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: 58

SERVER AND ENDPOINT SECURITY

Record 58 of processing operation "Server and Endpoint security"	
Date of last update	17/07/2025
Name and contact details of controller	ENISA, Corporate Support Services (CSS), IT Sector, it [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	• Microsoft Ireland, which provides the relevant services under a Framework Contract with the European Commission (Inter-Institutional Licensing Agreement - ILA to which ENISA is a party). • Fortinet B.V., which provides relevant licencing services for cybersecurity solutions deployed at ENISA servers and endpoints, under a Framework Contract to which ENISA is a party.
Purpose of the processing	Providing threat detection and response capabilities on ENISA endpoints. In particular: • Microsoft Advanced Threat Protection (ATP, also known as Defender for Endpoint) solution is applied, offering anti-malware/virus protection and allowing for centralised monitoring and logging capablities for the security of endpoints, in combination with Microsoft inTune for endpoints; • Microsoft inTune remotely enforcing security policies and, thus, reducing the risk of data breaches; • FortiAuthenticator as a RADIUS authentication server with Multi-Factor Authentication (MFA) and FortiClient Endpoint Management Server (EMS), for remote access (VPN) and ZTNA (Zero Trust Network Access) tagging, to achieve secure context-aware remote (VPN) and internal (LAN) access to internal resources;
Description of data subjects	All ENISA users of endpoints (laptops, mobile devices etc) i.e. ENISA contract and temporary agents, interim agents, SNEs, etc.
Description of data categories	**For ATP (Microsoft Defender for Endpoint):** • Diagnostic data that are continuously sent in pseudonymised form by the ENISA endpoints to ENISA's tenant in Microsoft's cloud for anti-malware/anti-virus checking. It is highly recommended by Microsoft that diagnostic data in ATP are activated in order to provide the service. • Customer data: content potentially associated with diagnostic data (e.g. file metadata, emails if malicious). Customer data are not continuously sent to Microsoft, but only in case of suspicion (in such case, diagnostic data are re-identified and relevant customer data are obtained from end-point and sent to ENISA's tenant in the cloud for further analysis). If the malicious event is confirmed, an alert is sent to endpoint. *For further information on Microsoft Defender, please see: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/data-storage-privacy?view=o365-worldwide* **For the Defender on Identity service:**

	• The service is linked to ATP and provides for endpoints related logging. In particular, it processes personal data from ENISA's Active Directory, including network activity and history (e.g. network traffic to and from domain controllers, security events, etc.). These data are used by Microsoft to proactively identify indicators of attack, generate alerts and enable the investigation of security threats in the network. *For further information, please see: https://docs.microsoft.com/en-us/defender-for-identity/privacy-compliance* **For inTune:** All required data for the operation of the service, as regards the endpoints at ENISA. A list of these data is provided here: https://docs.microsoft.com/en-us/mem/intune/protect/privacy-data-collect *Note: All optional data (Microsoft diagnostics) have been de-activated for inTune.* **For FortiAuthenticator:** • User data for secure authentication and access control including first and last name, email address, work phone number, company, department and work title. • FortiAuthenticator generates and logs Authentication Data specific to each login attempt, including timestamps, success/failure status, source IP and potentially MAC addresses, and details related to the user's FortiToken (serial number, MFA response, etc) **For FortiClient Endpoint Management Server (EMS):** • Data from managed devices such as device identifiers (MAC addresses, IP addresses, hostname), • User data and identity details such as logged-in username, domain, email, work phone number and some • Endpoint security posture data necessary for ZTNA tagging such as OS version, patch status, network connectivity, VPN connection details, antivirus and firewall status, disk encryption, and compliance with defined security baselines. • Endpoint telemetry and user session data to establish and maintain secure access based on device posture
Time limits (for the erasure of data)	For ATP (Microsoft Defender for Endpoint), FortiAuthenticator and FortiClient EMS: The current retention period applied by ENISA is 6 months. For Defender for Identity: After a user is deleted from ENISA's Active Directory, Defender for Identity automatically deletes the user profile and any related network activity within a year. For inTune: For as long as an endpoint device is enrolled in the service. After active deletion by ENISA, the personal data are removed from inTune (by Microsoft) within 30 days. Audit logs are retained for up to one year for security purposes. For further information regarding retention, deletion and destruction by Microsoft, please see: https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview?view=o365-worldwide.
Data recipients	Designated ENISA staff including ISO and IT functions responsible for managing and maintaining the security posture of the Agency. Designated staff of the ENISA processors that are involved in the management of the services might also have access for providing support and analysis. 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	For ATP, diagnostic (pseudonymised) data may be sent to Microsoft's global Threat intelligence database in the US. In addition, Microsoft sub-processors may be involved for technical support (follow-the-sun), in which cases (e.g. when a support ticket is opened) transfers of personal data (e.g. of staff handling the ticket) to third countries may take place. The EC SCCs are used as basis for such transfers under the European Commission's Microsoft ILA.

Security measures - General description	General security policy and technical/organisational measures applicable to ENISA's IT systems. In addition, security measures of the processor (under the European Commission's ILA for Microsoft online services).
Privacy statement	Information on endpoint security and data protection is available to all ENISA staff, further to the ENISA security policy.