20 March 2023
EMA/124004/2023

European Medicines Agency's Data Protection Notice

For the use of the MS Intune for personal and corporate-owned devices

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 the European Medicines Agency (hereinafter "EMA" or "Agency") in the context of accessing data held by the EMA via both personal and corporate-owned devices (i.e., smartphones, laptops, tablets and other mobile devices) and the use of Microsoft (MS) Intune with the objective to protect EMA corporate data. Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM).

1. Who is responsible for processing your data?

1.1. Who is the data controller?

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

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

1.2. Who is the data processor?

EMA engages a third party to process data on behalf of the Agency and, in particular, to provide the software tools enabling EMA to control access to its data when personal and corporate-owned devices are used by EMA staff.

The contact details of the data processor(s) 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

2. Purpose of this data processing

The purpose of this processing activity is to allow staff owned devices and the Agency's corporate devices to be configured to use M365 applications and corporate communication and collaboration such as telephone and conference calls. Personal devices owned by EMA staff may also be configured accordingly in line with EMA's Bring-Your-Own-Device (BYOD) policy.

MS Intune is a cloud-based service supporting mobile device management (MDM) and mobile application management (MAM). In EMA providing secure access to corporate data through MS Intune EMA staff can work on devices and applications to perform corporate tasks while data and resources are protected. MS Intune can be used on personal and corporate-owned devices in line with EMA's Bring-Your-Own-Device (BYOD) policy, which can be found here.

EMA applies MS Intune for the purpose of enabling the secure isolation of corporate data and to separate private (non-corporate) data and applications on the devices.

2.1. Personal data concerned – Processed by Microsoft Intune

When users enrol their personal and corporate-owned devices with Intune, Intune collects, processes, and shares some personal data to support business operations, conduct business with the customer and to support the service. Intune collects personal data from the following sources:

- EMA administrators' use of Intune in the Microsoft Endpoint Manager admin centre
- End-user devices (when devices are enrolled for Intune management and during usage)
- Customer accounts at third party services (per admin's instructions)

The following data categories are processed as part of this activity:

- Access control information (such as static authenticators e.g., customer's password)
- Admin and account information (such as admin username)
- User Information (such as phone number)
- Support information (such as contact details)
- Device Data (such as Intune account ID)
- Audit Log data (data about activities)
- Diagnostic, performance, and usage information

Intune collects information that falls into the following two categories: Required data and Optional data. For the specific required and optional data that is collected, see here for required data and optional data.

Users who enrolled to mobile Intune can find out more at:

Privacy and personal data in MS Intune

2.2. Personal data concerned – Processed by EMA

When you enrol a personal device, you give EMA permission to view certain pieces of information on your device, such as device model and serial number. This information is used by EMA to protect its corporate data on the device.

Corporate-owned devices are automatically enrolled with MS Intune.

EMA cannot view your personal, non-corporate information when you enrol with MS Intune using your personal device. The corporate platform keeps private and corporate data/folders separate.

Authorised EMA IT staff has access to the following data:	
Owner	The EMA MS Intune Administrator can see the ownership type for each individual device on the Intune Portal Device Details area.
App Inventory	For the use of Mobile Threat Defence, EMA will be able to view details about the apps that are on your iOS device. Find out more about Mobile Threat Defence. For corporate-owned devices, EMA can see all your app inventory. For personal-owned devices, EMA can only see your corporate managed app inventory. e.g., Outlook, Company Portal, Teams.
Location	For corporate-owned devices, EMA can see the location of a lost device. Further information can be obtained from the Apple iOS documentation to learn more about supervised devices. For personal devices, EMA cannot view the device location.
Phone number	For corporate owned devices your full phone number is visible. For personal devices only the last four digits of your phone number are visible.
Device storage space	If you can't install a required app, EMA may look at your device's storage space to determine if the space is too low.
Network Information	For corporate-owned devices, the location of corporate devices is tracked all the time. For personal-owned devices, some information about network connections may be obtained. This is in cases, where the Agency requires devices to access EMA network information for automatic log in to the

