European Union Agency for Cybersecurity (ENISA)
Agamemnonos 14 | Chalandri 15231 | Attiki | Greece | info@enisa.europa.eu | www.enisa.europa.eu

TLP - CLEAR

Record No 96

Cyber Resilience Act's Single Reporting Platform (CRA SRP)

Record 96 of processing operation "Cyber Resilience Act's Single Reporting Platform (CRA SRP)"	
Date of last update	07/09/2026
Name and contact details of controller	ENISA, Operations and Situation Awareness Unit, Incidents and Vulnerabilities Services (IVS), CRA-SRP Helpdesk, cra-srp-helpdesk [at] enisa.europa.eu and Operational Cooperation Unit, OCUtools [at] enisa.europa.eu
Name and contact details of DPO	dataprotection [at] enisa.europa.eu
Name and contact details of Joint Controller	N/A *Note that EU-login (ECAS account), used for identification/authentication of Appointed Representatives (ARs) to the platform is provided by European Commission (DIGIT) directly (who acts as data controller to this end). Contact: DIGIT-CIRCABC-SUPPORT [at] ec.europa.eu*
Name and contact details of processor	• Microsoft Azure offering MS Defender, under the Cloud II Framework Contract, to which ENISA is party; used for the SRP platform security protection; • UniSystems Luxembourg SARL, under a contract with ENISA, responsible for the development and maintenance of the SRP platform; • WEDOS SARL, under a contract with ENISA, responsible for security protection (DDOS) of the SRP platform; • Amazon Web Services offering Simple Email Service of (Amazon SES), under the Cloud II Framework Contract, to which ENISA is party, used for sending automated emails/notifications. *Note: Amazon SES only sends emails and it does not store any information for business use, apart from technical usage data that are necessary for the provision of the service (for example, emails bouncing back).* • ENISA contractors' responsible for security assessment and penetration testing of the platform.
Purpose of the processing	The purpose of this processing operation is to make available, maintain and manage day-to-day operations of the single reporting platform pursuant to articles 14 and 16 of Regulation

	(EU) 2024/2847 (CRA) and facilitate receiving and communicating notifications.
Description of data subjects	The data subjects are users of the platform: • ENISA staff members assigned to activities related to CRA SRP; • ENISA staff members and ENISA processors' appointed staff members under their capacity as platform administrators; • designated users from CSIRTs; • assigned representatives (AR) from manufacturers; • open-source stewards;
Description of data categories	• For ENISA staff members, CSIRTs designated users and ENISA contractors' staff members: o Identification data related to KeyCloak including Full name, email account, userID; • For Assigned Representatives (AR) and Open-source stewards: o EU-Login userID, First and Last name, email address o manufacturer details including name, designated CSIRT, additional information (optional) • Data reported/notified that might contain personal data • Audit logs and security protection (including DDoS protection) o IP addresses, browser agent/browser detail, connection details etc
Time limits (for the erasure of data)	• For ENISA and CSIRT users personal data are retained for as long as they are formally appointed to collaborate or facilitate collaboration through the SRP or until requested to be removed. • For assigned representatives, having validated association with a manufacturer, personal data is retained for as long as they are validated or until requested to be removed. • For assigned representatives having no validated association with manufacturer, personal data is retained for maximum 12 months or earlier upon request. • Personal data included in the notification will be redacted 10 years after the reporting has been marked as archived by the relevant CSIRT. • Security and Audit logs that may contain personal data are retained for 12 months.
Data recipients	Access to your data will be granted only to dedicated ENISA staff members, ENISA contractors' dedicated staff members,

	designated CSIRTs staff members, in their role as designated coordinator or concerned CSIRTs and CSIRTs through electronic notification end points. 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	No transfer outside EU/EEA is foreseen.
Security measures - General description	General security policy and technical/organisational measures applicable to ENISA's internal IT systems and external platforms.
Privacy statement	Available within the platform to all SRP platform users.