EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

08 August 2022
EMA/684879/2022

Record of data processing activity
EMA IT Security Operations Centre (SOC)

1.	Last update of this record, version number:	New
2.	Reference number:	EMA-I-003
3.	Name and contact details of controller:	Controller: European Medicines Agency Contact: Head of Information Management datacontroller.infomanagement@ema.europa.eu
4.	Name and contact details of DPO:	dataprotection@ema.europa.eu
5.	Name and contact details of joint controller (where applicable)	N/A
6.	Name and contact details of processor (where applicable)	Airbus CyberSecurity SAS Zac de la Clef Saint Pierre 1 Rue Jean Moulin 78990 Elancourt – France
7.	Purpose of the processing	In support of the IT security operations, the purpose of the processing of personal data is to: • communicate alerts and warnings relating to IT security events and incidents; • respond to and contain IT security events and incidents;

		• provide tools and facilitate operations through security audits, security assessments and vulnerability management; • increase the awareness of EMA staff in the field of cyber security and provide training to staff; • monitor, detect and prevent the occurrence of IT security events and incidents; • review privileged user accounts.
8.	Description of categories of persons whose data EMA processes and list of data categories	Description of categories of persons whose data EMA processes **Internal to EMA:** • Everyone with an active EMA account, users, owners and operators of EMA IT systems; • Individuals involved in IT security incidents or events that occur in the EMA IT systems (such as perpetrators and victims); • Owners of EMA IT assets involved in malicious traffic or subject to a specific vulnerability or infection; • Individuals who receive alerts and warnings from EMA SOC services; • Individuals who use corporate IT assets which are onboarded to the EMA SOC services. **External to EMA:** • Everyone with an active EMA account, users, owners and operators of EMA IT systems (including contractors with or without an EMA domain email address); • Individuals involved in IT security incidents or events that occur in EMA IT systems (such as perpetrators and victims); • Individuals who receive alerts and warnings from EMA SOC services; • Individuals who send an e-mail to the EMA without the ema.europa.eu or ext.ema.europa.eu domain; • Individuals who use publicly accessible EMA IT systems (EU Login, EU Guest Wifi, public web servers) and individuals who send e-mails to the EMA domain from

		outside the europa.eu domain or digitally collaborate with the EMA; • Individuals who had an active EMA account in the last 10 years; • Individuals who use corporate IT assets. **Data categories** • IP addresses, MAC addresses and IT asset inventory information of corporate devices and of non-corporate devices that are used to connect to EMA IT systems such as for example the IP address of home routers connected to the EMA VPN network during telework are processed in the security logs. Professional contact details; • Names, alias names and professional roles; • Only if there is an indication of malicious activity: e-mail content and file content; • System, application, web access and e-mail logs, network traffic and metadata; • Access rights of privileged accounts (departments and groups to which users belong, the hierarchy of roles and status of the staff -active/non-activate); • Mobile device serial numbers of corporately managed devices; • Location from where the user was connected (only if an indication of potential malicious activity is identified).
9.	Time limit for keeping the data	A three months retention period is applicable. The retention period starts from the time of the creation of the log.
10.	Recipients of the data	Personal data is only shared with recipients if this is necessary for the purpose of offering security operations and services i.e., • EMA SOC security team involved in managing the SOC services; • The SOC security team of the Processor, analysing suspicious events.

		The data collected may also be processed internally by administrators and technical teams of I-Division to further investigate a confirmed security incident.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	N/A
12.	General description of security measures, where possible.	Technical and organisational measures in place to ensure information security: • Physical security perimeter to data centres and EMA premises. • Security guards to protect the EMA premises. • Sophisticated access controls to IT systems that process personal data. • Monitoring and auditing controls. • Security clearance for operators who provide security services. • Sensitive information is shared in encrypted format to ensure secure transfer.
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	Details concerning the processing of your personal data are available on the Agency's website at: https://www.ema.europa.eu/en/about-us/legal/general-privacy-statement