30 October 2023
EMA/188185/2023 Rev.1

European Medicines Agency's Data Protection Notice for the use of Microsoft Applications: OneDrive, Outlook 365, Teams and SharePoint

The European Medicines Agency (hereinafter "EMA" or "Agency") processes the personal data of a natural person in compliance with "Regulation 2018/1725 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" (also referred to as "EUDPR").

This data protection notice explains the most essential details of the processing of personal data by EMA in the context of using the following Microsoft products and related processing activities:

- Outlook 365 (Exchange Online)
- Personal cloud storage – Microsoft OneDrive for Business
- Data storage in SharePoint Online (SPO)
- Microsoft Teams (Teams) and Microsoft Teams Calling Plans which allows Teams to be used to make calls to regular phones via the Public Switched Telephone Network (PSTN)
- The accessibility and functionality of Microsoft products allowing collaboration, communication and work to take place on draft documents between Agency staff and invited external users (e.g., representatives and experts of National Competent Authorities (NCAs) in Member States of the European Economic Area, the European Commission and EMA staff also referred to as the European medicines regulatory network).

This data protection notice only applies to the above-mentioned Microsoft products. Personal data processing related to other uses of Microsoft products at EMA are addressed in separate data protection notices.

Official address Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
Address for visits and deliveries Refer to www.ema.europa.eu/how-to-find-us
Send us a question Go to www.ema.europa.eu/contact **Telephone** +31 (0)88 781 6000 An agency of the European Union

1. Who is responsible for processing your data?

1.1. Who is the data controller?

EMA is ultimately responsible to comply with your data protection rights and freedoms. On behalf of EMA, the Head of 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 engages third parties to process data on behalf of the Agency and, in particular to provide and improve the service, enable use of service features and provide customer support.

The contact details of the data processor are the following:

Microsoft Ireland Operations Limited

One Microsoft Place, South County Business Park,

Leopardstown, Dublin 18 D18 P521, Ireland

Telephone: +353 (1) 706-3117

If you have a privacy concern, complaint, or question for the Microsoft Chief Privacy Officer or the Data Protection Officer, please contact them by using this web form.

2. Purpose of this data processing

The purpose of this data processing activity is to enable the Agency to function effectively and allow the performance of the following tasks:

- Collaboration on working documents
- Providing a storage depository (for professional and private use)
- Enabling electronic communications both internally and externally
- Receiving incoming telephone calls (PSTN) to the Agency and the possibility of the recording of these calls for monitoring and training purposes (via Teams)
- Allowing outgoing telephone calls (PSTN) from the Agency (via Teams)
- Allowing internal telephone calls within the Agency (via Teams)
- Supporting audio and video calls and meetings in Microsoft Teams, and the recording of meetings/calls where this is required (EMA will endeavour to inform attendees if a meeting/call is being recorded. If you do not wish to appear in the recording the data protection notice recommends that you switch off the camera function and mute your microphone)
- The use of integrated Office 365 functionality within these tools.

2.1. Personal data concerned

In this processing operation EMA process data directly collected from you when you access EMA's Microsoft Teams, OneDrive, Outlook 365 and/or SharePoint Online (SPO) services, and when you make or receive a phone call to/from the Agency (which is done under a Microsoft Teams Calling Plan). Personal data (as listed in this section) will be processed both by EMA (as the data controller) and Microsoft and their sub-processors, acting as data processors. Such data may include the following:

