

RECORD NO: 58

SERVER AND ENDPOINT SECURITY

Record 58 of processing operation “Server and Endpoint security”

| | |
|--|--|
| Date of last update | 07/04/2025 |
| 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 subject). The services are covered by the ILA's Data Processing Adendum. |
| Purpose of the processing | <p>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/laptops).</p> <p>The ATP/Defender service is an anti-malware/virus protection system, allowing also for centralised monitoring and logging capabilities for the security of endpoints (Microsoft Defender for Identity service).</p> <p>The inTune service enhances protection by remotely enforcing security policies and, thus, reducing the risk of data breaches.</p> <p>All services are part of Microsoft's online services and fall under the provisions of the Data Processing Adendum between the European Commission and Microsoft (European Commission's Microsoft ILA).</p> |
| Description of data subjects | All ENISA users of endpoints (laptops), i.e. ENISA contract and temporary agents, interim agents, trainees and SNEs. |
| Description of data categories | <p>For ATP (Microsoft Defender for Endpoint):</p> <ul style="list-style-type: none"> 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. <p>For the Defender for Identity service:</p> <ul style="list-style-type: none"> 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 |



| | |
|---|--|
| | <p>indicators of attack, generate alerts and enable the investigation of security threats in the network.</p> <p>For inTune:</p> <ul style="list-style-type: none"> All required data for the operation of the service, as regards the endpoints (laptops) at ENISA. |
| Time limits (for the erasure of data) | <p>For ATP (Microsoft Defender for Endpoint): The current retention period applied by ENISA is 6 months.</p> <p>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.</p> <p>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.</p> |
| Data recipients | <p>ENISA ISO, OCU and IT team, Designated staff of data processor (Microsoft - storage in ENISA's Azure tenant within EU).</p> <p>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).</p> |
| Transfers to third countries | No transfers outside EU/EEA are foreseen. |
| Security measures - General description | <p>Security measures of the processor (under the European Commission's ILA for Microsoft online services).</p> <p><i>Note: The applied services are aimed to strengthen ENISA's endpoint security (and subsequently protect information, including personal data, stored at endpoints).</i></p> |
| Privacy statement | Available at ENISA intranet. |

