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: 66

MELICERTES TOOLS COLLECTION (CHAT MESSAGING PLATFORM, IDENTITY SERVICE PROVIDER, TEAMS MANAGEMENT SOFTWARE, DOCUMENTS EXCHANGE PLATFORM)

Record 66 of processing operation “MeliCERTes Tools collection (chat messaging platform, identity service provider, teams management software, documents exchange platform)”

Date of last update	24/01/2023
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	ENISA is responsible for the IT operations, support and maintenance of the MeliCERTes tools collection. The national organisations participating in the CSIRTs network (CSIRTs Network members) are responsible with regards to incidents information sharing through the operational tools, like the CSIRT co-operation portal, the relevant mailing lists, the chat messaging platfrom. Contacted via CSIRTs Network Secretariat.
Name and contact details of processor	ENISA/OCU is the business owner of the systems for their IT operations, support and maintenance and under the CNW Secretariat role. In addition, the Simple Email Service of Amazon Web Services is used to especially support the operation of the MeliCERTes tools collection. Following the service specification, the service is used for sendingautomated outgoing emails that are generated by the operational tools like the identity provider and the chat messaging platform. It 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). Technical data storage at rest is within the EU only. The service is obtained via the European Commission's Cloud II Framework Contract which ENISA uses to cover business needs.
Purpose of the processing	The “MeliCERTes 2" project (SMART2018/1024 project, contract NUMBER - LC-0133746) was 100% EU-funded, for which the European Commission was the owner of its outcomes until 18/12/2022. Since then, the legal ownership was

	transferred to ENISA with the handover letter of 16/12/2022, Ref. Ares (2022)8749927. The collection of tools used under the MeliCERTes Facility and which may include processing of personal data are: IAM/SSO (Identity and Access Management solution/Single Sign On) used for federated authentication. User accounts, user logs containing personal data are created and maintained.Chat messaging platform. Users, logs, posts, files.Video Teleconference system. Users in the admin part of the application.Team Management software. Users and teams information, logs.Csirts Network (CNW) Portal for files storage and online editing. Users, teams information, files. The overall purpose is to support the CSIRT Network in the operational information exchange and incident response. Record No 33 provides more info for the CNW processing activity. Further to this, monitoring and logging software as service mechanism is used for better visibility on the security status of the above mentioned tools eg Microsoft Defender and Redhat Insights. In both services, diagnostic data is stored and further processed in pseudonymised form. Retention period in ENISA's tenant is configurable by ENISA (minimum 1 month). Record No 47 covers the processing of personal data with Microsoft Defender
Description of data subjects	• CNW Members- ENISA CNW Secretariat • ENISA OCU staff members dealing with tools IT operations • ENISA/OCU contractors for the support and maintenance of the tools • 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	• Reports • IoCs - Indicators of Compromise • Users accounts info • Posts • Logs • Ad hoc personal data that might be included in the context of information sharing on incidents through the tools. Note: ENISA does not generate itself operational data but rather supports the exchange of operational data between CSIRT network members.
Time limits (for the erasure of data)	Personal data of platform users will be kept until their nomination is revoked or they request to be removed. Backups of data are kept for 6 months.
Data recipients	- All the beneficiaries of MeliCERTes can view certain personal data (depending on the tool) of the beneficiaries for team management purposes and information exchange. - All admin users in the tools, this means ENISA/ OCU staff and ENISA/OCU contractors that deal with the support and maintenance of the tools 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	All MeliCERTes tools and backups are hosted on ENISA premises with the exception of the Simple Email Service (SES) of Amazon Web Services and MS Defender and RH Insights (used to especially support the operation of the MeliCERTes tools collection). Following the SES service specification, the service is used for sending emails only 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). Technical data storage at rest is within the EU only. Any transfer of personal data outside the EU/EEA is performed in line with Chapter V Regulation 1725/2018 (EUDPR). MS Defender Microsoft Defender is a cloud service that offers:

	Security posture managementAntimalwareEndpoint detection and response (EDR)Extended detection and response (XDR)Virtual machine behavioral analytics and security alertsThreat detection for OS-level and Network-levelSecurity Policy and Regulatory ComplianceQualys vulnerability assessmentFile integrity monitoringand more. It keeps diagnostic (pseudonymised) data in EU. (Microsoft 365 Defender data security and privacy | Microsoft Learn .) MS Defender for Cloud uses Azure Arc to protect non-Azure machines. (Plan Defender for Servers agents and extensions deployment | Microsoft Learn) Relevant public record on https://inet/edo/cntr/dpo/Lists/records/DispForm.aspx?ID=58 Redhat insights is a SaaS (US located) which offers value in our environment, proactively identifying and remediating threats, assessing vulnerabilities, analysing compliance, creating inventories, determining missing patches, identifying configuration risks. By default, no personal information is collected: The design principle with Insights is simple: collect only the minimum data that is needed for analysis, issue identification, and remediation. Complete volumes of system information such as core dumps or full log files are not collected. Insights, by default, does not collect personal information. Red Hat Insights for Red Hat Enterprise Linux Technical FAQ - Red Hat Customer Portal
Security measures - General description	• Enabled MFA • Hardened images • Implementation of referenced security baselines • Enabled auditing and logging • Logs collection to ENISA Splunk • Logs monitoring and analysis • Incident response
Privacy statement	Available to the CIRST network members via the portal.