

The service provider shall adopt appropriate technical and organisational security measures relating to the provided services[7]. 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.

10) 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?

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

See further details in the Data Protection notice: e-mail to it.helpdesk@fra.europa.eu

Data subject rights

☒ Right of access

☒ Right to rectification

☒ Right to erasure (right to be forgotten)

☒ Right to restriction of processing

☒ Right to data portability

☒ Right to object

☒ Notification obligation regarding rectification or erasure of personal data or restriction of processing

☒ Right to have recourse

☐ Right to withdraw consent at any time

Restrictions may apply on a case-by-case basis.

Part 2 – Compliance check and risk screening (internal)

11) Lawfulness of the processing (Article 5.1.(a)–(e))[8]: Processing necessary for:

Mention the legal basis which justifies the processing and assess that the purposes specified are purposes specified, explicit, legitimate.

[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.