European Union Agency
for Cybersecurity
Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

RECORD NO: 91

EU CYBERSECURITY RESERVE

Record 91 of processing operation "EU Cybersecurity Reserve"	
Date of last update	18/2/2026
Name and contact details of controller	ENISA, Operational Support Unit (OSU), osu [at] enisa.europa.eu
Name and contact details of DPO	dataprotection [at] enisa.europa.eu
Name and contact details of Joint Controller	N/A
Name and contact details of processor	• Unit of DIGIT.A3, Directorate- General for Informatics (DIGIT) of the European Commission, that provides the CIRCA-BC platform and relevant technical support. Additional information is available under Record No 45 - CIRCA-BC and Secure CIRCA-BC Document management platforms; • Relational FS offering the JIRA platform under EC Framework Contract DI/08030 – SIDE III to which ENISA is also a party.
Purpose of the processing	The purpose of this processing operation is to avail, under it's capacity as the contracting authority, and monitor proper management and delivery of pre-committed services of a trusted managed security service providers for incident response, and/or preparedness services related to incident prevention and response where those pre-committed services are not used, to Member States' cyber crisis management authorities and CSIRTs, DEP-associated third countries or CERT-EU on behalf of Union institutions, bodies, offices and agencies.
Description of data subjects	• ENISA staff members involved in EU Cybersecurity Reserve; • Nominated Single Points of Contact (SPOCs) from MS; • Nominated representatives of entities designated to act as SPOCs for DEP-associated third countries; • CERT-EU staff members involved in EU Cybersecurity Reserve; • Nominated representatives of entinties requesting a service; • Nominated representatives from selected trusted managed security service providers responsible for provision of a service.
Description of data categories	• Contact data including First and Last Name, email address, position, representing entity; • Data related to Jira usage, available under Record No 90 - Jira OCI; • Data related to CIRCA-BC usage, available under Record No 45 - CIRCA-BC and Secure CIRCA-BC Document management platforms;
Time limits (for the erasure of data)	• Data related to interactions between ENISA and users of EU Cybersecurity Reserve according to Article 14 (3) of Regulation (EU) 2025/38 (i.e. EU MS, CERT-EU, DEP-associated third countries) are retained for two (2) years. • Data related to interactions between the users of EU Cybersecurity Reserve (i.e. EU MS, CERT-EU, DEP-associated third countries) and trusted managed security service providers are retained for five (5) years. • Data related to interactions between trusted managed security service providers and entities benefiting from support from EU Cybersecurity Reserve,

	according to Article 14 of Regulation (EU) 2025/38 are retained for five (5) years. • Data related to financial transactions are retained in accordance with Record 17 - Financial transaction.
Data recipients	• **"**Entity**";** a natural or legal person created and recognized as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations, according to the definition of Article 6 (38) of Directive (EU) 2022/2555 (L 333); • "Union entities"; the Union institutions, bodies, offices and agencies set up by or pursuant to the Treaty on European Union, the Treaty on the Functioning of European Union (TFEU) or the Treaty establishing the European Atomic Energy Community, as per the definition provided in Article 1 point (1) of Regulation (EU, Euratom) 2023/2841 • User"; ○ in the case of EU MS: cyber crisis management authority and CSIRT as referred to, respectively in, Article 9(1) and (2) and Article 10 of Directive (EU) 2022/2555; ○ in the case of CERT-EU: the Cybersecurity Service for the Union institutions, bodies, offices and agencies (CERT-EU) in accordance with Article 13 of Regulation (EU, Euratom) 2023/2841; ○ in the case of DEP-associated third countries: means a competent authority such as computer security incident response team and cyber crisis management authority or equivalent entity and cyber crisis management authority of DEP-associated third countries, in accordance with Articles 14 (3) (c) and 19 (8) of Regulation (EU) 2025/38 • Designated staff of ENISA IT and ENISA contractors responsible for system operation and maintenance, in case of troubleshooting or investigation of security incidents. • The data may also be available to EU bodies charged with monitoring or inspection tasks in application of EU law (e.g., internal audits, European Anti-fraud Office – OLAF).
Transfers to third countries	Further to data transfers across EU and EEA/EFTA countries, tranfers take place with DEP-associated third countries. Any transfer of personal data outside the EU/EEA is performed in compliance with Chapter V EUDPR.
Security measures - General description	General security policy and technical/organisational measures applicable to ENISA's internal IT systems. and external platforms such as JIRA and CIRCA-BC.
Privacy statement	Available to all data subjects when joining the EU Cybersecurity Reserve and on ENISA intranet..