- Username, e-mail address, IP address and profile photo of each authorised user (if applicable).
- Any content shared by users, including chat messages (one-to-one as well as group messages) and any other personal information voluntarily posted on the platform.
- Audio and video calls in Microsoft Teams, processed in 'real time' and meeting/call recordings and/or chat transcription files which can be generated by an internal participant (where meetings are recorded, all meeting participants are informed visually when the recording is initiated during the meeting).
- All 'customer data' collected in the OneDrive, Teams, Outlook 365 and SPO platforms. Customer data include all data, including text, sound, video or image files, and software that you provide to Microsoft or that is provided on your behalf through your use of these Microsoft online services. This includes customer content, which is the data you upload for storage or processing and apps that you upload for distribution through a Microsoft enterprise cloud service. For example, customer content includes Teams or SharePoint Online site content, Teams meeting recordings or instant messaging conversations.
- For MS Teams PSTN Telephone calls:
  - The telephone number of the caller
  - The telephone number of the callee
  - Statistical data of the call such as start and end time, and duration
  - Usage reports and logs related to calls, such as PSTN usage reports, PSTN blocked users reports and PSTN minute pools report
  - Call recordings for internal PSTN calls. For more information on this see the separate data protection notice covering this processing: https://www.ema.europa.eu/en/documents/other/european-medicines-agencys-data-protection-notice-recording-telephone-calls-ema-official-telephone_en.pdf

Details on the reporting and the data collected on Teams are available at https://learn.microsoft.com/en-us/microsoftteams/teams-analytics-and-reports/teams-reporting-reference.

Access to EMA's OneDrive, Teams, Outlook 365 and SPO platforms is restricted to users with a valid credentials and access to use these services. These users include EMA staff, EMA contractors, delegates, experts of NCAs, international partners and expert communities.

When access and use EMA's OneDrive, Teams, Outlook 365 and SPO platforms your personal data will be collected and processed. Representatives and experts of the European Medicines Regulatory Network, contractors and other approved users agree to comply with the EMA Teams governance and user guide before using Outlook 365, OneDrive, Teams and SPO for the first time.

2.2. Legal basis of the processing

The use of EMA's OneDrive, Teams, Outlook 365 and SPO platforms, is necessary for the day-to-day functioning and management of the Agency as mandated by EMA's Founding Regulation (EC) No 726/2004 and other Union legislation.

Collaboration and/or communication over EMA's OneDrive, Teams, Outlook 365 and SPO is necessary for the performance of the Agency tasks carried out in the public interest as required by Regulation (EC) No 726/2004, Regulation (EU) 2019/6, Directives 2001/83/EC and 2001/82/EC and other applicable Union legislation. Data processing is based on Article 5(1)(a) of the EUDPR, i.e., the processing is necessary for the performance of EMA's task in the public interest.

2.3. Transfer of personal data outside of EU

The personal data used in OneDrive, SharePoint Online, Teams and Outlook 365, including all customer data is stored within the EU/EEA.

Microsoft may temporally grant access to technical staff and sub-processors located outside EU/EEA where this is necessary to provide their services. Microsoft will only grant access to either pseudonymised personal data or pseudonymised personal identifiers to its sub-processors. Microsoft's sub-processors are required to maintain the confidentiality of data and are contractually obligated to meet strict privacy requirements. These sub-processors are also required to meet the requirements of the EUDPR, including those related to implementing appropriate technical and organisational measures to protect personal data. For the full list of sub-processors, who may have access to data outside of the EU/EEA and their location, please see section 4.

The only instance where access to any personal data is granted to Microsoft itself from outside of the EU/EEA is where assistance is required for technical support. Where this is the case, access is only granted to remote screen sharing sessions which take place with the consent and in the presence of the data subject.

In addition, as with all Microsoft products, Microsoft does not control or limit the regions from which the customer or its end users may access or move customer data. Therefore, where an end user travels outside of the EU/EEA and uses the services, personal data may be processed outside the EU/EEA to enable these users access to the online services from their location.

All user data is stored and encrypted inside EU/EEA regardless of if the users connecting inside or outside of the EU/EEA. For authentication purposes, to enable global access, servers may collect identity and authentication data from outside of the EU/EEA. However, this is true for all the MS 365 environments and includes OneDrive, Teams, Outlook 365, and SharePoint.

Microsoft has implemented measures for data transfers (e.g., Standard Contractual Clauses embedded in the Online Services Terms and additional GDPR-specific clauses in the Online Services Terms).

