EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

11 November 2024
EMA/124628/2025

Records of data processing activity for EMA Authentication Services and Microsoft Entra ID (public)

1.	Last update of this record, version number:	09 April 2025, version no 1
2.	Reference number:	AFINS-002
3.	Name and contact details of controller:	European Medicines Agency Internally: Head of Information Security Contact: datacontroller.informationsecurity@ema.europa.eu
4.	Name and contact details of DPO:	dataprotection@ema.europa.eu
5.	Name and contact details of joint controller (where applicable)	Not Applicable
6.	Name and contact details of processor (where applicable)	Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521, Ireland NTT Data Belgique SRL Société rèsponsabilité limitée/Besloten Vennottschap met Beperkte Aansprakelijkheid Rue de Spa 8, 1000 Brussels, Belgium Adinsec BV (Commercial name Grabowsky) Gemeenteplein 13, 1730 Asse, Belgium 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
7.	Purpose of the 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.
8.	Description of categories of persons whose data EMA processes and list of data categories	Any person applying for an EMA account to access EMA systems: EMA staff members, members of EMA Management Board, members of scientific committees and working parties, experts working on behalf of EMA, trainees, interims, seconded national experts, contractors, consultants, members of the public. <u>Data categories processed:</u> • 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). • 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 Azure. • Technical details of your source internet protocol address, browser type and configuration
9.	Time limit for keeping the 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).
10.	Recipients of the data	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.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	All customer data, for Core Online Services (Office 365 included), are stored within the EU/EEA at rest. 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.
12.	General description of security measures, where possible.	The Agency has put appropriate technical and organisational measures (security policies and procedures) in place to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. The Agency takes all necessary measures to ensure the maximum safety and security of personal data held both offline and online, in hardcopy and digital forms. The personal data of users, are normally collected through EMA's Account Management system and propagated to Microsoft Entra ID, which abides by the security provisions established in the Agency's security policies. Access by EMA internal users is protected by modern authentication including multi factor authentication.
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 Here you may find the data protection notice regarding this specific data processing operation as well. https://www.ema.europa.eu/en/documents/other/european-medicines-agencys-privacy-statement-ema-account-management-system_en.pdf