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: 33

CSIRTS NETWORK SECRETARIAT

Record 33 of processing operation "CSIRTs Network Secretariat"	
Date of last update	25/07/2024
Name and contact details of controller	ENISA, Operational Cooperation Unit (CSIRTs Network Secretariat), cnw [at] enisa.europa.eu
Name and contact details of DPO	dataprotection [at] enisa.europa.eu
Name and contact details of Joint Controller	The national organisations participating in the CSIRTs network (CSIRTs Network members) with regard to incident information sharing through the CSIRT co-operation portal website and the relevant mailing lists. Contacted via CSIRTs Network Secretariat.
Name and contact details of processor	L-Soft: mailing list provider listserv (www.lsoft.com), based in Sweden (contract with ENISA). DFN-CERT Services GmbH: encrypted mailing list provider, based in Germany. Microsoft GitHub Enterprise Cloud: support tool offered optionally to the CSIRTs network members upon request and to ENISA staff, based in US (subscriptions purchased through EC DG DIGIT SIDE II Framework Contract). Microsoft AzureAD Connect Health: Active Directory Federation Services (ADFS) Health Service provider, based in EU. The service is used to strengthen the security of the authentication service in the CISRT's portal. It is obtained through SLA with European Commission DG DIGIT.
Purpose of the processing	The purpose of this processing operation is to: 1) Facilitate ENISA's management of the CSIRTs Network Secretariat (management of contact points and communication, meetings organisation, sharing of documents, maintenance of mailing lists, etc.), as this is established by the article 12 (1) & (2) of the Directive on security of network and information systems (NIS Directive). 2) Actively support the cooperation among the CSIRTs by allowing non-sensitive information exchange, in accordance with the NIS Directive and relevant Terms of Reference of the CISRTs network (information on organisational, governance, working group matters, as well as operational topics). 3) Ensure service continuity through proactive detection of any technical issues.
Description of data subjects	CSIRTs network members for administrative purposes. For operational data (information exchange) potentially any individual whose personal data are processed in the context of an incident information sharing within the CSIRTs network (see data categories).
Description of data categories	The following personal data are collected: (a) Administrative data on CSIRT network members: first name, surname, organisation, position held, address, email, telephone number, picture (optional). These data are necessary for the management of the CSIRTs Network Secretariat by ENISA. (b) Ad hoc personal data that might be included in the context of information sharing on incidents through the CSIRT co-operation portal website and relevant mailing lists (operational data). Depending on the type of incident, this information

	might include: any file (with user id included) stored in or transmitted from / to a host involved in an incident (as victim, relay or perpetrator), email addresses, user account name (for operating systems, applications, centralised authentication services, etc.), technical protocol data (IP address, MAC address). These data might be shared by the CSIRT network member organisations, who are also joint controllers to this end. Note: ENISA does not generate itself operational data but rather supports the exchange of operational data between CSIRT network members. (c) For the Microsoft GitHub Enterprise Cloud service: account information (username, name, email), device info; usage info (IP address, session, etc.); profile data. Note: this service is optional and may be used only for those members of the CSIRTs network that explcitly ask for it (at the moment only used by designated ENISA staff). (d) For the Microsoft Azure AD Connect Health service: account usernames, server logs related to the authentication service to the CSIRTs portal.
Time limits (for the erasure of data)	Administrative data of the CSIRT network members are kept for as long as a person is appointed member of the CSIRT network by his or her Member State. Operational data will be kept for as long as the information sharing on a particular incident is required, in accordance with rules and procedures of the CSIRTs network. Data related to incidents that are older than 3 years will be kept for operation needs but irrelevant personal information will be removed and the remaining data will be stored on the Cooperation Portal in a folder that is encrypted with the PGP keys of the CISRT network members. Log data from the CISRT network systems and similar data will be stored for a maximum period of three years. Data that needs to be kept longer to allow investigating breaches that took place in the past will be stored according to the highest security standards. For the Microsoft GitHub Enterprise Cloud service: until 90 days after cancellation or termination of a user's account (though some information may remain in encrypted backups). For the Microsoft Azure AD Connect Health service: until 30 days from the data generation.
Data recipients	All members of the CSIRTs Network and the ENISA staff responsible for the operation of the CSIRT Network Secretariat. The processor's staff with regard to the processing of data in the context of the CISRT network mailing list. In rare cases, an ENISA contractor (developer) might require access to the system for debugging purposes (under supervision by ENISA staff). The providers of multifactor authentication services have access to a strictly defined subset of data to enable them to provide the service to ENISA. The access to the data is both limited in scope and time. All CSIRT members have access to contact information regarding the rest of the members. For Microsoft GitHub Enterprise Cloud service: staff of the processor and involved subprocessors (https://docs.github.com/en/free-pro-team@latest/github/site-policy/github-subprocessors-and-cookies). For Microsoft Azure AD Connect Healt: staff of the processor, in the Microsoft EU Datacentres.
Transfers to third countries	CSIRTs network data are not transfered to third countries. As regards the Microsoft GitHub Enterprise Cloud service, personal data related to users' accounts are stored in US (Microsoft GitHub and subprocessors). This tool is auxiliary/optional and individual registration to the service is provided only upon request to ENISA of a CSIRTs network member. The Microsoft Azure AD Connect Health service is provided within EU.
Security measures - General description	PGP Encryption for the operatinal mailing list. Multifactor Authentication for access to the Portal. Best practices followed for Mailing lists and Portal. Portal regularly pentested.
Privacy statement	Available through CIRST network members/portal.