March 31st 2026
EMA/77651/2026

Records of data processing activity for the Critical Medicines Vulnerability Assessment (public)

1.	Last update of this record, version number:	1.0
2.	Reference number:	TRS-12
3.	Name and contact details of controller:	European Medicines Agency Internally: Head of Regulatory Science and Innovation Task Force (TRS) Contact: Datacontroller.Horizonscanning@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, South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland
7.	Purpose of the processing	The purpose of this data processing activity is the exchange of information needed to conduct the Critical Medicines Vulnerability Assessment Exercise. This information relates to structural and conditional supply chain vulnerabilities for medicinal products containing International Non-proprietary Names (INNs), which have been selected for the exercise.

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

8.	Description of categories of persons whose data EMA processes and list of data categories	The categories of data subjects whose personal data will be processed are: • An individual acting as a contact person for MAHs or acting on behalf of MAHs, which hold a marketing authorisation for one or more of the products selected for the Supply Chain Vulnerability Assessment Exercise. The personal data of the individuals listed above may include the following: • Name and last name • Job position and organisation • Professional email address • Any other personal data (e.g., professional phone number) that may be processed when you submit the Vulnerability Assessment Template, and/or if you send further communications to EMA's Vulnerability Assessment mailbox.
9.	Time limit for keeping the data	This vulnerability assessment exercise is expected to be finalised by the end of 2026. For those registered as an i-SPOC contact point, their contact details will be kept in line with the i-SPOC system retention period, i.e., as long as the individual is the i-SPOC for the MAH, and until a replacement has been named. This is necessary to ensure an agile action by the EU Regulatory Network in the context of a major event or a public health emergency. For those that are not registered as such, EMA will retain their contact details until they have registered as an i-SPOC for the MAH in IRIS. Registration of an i-SPOC is a two-step process which might take up to 5-10 working days. Once complete, their data will be kept in line with the i-SPOC retention period as explained above.
10.	Recipients of the data	The personal data will be processed by the data processors listed in Section 1.2 and internally by the relevant staff at the Agency within the EMA Task Force responsible for the specific procedure. The personal email addresses may be shared with the national competent authorities of EU member states, as well as the European Commission on a need-to-know basis for the purpose of the exercise.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to	The personal data processed in Microsoft is stored within the EU/EEA. From time to time, Microsoft, acting as a processor of the Agency and together with its subcontractors, may need to transfer personal data to countries outside the EU. This can happen, for example, when they need to prevent or solve security issues. Any such transfers are only

	which ones and with which safeguards?	made with proper safeguards in place, as required by EU data protection law. This means that Microsoft will only transfer your personal data if the Agency instructs them to do so, or if they must comply with a specific legal obligation, and always in line with the rules set out in Regulation (EU) 2016/679 and the EUDPR. Microsoft Corporation is certified under the EU-U.S. Data Privacy Framework, so any transfers of your personal data to the U.S. follow the requirements of this framework. If, for any reason, it is not possible to use the Data Privacy Framework, these transfers will then be governed by the 2021 Standard Contractual Clauses agreed between Microsoft Ireland Operations Limited and Microsoft Corporation. Even when relying on these Clauses, Microsoft limits the number of transfers to countries that have not received an adequacy decision from the European Commission. These limited transfers are made based on Article 50(1)(d) of Regulation 2018/1725 i.e. the transfer is necessary for reasons of public interest.
12.	General description of security measures, where possible.	The Agency has appropriate technical and organisational measures in place, including organisational policies, to safeguard the security of personal data and ensure the confidentiality, integrity and availability of the relevant systems, services and the personal data processed within them.
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/data-protection-privacy-ema Here you may find the data protection notice regarding this specific data processing operation as well.