29 November 2023
EMA/525038/2023

Records of data processing activity relating to pre-employment medical examination

1.	Last update of this record, version number:	29 November 2023, version 1
2.	Reference number:	A64
3.	Name and contact details of controller:	European Medicines Agency Internally: Head of Administration and Corporate Management Division datacontroller.administration@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)	KLM Health Service B.V. Stationsplein NO 236 111 CJ Schiphol ema.health@klm.com
7.	Purpose of the processing	The purpose of this data processing activity is to enable candidates to undergo a medical examination in accordance with Articles 28(e) and 33 of the Staff Regulations of Officials of the European Union (SR) [1], as well as Articles 12(d) and 82(3.d) of the Conditions of Employment of Other Servants of the European Union (CEOS).

[1] Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community. Available here: https://eur-lex.europa.eu/eli/reg/1962/31(1)/oj/eng

		In addition, to carry out the pre-employment medical examination, the medical service provider will process your data for the following purposes: • Creating your account to register with the medical service provider; • Allocating login details to your account; • Updating your medical record; • Scheduling an appointment; • Updating your preferences; • Processing payments (invoicing); • Preparing periodic management reports (only anonymised aggregated data); • Issuing a fit-for-employment certificate for EMA; • Organising the translation of medical findings from a treating doctor, if applicable; • Updating results from previous examinations and treatments, if applicable.
8.	Description of categories of persons whose data EMA processes and list of data categories	In this processing operation the medical service provider processes data directly collected from you. Such data may include the following: • Name and address details; • Personnel number (if applicable); • Date of birth; • Gender; • E-mail address; • Telephone number; • Job title (e.g. Assistant, Administrator, Head of ...) • Job role and description. • Information regarding your health; • Partner and family status; • Information about your appointment; • IP address; • Practitioners (for example, general practitioner, specialist and their telephone number); • Results of your diagnostic examination and laboratory results; • Medical reports and advice from doctors who treated you, including any translations, if applicable, to determine, for example, reasonable workplace adjustments due to illness; • Medical recommendations to carry out a consultation with the Agency's occupational health physician, if applicable. In the context of this processing operation, the Agency processes only the fit-for-employment certificate, the examination date and the invoice.

		In addition, the Agency may process the medical recommendations to carry out a consultation with the Agency's occupational health physician and reasonable workplace adjustments, if applicable.
9.	Time limit for keeping the data	The appointed medical service provider does not store data for longer than necessary to comply with legal requirements (such as the period set by the Dutch authorities for the administration of medical data in the Netherlands). In accordance with its legal obligations, EMA shall keep the financial documentation for 5 years from the date of budget discharge (which is the date of the European Parliament's final approval of the budget implementation for the concerned year). Accordingly, EMA will delete your personal details no later than within 8 years following your examination
10.	Recipients of the data	The data provided to or collected by the medical service provider (as explained in Section 2.1 above) will be processed only by the service provider and their authorised subcontractors (i.e. provider responsible for software used for the purpose of booking appointments and completing a medical questionnaire and the laboratory for processing samples). The medical service provider has a valid information security certification and has appropriate measures to protect your data. The medical service provider will only share with EMA: • Fit-for-employment certificate and examination date, proposed workplace adjustment or recommendation for an appointment with the occupational health physician (if required). No medical data will be included in the certificate. • Personal data related to processing payments (name, surname, date of birth and date of examination). The data related to workplace adjustments will be processed in accordance with the Data Protection Notice on reasonable accommodation. The data related to payments will be processed internally by EMA-nominated and restricted staff members within the Administration and Corporate Management Division responsible for the Medical Service in the Staff Matters Service.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	Not applicable

12.	General description of security measures, where possible.	The service provider will process data and apply restrictions and safeguards that fully consider the nature of the data and the risks involved. The service provider complies with laws and regulations including the General Data Protection Regulation, the Medical Treatment Agreement Act, the Utilisation of Citizen Service Numbers in Healthcare Act, The Healthcare Insurance Act, the Absenteeism Reduction Act, the Working Conditions Decree, the General Tax Act and the Guidelines of the Royal Dutch Medical Association. The personal and medical data is only accessible to authorised staff providing treatment or support. The staff signs confidentiality agreements. The management system of the provider confirms with the Information Security Management System standard ISO 27001:2013 and NEN 750-1:2017 + A1:2020. Furthermore: 1. The service provider has assigned and specified responsibilities for information security within the organisation and appointed a Data Protection Officer. 2. Whenever the service provider engages in cooperative agreements with external parties, explicit attention is paid to information security. Processing agreements are laid down with suppliers whenever personal data is processed. 3. Company processes, information systems and data gathering are all classified in terms of availability, integrity and confidentiality. 4. At recruitment, during the term of employment and if an employee is discharged, explicit efforts are made to ensure the trustworthiness of employees and confidentiality of information. 5. The service provider pursues an active policy in encouraging security awareness and has a code of conduct governing the use of information facilities. 6. The service provider has taken measures to ensure the physical security of people and resources. 7. The service provider has taken measures to ensure the security and control of operational information and communication facilities. 8. The service provider has taken measures to ensure that only authorised employees make use of information and communication facilities. 9. During the development and procurement of information systems, attention is explicitly paid to information security during all phases of development and procurement. 10. Within the policy process for information security, it is stipulated that internal and external parties are required to monitor compliance with information security policy. 11. The service provider has the means to report and deal with security incidents and data leaks. The handling of security incidents and data leaks is evaluated to improve the information security and better protect personal details.

		12. The organisation maintains a processing register of all personal data gathered by the organisation.
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 processing your personal data are available on the Agency's external website among the Data Protection Notices, where you may find the specific data protection notice.