3. How long do we keep your data?

All personal data relating to your EMA account will remain in the cloud storage until your EMA account has been deactivated, after which they will be deleted from Microsoft's servers after a 30-day retention period. Deactivation occurs for staff and contractors based on the date of their departure from the Agency. For external users deactivation occurs after 6 months of inactivity and after 14 months for experts.

The following specific retention periods apply to personal data included in any of the below data categories:

Platform	Data Type	Retention period
Teams	Site data - All data within a Team site accessible by the members and owners of the Team (e.g., Posts, Files, add-ons).	Retained until deletion of the site. The data can be restored within 30 days of the deletion of the site, after which the data is purged.
Teams	Ad-hoc chats (1 to 1) and meeting chats.	Retained for 6 months. Each user can delete his/her own messages within the chats. Only individual messages in the chats can be deleted by the message author and on a message-by-message basis, not per conversation.
Teams	Files shared on an ad-hoc basis, e.g., in ad-hoc chats and meeting chats.	Retained until deleted by any chat participant. The file will be completely deleted after 30 days after deactivation of the owner's account. **Users are responsible for deleting any files that are no longer required in line with the principle of storage limitation.**
Teams	Files shared within a Teams channel (stored in the underlying SharePoint library).	Retained until 30 days after the site is deleted. Where a document is given the label 'record' a retention period will not be applied. The document owner will be responsible for manually deleting the document when it is no longer required.
Teams	Audio and video calls in Microsoft Teams are processed only in 'real time'.	For call/meeting recordings these are retained by default for 30 days but the owner can amend the expiry date.

Platform	Data Type	Retention period
	Some meetings are recorded and/or transcribed. Teams meeting being recorded and chat transcripts.	There is no maximum retention period applied. **Users are responsible for deleting any files that are no longer required in line with the principle of storage limitation.** The file will be completely deleted 30 days after deactivation of the owners account.
Teams PSTN	Call recording - Telephone calls made to the EMA main switchboard (+31887816000) from an external number.	Retained for 28 calendar days on a rolling basis after which time they are deleted.
SharePoint	Username, e-mail address, IP address and profile photo of each authorised user (if applicable). Any content shared by users and voluntarily posted on the platform. All 'customer data' including text, sound, video or image files, and software that you provide to Microsoft or that's provided on your behalf through your use of Microsoft enterprise online services. This includes customer content, which is the data that you upload for storage or processing.	For SharePoint sites that are deleted, the retention period is 93 days as it goes through a lifecycle of two recycle bins. Where a document is given the label 'record' a retention period will not be applied. The document owner will be responsible for manually deleting the document when it is no longer required. **Users are responsible for deleting any files that are no longer required in line with the principle of storage limitation.** Where files are deleted, data will be retained for 30 days, after this time it will be purged.
Outlook 365	Username, e-mail address, IP address and profile photo of each authorised user (if applicable). Any content shared by users and voluntarily posted on the platform. All customer data.	Retained for 30 days after an account is deleted. **Users are responsible for deleting any files that are no longer required in line with the principle of storage limitation.** Data will be retained for 30 days after files have been deleted, after this time it will be purged.

Platform	Data Type	Retention period
OneDrive	Username, e-mail address, IP address and profile photo of each authorised user (if applicable). Any content shared by users and voluntarily posted on the platform. All customer data.	**Users are responsible for deleting any files that are no longer required in line with the principle of storage limitation.** Data will be retained for 30 days after files have been deleted, after this time it will be purged.

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 Division responsible for Microsoft OneDrive, Teams, Outlook 365 and SharePoint Online and by Microsoft their sub-processors only as is necessary for the purposes of providing the service.

Internal Access:

OneDrive and Outlook 365 are private and accessible only to active EMA staff members and contractors with a valid EMA Account.

Teams and SPO platforms are also private and accessible only to active EMA staff members, contractors and approved representatives and experts of the EU Medicines Regulatory Network and other stakeholders with a valid EMA Account. Only approved, invited participants are allowed to use these platforms, within strict controls.

All users who have shared their files can review, amend or revoke sharing as desired. Owners of the files also have full control to amend these access rights.

