DATA PROTECTION NOTICE

on CERT-EU Services

As an EU Agency, Eurofound embraces the need to protect your personal data. We, therefore, undertake to process it, with respect to the applicable law[1].

If after reading this notice you still have questions on the processing of your data, please contact us at dataprotectionofficer@eurofound.europa.eu. We will reply to you within one month.

❖ Why do we need to process your data?

Personal data are collected and processed in relation to the cybersecurity services provided to Eurofound (i.e., data controller) by CERT-EU (i.e., data processor) under the Service Level Agreement CERT-EU-035 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, which is to contribute to the security of the ICT infrastructure of all Union institutions, bodies and agencies by helping to prevent, detect and 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 are processed for specific purposes, such as prevention services, cyber threat intelligent, Intrusion and Detection Systems (IDS) monitoring, offensive security and incident response.

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council 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 (or the EUDPR).

❖ What data do we need to process?

We need to process the following data:

1. Automated processing may involve any personal data flowing or stored on Eurofound's electronic networks, namely logs and intrusion detention sensors; and
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 (such 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); and
    - Technical protocol data (IP address, MAC address) to which an individual may be associated.

❖ Under what legal basis we process your personal data?

Processing is necessary for the management and functioning of Eurofound, namely its ICT infrastructure, being therefore lawful under Article 5.1(a) and recital (22) of the EUDPR.

❖ Who will process your data?

Within Eurofound, your personal data are accessible by the Head of the ICT and the Local Information Security Officer.

To execute its tasks, CERT-EU shares personal data with its staff, the European Commission's staff, staff from other EU institutions, bodies or agencies, and CERT-EU trusted partners (limited personal data related to cyber-attacks and security incidents and other malicious actions) via confidential portals and secure channels.

❖ How do we protect your data?

Both Eurofound and CERT-EU follow strict security procedures to ensure that your data is safely protected and is not, in any way, damaged, destroyed, or disclosed to a third

party without your authorisation or without you being informed, as well as to prevent unauthorised access. The servers storing the information are kept in a secure environment with restricted physical access. IT systems use firewalls and other measures to restrict electronic access.

❖ For how long will we retain your data?

Data will be kept for the following retention periods:

a) Data processed for automated cybersecurity procedures:

Will be kept for 3 years. Online content will be kept as long as the data remains publicly available;

b) Data processed for Cyber Threat Management:

Reports will be kept for 5 years, after which they will be archived for an additional period of 5 years. All other data will be kept for 10 years, after which they will be archived for an additional period of 10 years

c) Data processed for Incident Response Management:

Will be kept for 2 years.

d) Data processed for administrative tasks:

Will be kept for 10 years starting from the payment of the balance of the last fee due.

❖ Do we transfer your data to outside the EU?

In principle, no such transfers are foreseen. However, CERT-EU may occasionally transfer data to organisations outside the EEU area. Please read section 7 (‘*Who has access to your personal data and to whom is it disclosed?*’) of the CERT-UE privacy policy to know more about possible international transfers of data.

❖ What are your rights?

Within the limits set by the EDPR, you have the right to access, rectify, erase and/or port your personal data, to restrict or object to the processing of your personal data, and to withdraw your consent (if obtained). Just note that withdrawal of your consent does not affect the lawfulness of processing while your consent was valid.

You may contact us at ictseccom@eurofound.europa.eu with your request. Your request is free of charge. However, if it is manifestly unfounded or excessive, Eurofound may refuse to act on it.

You also have the right to raise a complaint with the European Data Protection Supervisor should you consider that this processing is in violation of the law. You will find more information here.

❖ Can your rights be restricted?

Pursuant to the Decision no. 21 of the Management Board of Eurofound adopting internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of the functioning of Eurofound[2], your rights can be restricted for the following purposes:

- Important objectives of general public interest of the Union or of a Member State, in particular the objectives of the common foreign and security policy of the Union or an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security[3];
- Internal security of Union institutions and bodies, including of their electronic communications networks[4];
- Monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c) of paragraph 1 of Article 25 of Regulation (EU) 2018/1725[5]; and

[2] Adopted 20 December 2019.
[3] Article 25(1) (c) of Regulation (EU) 2018/1725.
[4] Article 25(1) (d) of Regulation (EU) 2018/1725
[5] Article 25(1) (g) of Regulation (EU) 2018/1725.

- Protection of the data subject or the rights and freedoms of others[6].

The above restrictions may apply to the following rights: right of information to be provided to the data subject, right of access, rectification and erasure of personal data and right of restriction to the processing of personal data.

The restrictions can also apply to the obligation imposed upon Eurofound of communicating a personal data breach to the data subjects affected[7], as well to the obligation of ensuring the confidentiality of electronic communications[8].

[6] Article 25(1) (h) of Regulation (EU) 2018/1725.
[7] Article 35 of Regulation (EU) 2018/1725.
[8] Article 36 of Regulation (EU) 2018/1725.