24 November 2022
EMA/905306/2022

Record of data processing activity for reporting fraud and irregularities (public)

1.	Last update of this record, version number:	24 November 2022, version 3
2.	Reference number:	GAF1
3.	Name and contact details of controller:	European Medicines Agency Internal contact: General Affairs and Anti-Fraud Office Contact: afo@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)	Not applicable
7.	Purpose of the processing	The purpose of the processing of the personal data by the EMA's General Affairs and Anti-Fraud Office of reported information regarding irregularities and potential fraud cases that are brought to its attention by way of reported information (internally by the EMA staff or externally from external whistleblowing) or that have reached the Agency by other means. This process will allow gathering information on the reported conduct in order to assess and identify which cases require to be transmitted to the European Anti-Fraud Office according to Article 8 of Regulation (EU, Euratom) No. 883/2013.
8.	Description of categories of persons whose data EMA processes and list of data categories	EMA's staff members, members of EMA's Management Board, members of scientific committees and working parties, experts working on behalf of EMA, trainees, interims, seconded national experts, contractors, consultants, persons referred to in the fraud reporting process.

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

		The data categories to be processed vary depending on the nature of the suspected fraud or irregularity reported, however, not exhausting examples of these data categories are the following: data concerning suspected offences, offences, criminal offences or security measures (e.g. police certificates); data concerning leave and absences; data concerning the data subject's family; data concerning the data subject's private sphere; data concerning pay, allowances and bank accounts; data concerning recruitment and contracts; data concerning missions and journeys; data concerning social security and pensions; data concerning medical benefits and expenses; data concerning telephone numbers and communications. Other types of personal data may be processed if included amongst the data on the nature of the facts potentially constituting fraud or otherwise in the data reported by the reporting person.
9.	Time limit for keeping the data	For cases that are not notified to the European Anti-Fraud Office (OLAF) and for which no further action is needed, the retention period of the data is 12 months from the closing of the assessment leading to the decision not to notify OLAF. Retention periods for cases that are notified to the European Anti-Fraud Office are aligned with those of OLAF, as follows: 15 years: data on a case with follow up 8 years: data in a case without follow up 5 years data: data in a case that has been dismissed All retention periods commence after the case has been closed. Improper and pointless messages will be deleted immediately.
10.	Recipients of the data	The recipients of the data will be identified on a need-to-know basis, but can include the Executive Director, the EMA's General Affairs and Anti-Fraud Office, Head of the Legal Department, Head of Audit, HR officers, EMA management involved in the specific case or EMA HR management, investigators appointed to undertake administrative inquiries, European Anti-Fraud Office, Disciplinary Board members.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No
12.	General description of security measures, where possible.	All areas of the EMA's building have electronic card access control in line with EMA's security procedures. All computer equipment is password controlled. Network firewalls protect the logic perimeter of the EMA's IT infrastructure. EMA's main security systems are security hardened. The EMA's documents and access thereto is subject the EMA's Document Classification Policy (Policy/0081). Documents pertaining to potential frauds are stored in secure locations and accessible only by the Head of the General Affairs and Anti-Fraud Office and staff members specifically delegated by him/her. The functional mailbox of the Anti-Fraud Office afo@ema.europa.eu, where the potential cases of fraud may be reported, is accessible only by the Head of the General

		Affairs and Anti-Fraud Office and by staff members specifically delegated by him/her. This mailbox has restrictions for the deletion of data or communication of such data. A specific fraud register/database is password protected and is accessible only by the Head of the General Affairs and Anti-Fraud Office and by staff members specifically delegated by him/her.
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the privacy statement:	In certain circumstances the Decision of the Management Board of the European Medicines Agency of 12 June 2019 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the Agency may be applicable to the handling of reports regarding irregularities and potential fraud cases. 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, where you may find the EMA's General Privacy Statement as well as the privacy statements on specific data processing operations.