	EMA LAN and your device would identify the network where it is connected, so your device location.
Device Name	
Serial Number	
Manufacturer	
Model	
Operating System	
The authorised EMA IT staff do not have access to:	
Call history	
Text messages	
Personal email, contacts, calendar	
Web history	
Camera roll	
Private used data	
Passwords	
Personal Apps	

Further information can be obtained as follows: https://docs.microsoft.com/en-gb/mem/intune/user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune

2.3. Legal basis of the processing

As stated in the EDPS guidelines[1], security is one of the main enablers of data protection. To guarantee an adequate level of protection, EMA must implement both organisational and technical measures, such as Mobile Device Management solutions. The implementation of MS Intune is necessary to implement such technical measures.

The enrolment to MS Intune on EMA laptops is provided by default. Corporate laptops are issued to each staff for the purpose of corporate business use only, the use of MS Intune is not optional.

The use of a corporate mobile phone which includes M365 corporate applications, is voluntary for EMA staff. However, if the staff member decides to use a corporate mobile phone, then enrolment to MS Intune is required to ensure the secure use of the Agency's data on the mobile device.

The collection and processing of personal data stated above are necessary for the performance of the Agency tasks carried out in accordance with Article 5(1)(a) of Regulation (EU) 2018/1725 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 the Agency.

[1] Guidelines on the protection of personal data in mobile devices used by European institutions (2015)

2.4 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.

The only instance where access is granted to Microsoft, from outside of the EU/EEA to any personal data is in instances 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. No access to personal data is granted to any of Microsoft's sub-processors.

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, in case an end user travels outside the EU/EEA and uses the services, personal data may be processed outside the EU/EEA to enable the user access to the online services from their location.

All user personal data is stored and encrypted inside EU/EEA regardless of if the users connect inside or outside of EU/EEA. For authentication purposes, to enable global access, servers collect identity and authentication data, this is true for all the MS 365 environment, such as Teams and SharePoint.

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

3. How long do we keep your data?

Data is not stored in MS Intune; the software enables the access to corporate application and storage folders.

For personal and corporate-owned devices:

- When you leave EMA or you no longer need access to EMA corporate data via a device, you can retire the device in your MS Intune account.
- This data is wiped by authorised IT staff on the first day after a staff member's contract termination/expiry or when the corporate-owned mobile device has been returned by the EMA staff member.
- A device is also automatically retired, if a mobile device has not checked in with MS Intune for more than 63 days. The data listed in section 2.2 is then also wiped.

For EMA corporate-owned devices, the data from lost devices are wiped centrally by EMA using the applicable MS Intune functionality.

The reason the retention period for this data is 63 days is to ensure data is wiped where devices are inactive whilst ensuring data is not lost in instances where a device is offline for a longer period of time due to staff absence.

Users can choose to remove their personal-owned device from Company Portal following this article: Remove your device from the Company Portal | Microsoft Learn

For personal-owned devices, the data from lost devices are removed from Intune after 63 days.

What does it mean that the device is retired?

This means that you no longer have access to corporate data using your personal device. To regain access, you need to follow the MS Intune enrolment process again.

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

The data collected through MS Intune will be processed internally by staff within the EMA Information Management (IT) Division responsible for securing corporate data on mobile devices. Please see section 2.2. for all personal data that these internal staff may have access to.

Authorised IT staff can take the following actions, after you have enrolled your mobile device, to make sure the Agency's corporate information is secure:

- Reset your corporate mobile phone to factory settings if it is lost or stolen
- Remove Agency-related files and apps (without removing your personal files or apps)
- Require you to use a password or PIN
- Make your mobile phone compatible with the Agency's security standards

When users enrol their devices with Intune, Microsoft Intune collects, processes, and shares some personal data to support business operations, conduct business with the customer and to support the service.

Microsoft do not share any personal data with vendors or agents working on their behalf for the purposes described in this statement. Data may be disclosed as part of a corporate transaction such as a merger or sale of assets. Personal data may be shared among Microsoft-controlled affiliates and subsidiaries where this is necessary for the services Microsoft provide.

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.

5. Your data protection rights

As data subject (i.e., the individual whose personal data is processed), you have the following 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 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 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 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. 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 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 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