EUROPEAN UNION AGENCY FOR RAILWAYS

Only the online version of this document shall be considered authoritative.

Record of processing activity

01 - Name of processing	CERT-EU services
02 - Reference	106
03 - Submission Date	23/03/2023
04 - Last update	23/03/2023
05a - Controller	RICOTTA Salvatore
05b - Unit-Sector	Resources and Support Unit
05c - Controller's email	salvatore.ricotta@era.europa.eu
06 - DPO	DataProtectionOfficer@era.europa.eu 120 Rue Marc Lefrancq, 59300 Valenciennes, France Tel. +33 (0) 32 70 96 503
07 - Name and contact details of joint controller(where applicable)	N/A
08a - Who is actually conducting the processing?(Article 31.1(a))	The data is processed by ERA (responsible unit) itself
08b - Name and contact details of processor (where applicable)	The processing operation is conducted together with CERT-EU, Rue de la Loi, 107 – 1000 Brussels – Belgium, email: services@cert.europa.eu [mailto:services@cert.europa.eu], on the basis of a data processing agreement annexed to the Service Level Agreement signed between ERA and DIGIT, where the service provider (CERT-EU) acts as processor and the client (ERA) acts as data controller.
09 - Purpose of processing	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 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, Intrusion Detection System monitoring, offensive security and incident response.

10a - Data Subjects	* Internal to the organisation: ERA staff, SNEs, trainees, contractors that are assigned with an ERA information asset (E.G., email, end-point equipment, etc.); * external to the organisation: Any natural person that has an interaction with the ERA information systems through electronic means. 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). Processing for HR and administrative purposes includes staff members of CERT-EU and contacts of CERT-EU in the constituents.
10b - Personal data	* Automated processing may involve any personal data flowing or stored on electronic networks of any EU Institutions, Bodies and Agencies. * Manually 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.
11 - Time limit for keeping the data	* Personal data that might be processed for automated cybersecurity procedures will be kept for up to 3 years. For online content as long as the data remain publicly available. * 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. * Personal data processed for Incident response management will be kept for up to 2 years. * Personal data stemming for administrative tasks will be kept up to 10 years and an additional 10 years period for archiving. 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 required 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.

12 - Recipients of the data	The recipients of the personal data are: * authorised staff according to the “need to know” principle. Such staff abide by statutory, and when required, additional confidentiality agreements. Those members of staff include ERA staff, CERT-EU staff, EC Staff, EUIBAs (EU institutions, bodies and agencies) Staff, CERT-EU trusted partners (limited personal data related to cyberattacks and security incidents and other malicious actions). All recipients of the data are reminded of their obligation not to use the data for any further purpose other than the ones for which they were collected. The personal information collected will not be communicated to third parties, except where necessary for the purposes ERA may be required to do so by law.

13 - Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	Yes Incident handling: If needed, data related to incidents is shared with trusted partners subject to all the necessary safeguards (contracts, NDAs) Data sharing with trusted partners in the context of combatting cyberattacks and cybercrime: international organisations based on bilateral agreements. Data sharing with trusted partners in the context of combatting cyberattacks and cybercrime: international organisations: NATO NCIRC (NATO Cybersecurity Incident Response Center): mutual sharing of cyber threat information. The NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team of the European Union (CERT-EU) signed a technical arrangement on 10 February 2016. The NCI Agency and CERT-EU have established a robust partnership based on thorough cyber defence information sharing to improve incident prevention, prediction, detection and response. UN OICT (Office of Information and Communications Technology): mutual sharing of cyber threat information. The transfer is subject to appropriate safeguards (Article 48.2 and .3): a legally binding and enforceable instrument between public authorities or bodies. Derogation(s) for specific situations in accordance with Article 50.1 (a) - (g) apply(ies) when the transfer is necessary for important reason of public interest, where the cyber threat information shared internationally is necessary to help protect the EU institutions, bodies and agencies. Based on Article 249 Treaty of the Functioning of the EU:“ The Commission shall adopt its Rules of Procedure so as to ensure that both it and its departments operate. It shall ensure that these Rules are published. In this context, public interest includes the processing operations needed for the management and functioning of the European institutions. This legal ground stems from Articles 3, 7, 14 and 15 Commission Decision 2017/46 on the security of communication and information systems in the European Commission. In addition, articles 36 and 37 of Regulation 2018/1725 apply as well as articles 13.7 of Commission Decision 2015/443. The processing of personal data is necessary for the protection of the EC’s information technology systems and infrastructures and proportionate to the fundamental rights and freedoms of the data subjects. The protection of other EUIs has also been taken into account and is part of the mandate of CERT-EU as described in the Interinstitutional 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.
14 - How is data stored? What are the security measures implemented?	CERT EU has implemented security measures to protect server hardware, software and the network from accidental or malicious manipulations and loss of data. Data is stored on servers managed by CERT-EU in line with the technical security provisions laid down in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, its subsequent versions, its implementing rules (as adapted from time to time) and the corresponding security standards and guidelines, as well as the Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on the security in the Commission, its implementing rules and the corresponding security notices or on servers managed by the respective EU institutions, bodies and agencies. These documents (as adapted from time to time) are available for consultation at the following address: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en.
15 - For more information, including how toexercise your rights to access, rectification, objectand data portability (where applicable) see the data protection notice	the process on how to exercise the rights is described on data protection notice
15a - Data subject rights	Right to have access
16 - Legal Basis	Inter-institutional Arrangement 2018/C12/01
17 - Lawfulness of processing	The data processing is considered lawful under art. 5.1 (a), (b) of the Regulation (EC) 2018/1725, because it 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, Processing is necessary for compliance with a legal obligation to which the controller is subject.
18 - Data minimisation	The listed data items are the required data to ensure the proper execution of the CERT-EU tasks and related supporting operations.
19 - Accuracy	All the information are collected by means of automatic and manual operations. The information about data subjects that are managed by the EUIBAs are acquired through formal processes entailing data quality. Information about data subject external to the EUIBAs could not have the same level of accuracy due to the specific mature of some actions (E.G., use of false information when hacking systems).

20 -Threshold assessment, fill in the specific Threshold assessment-Risks entry in sharepoint.	N/A
21 - Special category data	Not applicable.
22 - DPIA	Not required as the processing operation does not involve high level risks.
23 - Link to the Threshold assessment-Risks	N/A
24 - Other related documents	N/A