EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

20 March 2023
EMA/124005/2023

Records of data processing activity for the use of Microsoft Intune

1.	Last update of this record, version number:	20 March 2023, version 1
2.	Reference number:	EMA/124005/2023
3.	Name and contact details of controller:	European Medicines Agency Internally: Head of Information Management Division Contact: Datacontroller.infomanagement@ema.europa.eu
4.	Name and contact details of DPO:	dataprotection@ema.europa.eu
5.	Name and contact details of joint controller (where applicable)	N/A
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 Telephone: +353 (1) 706-3117
7.	Purpose of the 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.
8.	Description of categories of persons whose data EMA processes and list of data categories	As part of this processing activity the following data categories may be processed: • 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 and device storage data) • Audit Log data (data about activities) • Diagnostic, performance, and usage information • Location Data • Network Information • Application Inventory (for corporate devices or corporate managed apps) 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.
9.	Time limit for keeping the data	Data is not stored in MS Intune; the software enables the access to corporate application and storage folders. When a staff member leaves EMA or no longer needs access to EMA corporate data via a device, the staff member 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 then the data is also wiped.
10.	Recipients of the data	EMA IT Administrators and Microsoft support
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	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. Microsoft has implemented measures for data transfers (e.g., Standard Contractual Clauses embedded in the Online Services Terms and additional GDPR/EUDPR-specific clauses in the Online Services Terms).
12.	General description of security measures, where possible.	EMA IT network is protected by multi-factor authentication (MFA). Data is encrypted at rest and in transit. To protect personal data of data subjects, EMA has put in place several contractual safeguards complemented by technical and organisational measures. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.
13.	For more information, including how to exercise your rights to access, rectification, erasure, restriction object and data portability (where applicable), see the privacy statement:	Details concerning the processing of your personal data and your data subject rights 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 EMA General Privacy Statement as well as the privacy statements on specific data processing operations. DPN- Intune EMA/124004/2023 https://docs.eudra.org/webtop/drl/objectId/090142b2856346c3