15 January 2024
EMA/684090/2022
Information Management Division

European Medicines Agency's Data Protection Notice

For the Security Operation Centre (SOC)

This Data Protection Notice explains the most essential details of the processing of personal data by the European Medicines Agency (hereinafter "EMA" or "Agency") in the context of setting up and operating the Security Operation Centre (SOC).

1. Who is responsible for the processing of your data?

1.1. Who is the data controller?

The European Medicines Agency ("EMA") is ultimately responsible to comply with your data protection rights and freedoms. On behalf of EMA, the Head of the Information Management Division (I-Division) is appointed as 'Internal Controller' to ensure the lawful conduct of this processing operation.

You may contact the Internal Controller via the following email address:
datacontroller.infomanagement@ema.europa.eu

1.2. Who is the data processor?

The Agency may engage third parties to process data on behalf of the Agency and, in particular, to carry out the following activities:

- Providing access to cybersecurity expertise, services and tools, and
- Setting up SOC processes, systems and resources.

In support of these two activities, EMA is using the following processor:

Airbus CyberSecurity SAS

Zac de la Clef Saint Pierre 1 Rue Jean Moulin

78990 Elancourt

France

2. Purpose of this data processing

In the context of the Agency's mission and tasks as set out in Regulation (EC) No 726/2004[1] and other applicable Union legislation, the purpose of this data processing activity is the provision of EMA cybersecurity capabilities, which include, *inter alia*, the prevention of data leaks.

As part of a SOC, a security team, which consists of both security analysts and engineers, oversees activities on servers, databases, networks, applications, endpoint devices, websites and other systems for the sole purpose of pinpointing potential security threats and thwarting them as quickly as possible.

A SOC is not only identifying threats, but analyses them, investigates the source, reports on any vulnerabilities discovered and plans how to prevent similar occurrences in the future. In other words, a SOC is dealing with security problems in real time, while continually seeking ways to improve the organisation's security posture and protection of personal data. More specifically, the purpose of the data processing activities SOC services is to:

- Monitor the Agency's IT environment 24/7/365;
- Detect network intrusions;
- Investigate network intrusions;
- Prevent network intrusions;
- Prevent loss of data;
- Respond to security incidents.

2.1. Personal data concerned

EMA processes data collected by means of automatic traffic analysis and log reporting. Such data may include the below data types.

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);

[1] REGULATION (EC) No 726/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency

- 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.

The data categories can be summarised as follows:

- 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).

2.2. Legal basis of the processing

The legal basis of the processing of personal data in the context of the SOC services is Article 5(1)(a) of Regulation (EU) 1725/20182 i.e., the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in EMA. In accordance with preamble 22 of the same Regulation, processing of personal data for the performance of tasks carried out in the public interest by the Union institutions and bodies includes the processing of personal data necessary for the management and functioning of those institutions and bodies.

The management and functioning of the Agency is further defined as follows:

[2] REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

- Regulation (EC) No 726/20043 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency;
- Financial Regulations4, in particular Article 30(2)(c) stating that for the "purposes of the implementation of the budget of the Union body, internal control shall be applied at all levels of management and shall be designed to provide reasonable assurance of achieving the […] objective[s] of safeguarding of assets and information'' (emphasis added);
- Regulation (EU) 1725/20185, Article 4(1)(f), requiring that personal data "shall processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')";
- Directive (EU) 2016/11486 concerning measures for a high common level of security of network and information systems across the Union.

3. How long do we keep your data?

The retention period of the data is defined by the purpose of storing and applicable internal policies and procedures. For the SOC system, the following retention applies:

- For logs that were escalated to the security incident: 5 years;
- For logs that were escalated to an alert: 12 months and 36 months for encrypted backups in the secure EMA location;
- For logs that did not include alerts or incidents: 7 months; this is for the purposes of technical analysis should subsequent logs indicate alerts and incidents.

After this expiry period, the data becomes permanently erased. Any changes to these policies will be updated in this Data Protection Notice.

4. Who has access to your information and to whom is it disclosed?

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.

[3] REGULATION (EC) No 726/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency

[4] Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council;

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

5. Your data protection rights

As data subject (i.e., the individual whose personal data is processed), you have a number of rights:

- **Right to be informed** – This Data Protection Notice provides information on how EMA collects and uses your personal data. Requests for other information regarding the processing may also be directed to the Internal Controller.
- **Right to access** – You have the right to access your personal data. You have the right to request and obtain a copy of the personal data processed by EMA.
- **Right to rectification** – You have the right to obtain - without undue delay - the rectification or completion of your personal data if it is incorrect or incomplete.
- **Right to erasure** – You have the right to require EMA to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing. In certain cases your data may be kept to the extent it is necessary, for example, to comply with a legal obligation of the Agency or if it is necessary for reasons of public interest in the area of public health.
- **Right to restrict processing** – In a few, codified cases, you have the right to obtain the restriction of the processing, meaning that your data will only be stored, but not actively processed for a limited period of time. For more information about this right and its limitations, see the EMA General Privacy Statement, hosted at www.ema.europa.eu/en/about-us/legal/privacy-statement.
- **Right to object** – You have the right to object at any time to this processing on grounds related to your particular situation. If you do so, EMA may only continue processing your personal data if it demonstrates overriding legitimate grounds to do so or if this is necessary for the establishment, exercise or defence of legal claims.

The rights of the data subject can be exercised in accordance with the provisions of Regulation (EU) 2018/1725. For anything that is not specifically provided for in this Data Protection Notice, please refer to the contents of the general EMA Privacy Statement: www.ema.europa.eu/en/about-us/legal/privacy-statement

6. Recourse

In case you have any questions regarding the processing of your personal data, or you think that the processing is unlawful or it is not in compliance with this Data Protection Notice or the general EMA Privacy Statement, please contact the **Internal Controller** at datacontroller.infomanagement@ema.europa.eu or the **EMA Data Protection Officer** at dataprotection@ema.europa.eu

You also have the right to lodge a complaint with the **European Data Protection Supervisor (EDPS)** at any time at the following address:

- Email: edps@edps.europa.eu
- Website: www.edps.europa.eu
- Further contact information: www.edps.europa.eu/about-edps/contact_en