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

ENDPOINT SECURITY

Record of processing activity	
Title	Endpoint security
Name and contact details of controller	ENISA, Corporate Support Services & ISO
Name and contact details of DPO	dataprotection@enisa.europa.eu
Name and contact details of Joint Controller	
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 subject). The services are covered by the ILA's Data Processing Adendum.
Purpose of the processing	Improving the current threat detection and response capabilities on the ENISA endpoints (laptops) by deploying a modern endpoint detection and response. In particular, the Microsoft Advanced Threat Protection (ATP, also known as Defender for Endpoint) solution is applied, in combination with Microsoft inTune for endpoint (only for ENISA endpoints/laptps). The ATP/Defender service is an anti-malware/virus protection system, allowing also for centralised monitoring and logging capablities for the security of endpoints (Microsoft Defender for Identity service). The inTune service enhances protection by remotely enforcing security policies and, thus, reducing the risk of data breaches. All services are part of Microsoft's online services and fall under the provisions of the Data Procesing Adendum between the European Commmission and Microsoft (European Commission's Microsoft ILA).
Description of data subjects	All ENISA users of endpoints (laptops), i.e. ENISA contract and temporary agents, interim agents and SNEs.
Description of data categories	For ATP (Microsoft Defender for Endpoint): a) 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. b) 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 for 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 (laptops) at ENISA. A list of these data is provided here: https://docs.microsoft.com/en-us/mem/intune/protect/privacy-data-collect All optional data (Microsoft diagnostics) have been de-activated for inTune.
Time limits (for the erasure of data)	For ATP (Microsoft Defender for Endpoint): 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	ENISA ISO and IT team; Designated staff of data processor (Microsoft - storage in ENISA's Azure tenant within EU).
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 open) 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	Security measures of the processor (under the European Commission's ILA for Microsoft online services). Note: The applied services are aimed to strengthen ENISA's endpoint security (and subsequently protect information, including personal data, stored at endpoints).
Privacy statement	Information on endpoint security and data protection to be communicated internally to all staff.