All users who have joined a particular Teams site can see activity approved within their permissions, which may include your posts, your replies to comments, your 'likes', etc. Permissions are configured on a site-by-site basis by the Teams site owner and can be set at a team, channel or chat level.

Messages sent to individual users using the chat functionality can be seen only by the recipient and potentially by network administrators (see the following note).

A defined population of approved EMA network administrators from within the Agency's Information Management Division (I-Division) and Information Security Service (DED-INS) can temporarily access all exchanges made within the Teams, Outlook 365, OneDrive and SPO platforms if there is a legitimate reason to do so, e.g., for the purpose of providing technical support and compliance with applicable terms of use and *EMA's code of conduct* (see https://www.ema.europa.eu/en/documents/other/european-medicines-agency-code-conduct_en.pdf) . This includes exchanges in chats that the administrator is not a member of, as well as messages sent using the chat functionality.

In regards to access required to in relation to administrative inquiries and disciplinary proceedings, please refer to the EMA data protection notice covering this processing, (see

https://www.ema.europa.eu/en/documents/other/privacy-statement-processing-personal-data-context-administrative-inquiries-disciplinary-proceedings_en.pdf).

Where EMA receives a request for access to data from a data subject, the EMA data protection officer may access data within the Microsoft applications for the purpose of fulfilling the request.

External Access:

Information collected on OneDrive, Teams, Outlook 365 and SPO may additionally, and only where necessary, be transmitted to the bodies in charge of monitoring or inspection tasks in accordance with European Union legislation.

Microsoft and its following sub-processors may process personal data only as is necessary to provide their services:

- Databricks Inc.*: Who assist with operating and troubleshooting for Azure Databricks (Teams utilises Databricks), located in Canada, France, Germany, Netherlands, United Kingdom and United States.
- Akamai Technologies Inc.*: Who provide Operating Content Delivery Network (CDN) infrastructure to efficiently deliver content, located worldwide.
- Edgecast Networks Inc.*: Who provide Operating Content Delivery Network (CDN) infrastructure to efficiently deliver content, located worldwide.
- Adjust Inc.*: Who provide Data Analytics for analysis of customer feature usage patterns for Outlook 365, located in Germany, Netherlands and United States.
- Scuba Analytics Inc.**: Who provide customer analytics for Teams, SPOL and OneDrive, located in US.
- Microsoft Contract Staff provided by third parties*: Who help operate, deliver, and maintain the Microsoft Online Services, located worldwide (all data resides only on Microsoft systems). [1]

*These sub-processors only have access to pseudonymised personal identifiers.
**These sub-processors only have access to pseudonymised personal data.

For more information on how Microsoft's sub-processors process your personal data please see the below:
https://servicetrust.microsoft.com/DocumentPage/aead9e68-1190-4d90-ad93-36418de5c594

All data is stored in Microsoft data centres based in the EU, Microsoft will only access data where it is necessary to provide their services. For example, where assistance is required for technical support Microsoft may request remote screen sharing access. Remote screen sharing access is only requested for the purpose of helping to resolve technical issues and will always take place with the consent and in the presence of the data subject.

No personal data are transmitted to parties outside the scope mentioned herein, and neither Microsoft nor EMA share personal data with any other third party for any other purpose (e.g., direct marketing).

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.

[1] Sub-processor list corrected as of 7th February 2023

- **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 withdraw consent –** You have the right to withdraw your consent to the processing of your personal data. However, this will not affect the lawfulness of any processing carried out before consent is withdrawn.

  Please note that if you withdraw your consent, the Agency may not be able to provide certain services to you. EMA will advise you if this is the case at the time you withdraw your consent.
- **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 to portability** - Where the processing is carried out based on your consent and in automated means you have the right to receive your personal data (which was provided to the EMA directly by you) in a machine-readable format. You may also ask the EMA to directly transfer such data to another controller.
- **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. Please note that there are limitations and exceptions to these rights, more information on this can be found here. For anything that is not specifically provided for in this Data Protection Notice, please refer to the contents of the general EMA General 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 General Privacy Statement, please contact the **Internal Data 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