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: 72

SERVICENOW ITSM

Record 72 of processing operation “ServiceNow ITSM”

Date of last update	11/6/24
Name and contact details of controller	ENISA, Corporate Support Services (IT) (itsupport [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	ServiceNow Nederland B.V., Hoekenrode 3,1102 BR, Amsterdam Zuidoost, (THE NETHERLANDS) Sub-processors (in case of requested and authorised support) - Further information are provided below in the section "Transfer to third countries": ServiceNow, Inc. (USA), ServiceNow Australia Pty Ltd (Australia), ServiceNow Software Development India Private Limited (India), ServiceNow UK Ltd. (United Kingdom). ServiceNow Ireland Limited (Ireland) and ServiceNow Japan K.K (Japan) (collectively, "Sub-Processor Affiliates"). A master Subscription Service Agreement between ServiceNow and DIGIT is available.
Purpose of the processing	The purpose of this processing operation is to support various ENISA IT management processes that are required for the agency's IT and systems operation (e.g. access rights to various internal systems/ internal tools/services, corporate email management, corporate device management (e.g. laptops, mobile phones), IT systems software and hardware inventory (e.g. physical and virtual servers, software).
Description of data subjects	All ENISA staff, including statutory staff, SNEs, interims,trainees and intra-muros.
Description of data categories	Personal data associated with user management and administration within different internal ENISA IT systems, i.e. - user account information of ENISA staff (name, username, position/department/unit), associated access rights and user account information of ENISA staff using ServiceNow (ServiceNow local accounts) - device ID(s) associated to ENISA users, - troubleshooting tickets, issues referred to IT by ENISA users, etc. - requests issued to IT by ENISA users - comments and ratings in knowledge base articles The above-mentioned data on user accounts can be imported from ENISA Active Directory, other ENISA IT system like SCCM (System Center Configuration Manager) and user input (for tickets, requests, comments and rating)

Time limits (for the erasure of data)	The retentions policy for the tickets varies depending on the nature of the tickets. The incidents will be retained for 48 months in the system in order to have a record of issues of each device for warranty proposes. The requests will be held for 30 months for traceability; for example, user rights, similar requests. During both periods mentioned above, aggregated data will also used for statistic proposes. After the corresponding period, the ticket/request will be deleted from the system. Comment and rating for the knowledge articles are deleted upon request from the user. When the user is removed from the system most connections with him/her are removed, except in cases where data such as audit logs and history on the records that cannot be removed from the system and remains visible only to system administrators.
Data recipients	Designated ENISA staff involved in IT management, ENISA Information Security Officer, Service Now dedicated staff responsible for technical support, ENISA contractors' tasked with the development of the platform. 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	Personal data may be transferred to ServiceNow affiliates in third countries when a request for advanced technical support is made by ENISA platform administrators to ServiceNow. The personal data transferred and the ServiceNow affiliate involved would depend on the nature of the technical issue. Access will be granted, upon ENISA IT approval, via a dedicated account with the access rights needed and for a predefined time period. Any transfer of Personal Data outside the EU/EEA takes place in accordance with Chapter V of the EUDPR or Chapter V of the GDPR. The data importer has entered into standard data protection clauses, in accordance with Article 46(2)(c) of GDPR. Technical features such as access controls and database encryption are used to limit the scope and protect the data.
Security measures - General description	Technical/organisational measures include ENISA's SSO, access control, encryption at transfer and at rest, bring your own key etc.
Privacy statement	Available through the platform.