EMA/124625/2025

European Medicines Agency's Data Protection Notice

For the use of EMA Authentication Services and Microsoft Entra ID

The European Medicines Agency (hereinafter "EMA" or "Agency") processes the personal data of a natural person (individual) in compliance with "Regulation 2018/1725[1].

This Data Protection Notice explains the most essential details of the processing of personal data by the Agency in the context of user authentication, including multi factor authentication via Microsoft Entra ID. This includes the collection and processing of personal data of the Agency's partners and networks[2], interested persons, delegates, EMA staff and contactors and the public. If you belong to one of these categories, it is important that you read and retain this data protection notice, together with other notices EMA provides when it is collecting or using your personal data so that you are aware why EMA is processing personal data and you understand your data protection rights.

Microsoft Entra ID, formerly known as Azure Active Directory (AD), is a cloud-based service that combines core directory services, application access management, and identity protection into a single solution.

1. Who is responsible for processing your data?

1.1. Who is the data controller?

The Agency is ultimately responsible to comply with your data protection rights and freedoms. On behalf of EMA, the Head of Information Security service 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.informationsecurity@ema.europa.eu.

1.2. Who is the data processor?

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

[1] 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

[2] Partners & networks | European Medicines Agency (EMA)

- Maintain the hardware, software and cloud infrastructure required to support processing of data in compliance with EU legislation. The contact details of the processors are the following:
  - NTT Data Belgique SRL
    Société rèsponsabilité limitée/Besloten Vennootschap met Beperkte Aansprakelijkheid
    Rue de Spa 8, 1000 Brussels, Belgium
  - Adinsec BV (Commercial name Grabowsky)
    Gemeenteplein 13,
    1730 Asse, Belgium
  - Microsoft Ireland Operations Limited
    One Microsoft Place, South County Business Park, Leopardstown,
    Dublin 18 D18 P521, Ireland

- Support users in accessing EMA systems by approving, enabling and unlocking user accounts and resetting their multifactor authentication methods. The contact details of the data processor are the following:
  - Axianseu Digital Solutions S.A. (two sub-contractors both based in the EEA)
    Edificio Atlantis, Av.Dom João II, 44C,
    Piso 5, 1990-095 Lisbon,Portugal

2. Purpose of this data processing

The purpose of this data processing activity is the verification and authentication of user accounts to protect EMA's systems against unauthorised access using Microsoft Entra ID authentication, multifactor authentication and risk detection capabilities.

The data held in Microsoft Entra ID is required to:

- Control the access to EMA systems and applications.
- Support the self-service password management.
- Perform necessary identity and security verifications.
- Authorise your access to EMA applications and services.
- Understand and collect data about faults and failures for the purposes of improving services and service delivery.
- Respond to technical issues, questions and queries.
- Detect security incidents, protect against malicious, deceptive, fraudulent, abusive, or illegal activity and provide data in security investigations.
- Support administrative enquiries or disciplinary procedures following a regulated and documented process.
- Where justified, generation of reports for the purpose of monitoring of adherence with EMA's acceptable use of the Agency's Equipment, Software, Networks and Applications including locations from where EMA's systems are accessed.
- Co-operate with law enforcement and legal authorities, if required.

- Comply with any legal obligations or defend any legal claims.

2.1. Personal data concerned

When users authenticate to EMA systems or setup their Multi Factor Authentication methods, Microsoft Entra ID collects, processes, and shares personal data to allow for secure user authentication into EMA services. Such data include the following:

- First name and last name
- E-mail address
- Phone number (if provided)
- IP Address when authenticating to EMA systems
- Profile picture (if provided and applicable).

Furthermore, the following data categories are processed as part of this activity:

- Details of your authentication attempts including general geographic location, public IP address, browser meta-data, and other metadata logged by Microsoft during the authentication process.
- Information about the success or failure of multi-factor authentication attempts including metadata surrounding the device type used in the multi-factor authentication process.
- Usage information surrounding the date, time and duration of applications accessed through Microsoft Azure.
- Technical details of your source internet protocol address, browser type and configuration.

2.2. Legal basis of the processing

As stated by the European Data Protection Supervisor (EDPS)[3], security is an essential enabler for the protection of privacy and data protection. In accordance with Article 33 of Regulation (EU) 2018/1725, EMA as the controller and its processors are required to implement appropriate organisational and technical measures which include secure authentication solutions and identity management to ensure the security of the processing of personal data. The implementation of Microsoft Entra ID is necessary to implement such technical measures.

In accordance with Article 5(1)(a) of Regulation (EU) 2018/1725, the processing of your personal data in the context of the Microsoft Entra ID is necessary for the performance of a "task carried out in the public interest or in the exercise of official authority vested in the Agency". The tasks of the Agency are set out in Regulation (EC) 726/2004 and Directive 2001/83/EC and other applicable Union legislation[4]. Furthermore, the security of processing of personal data is required in accordance with Article 33 of Regulation (EU) 2018/1725 and in compliance with EMA's Security Policy.

In this regard, please note that you have the **right to object** against the processing as explained in Section 5 below.

2.3. Transfers of personal data outside of EU

All customer data, for Core Online Services (Office 365 included), are stored within the EU/EEA at rest.

[3] Information Security | European Data Protection Supervisor
[4] EudraLex - Volume 1 - European Commission

The only instances where access is granted to Microsoft, from outside of the EU/EEA to any personal data are:

- where assistance is required for technical support. Where this is the case, access is only granted to remote screen sharing sessions. No access to personal data is granted to any of Microsoft's sub-processors.
- When an IP Address or phone number is determined to be used in fraudulent activities, they are shared globally to block access from any workloads using them.

In support of its partners and networks and the medicines regulatory processes, EMA does not control or limit the regions from where you may access, or you move your data. Therefore, in case you travel outside the EU/EEA and you use the Agency's services, personal data may be processed outside the EU/EEA to enable your access to the Agency's online services from your location.

All your user data is stored and encrypted in the EU/EEA regardless if you connect from within or outside of EU/EEA. For authentication purposes, to enable global access, servers collect identity and authentication data.

Microsoft has implemented safeguards for transfers of personal data to third countries based on Standard Contractual Clauses embedded in the Online Services Terms.

EMA relies on Article 50(1)(d) of the EUDPR i.e. the occasionally transfer is necessary for important reasons of public interest.

3. How long do we keep your data?

Your account will be disabled after 180 days of inactivity on EMA systems (i.e. if you do not use your account on any of the Agency's systems) or after your contract with the EMA is terminated.

Your data will be deleted after further 180 days from the date your account has been disabled. You will receive a reminder before your data will be deleted. Deleted data are available in a recycle bin for further 30 days, after this period is not possible anymore to recover data.

Your authentication and activity logs are retained for one year (365 days).

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

The data collected will be processed internally by staff within the EMA Service responsible for information security services and by EMA's contractors responsible to provide technical support (via Service Desk) and system maintenance services (see processors in Section 1.2).

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 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.
- **Right not to be subject to automated decision making** – You have the right to not to be subject to a decision based solely on automated processing if such decision has legal effect on you.

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.informationsecurity@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