EMA/36991/2021 ver 7

Record of data processing activity relating to the Security Access Control System (public)

1.	Last update of this record, version number:	23 April 2024, version 7
2.	Reference number:	A35
3.	Name and contact details of controller:	European Medicines Agency Internally: Head of Administration and Corporate Management Division of EMA, dataprotection.administration@ema.europa.e
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)	Contracted security company: **SECURITAS BEVEILIGING B.V.** De Corridor 3ª, 3621 ZA Breukelen Email: dataprotectionofficer@securitas.nl Reception and hosting service company: **SPIRIT HOSTESS SERVICES PROMO ADVIEZEN B.V**. General Aviation Terminal, Thermiekstraat 30, 1117 BC Schiphol-Oost Email: info@spirithospitality.nl
7.	Purpose of the processing	The purpose of this data processing activity is to operate the Agency's Security Access Control System (AACC) to protect EMA's premises against unauthorised access and theft, as well as against both external and internal threats. The AACC system consists of a central server, door controllers, a software application and card readers installed at the entrances of the building, to the entrances on each floor and to the entrances to different rooms. These entrances open only if an access card which has authorisation to access the premises is swiped at the card reader.

		The data held in the Security Access Control System (AACC) is required to control the access to different areas within EMA premises and to ensure the security of its personnel, delegates, contractors, visitors, operations and assets. The system is also used • for the investigation of security-related incidents, • to generate a list of persons, present in the building in the event of a building evacuation, • to generate a report of EMA staff attendance in the building for the purpose of monitoring the effective implementation and compliance with EMA's decision on working time and hybrid working, • to generate a report of EMA staff attendance in the building for the payment of a contribution to staff commuting costs, • to generate a report of contractors' attendance in the building to verify the physical presence in the building of contractors where the applicable contract specifies that *intra-muros ('on-site')* rates apply and, therefore, said verification is necessary to process the payment of services to the contractor, • to verify the physical presence of Emergency Response Team (ERT) members and First Aiders to assess and coordinate ERT and first aid response in the EMA building, and • in case of need, the system data might also be used in an administrative enquiry or disciplinary procedure following a regulated and documented process.
8.	Description of categories of persons whose data EMA processes and list of data categories	The following categories of data subject are subject to this processing operation: • EMA staff members (including national experts, interim and trainee staff), as well as contractors, delegates & visitors entering the EMA premises. The following categories of personal data are collected for this processing operation: • For permanent badge holders, contractors, and delegates, the collected personal data include: Permanent badge holder's name, staff identification number (EMA staff only), photo, badge number/ID, badge type, entry/expiry date and access level • For temporary badge holders the same data as above is collected, excluding the photo and the staff identification number. • Movement data regarding all badges: date, time, and location where card is swiped.
9.	Time limit for keeping the data	Duration of contract/nomination for permanent badge holders, such as EMA staff members (including interim and trainee staff), contractors or delegates. 6 months for movement data referred to permanent and temporary badge holders including period after

		termination of employment/nomination or visit, for investigative purposes. 5 years following discharge of the relevant budget year, for the report from the system for the purposes of: i) calculation of payment for "intra-muros" rates for contractors; ii) calculation of a payment to individual EMA staff commuting costs.
10.	Recipients of the data	EMA staff within Security Service responsible for enrolling and processing staff, delegates, contractors, and visitor access cards in the security access control system. EMA security and reception contractors for processing visitors, contractors, delegates and provide temporary cards to staff in case of forgotten permanent badges or answer other queries. Staff Matters Service receives a quarterly report from the system about EMA staff presence in the building for the purpose of the payment of a contribution to staff commuting costs. The Head of A-ST Department, upon request from the Head of A-Division, receives reports from the system about EMA staff presence in the building in the context of carrying out ex-post controls to monitor compliance with weekly presence in the office. The access may also be granted to line managers on a need-to-know basis. Office of the Central Information Technology Office receives the report receives the report for the purpose of verifying the physical presence in the building of contractors where the applicable contract specifies that intra-muros ('on-site') rates apply. Managers and investigators when requested in the framework of administrative enquiries or disciplinary procedures. All personnel with access rights to the AACC system receive data protection training.
11.	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	N/A
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. In particular, • The servers storing the access control data are located within secure premises on a secure network and protected by additional physical security measures. • Access rights to AACC system users are granted only to the system modules which are strictly necessary to carry out their roles. The access to those modules is protected with personal password. • Very limited access to the Security Office and other security areas where access to Access Control software is possible. • No longer usable media are safely disposed in such a way that remaining data on them are permanently and irreversibly deleted. This is done in accordance with ICT policies.

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/legal/general-privacy-statement, where you may find the EMA General Privacy Statement as well as the privacy statements on specific data processing operations. Training is provided for new members of EMA staff and contractors explaining AACC data transfer process and data protection regulations.