



EMA/225533/2023 version 9

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

1.	Last update of this record, version number:	17 February 2026, version 9		
2.	Reference number:	A35		
3.	Name and contact details of controller:	European Medicines Agency Internally: Head of Administration and Corporate Management Division of EMA 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)	N/A		
6.	Name and contact details of processor (where applicable)	Processor	Activity	Contact Details
		SECURITAS BEVEILIGING B.V.	Processing of staff, visitors', contractors', delegates' data to issue either permanent or temporary badges for entrance and movement in the building	De Corridor 3 ^a , 3621 ZA Breukelen-The Netherlands Dataprotectionofficer@securitas.nl
		SPIRIT HOSTESS SERVICES PROMO ADVIEZEN B.V.		General Aviation Terminal, Thermiekstraat 30, 1117 BC Schiphol-Oost-The Netherlands Info@spirithospitality.nl
		Microsoft Ireland Operations Limited	MS 365 services and applications to support EMA's administrative tasks and	One Microsoft Place, South County Business Park, Carmanhall and Leopardstown, D18 P521, Dublin-Ireland

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



			reporting processes	https://www.microsoft.com/en-us/concern/privacyrequest-msa
		DOMENICO SCARLATTI V.O.F.	Building Access Control System maintenance services	Graafsebaan 65, 5248JT Rosmalen-The Netherlands EMA-maintain@heijmans.nl
7.	Purpose of the processing	<p>The purpose of this data processing activity is to operate the Agency's Security Access Control System ('AACC') in order 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, doors' 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 after an access card which has authorisation to access the premises is swiped at the card reader.</p> <p>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, but also operations and assets. The system is also used:</p> <ul style="list-style-type: none"> • to investigate 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 decision on working time and hybrid working; • to generate a report of EMA staff attendance in the building for the purpose of the payment of a contribution to staff commuting costs; • to generate a report of contractors' attendance in the building for the purpose of verifying the physical presence in the building of contractors where the applicable contract implies physical presence in the building or it 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 physical presence of Emergency Response Team ('ERT') members and First Aiders for the purpose of assessing and coordinating ERT and first aid response in the 		

		<p>EMA building; and</p> <ul style="list-style-type: none"> in case of need, the system data might also be used in the framework of 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	<p>The following categories of data subject are subject to this processing operation:</p> <ul style="list-style-type: none"> people working at the Agency (Contract and Temporary Agents, Trainees, Interims, Seconded National Experts, and other types of contractors), delegates and visitors who enter the EMA premises. <p>The following categories of personal data are collected for this processing operation:</p> <p>For EMA staff, contractors and visitors: the permanent or temporary badge holder's name, surname, staff identification number (personnel number), photo, badge number/ID, badge type, entry/expiry date and access level. The latter two are linked to different access level depending on status as staff member or other type of contractor. Visitors do not receive staff identification number and do not have a picture obligation.</p> <p>The AACC system also processes movement data of permanent and temporary badges including date, time, and location where a card is swiped. The system also records anomalies in badge, for example use of an expired card, or failure of a card to function or access denied due to lack of privileges to enter a specific area.</p>	
9.	Time limit for keeping the data	Type of data	Retention Period
		Personal data (name, surname, personnel number, photo) recorded in the AACC referring to EMA staff, other type of contractors and delegates	For the duration of their contract (staff) or the professional engagement with the Agency
		Personal data (name, surname, personnel number) extracted from the AACC referring to Emergency Response Team members (ERT) and First Aiders	Report is automatically overwritten in the system every calendar week; For the transfer of the report, we refer to EMA's Data protection notice on Microsoft Applications
		Names and movements of persons present in the building	6 months from last day in the building
		Report (name, surname, personnel number) extracted from the AACC on the verified presence of staff and other contractors in the building for	EMA's Microsoft Applications retention policy applies

		calculation and payment of commuting costs	
10.	Recipients of the data	<p>AACC data is accessed and processed on a need-to-know basis by:</p> <ul style="list-style-type: none"> dedicated EMA staff members from the facilities support services, as well as contractors within the security and reception services responsible for enrolling and processing staff, delegates, contractors, and issuing visitor access cards; dedicated 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; dedicated members of the Staff Matters service. The report from the AACC system is received on a quarterly basis to calculate the contribution towards staff commuting costs; the EMA Health & Security Officer and First Aid coordinator. The report of the AACC system they receive contains personal data referring only to Emergency Response Team members (ERT) and First Aiders and it is used for operational and statistical purposes of this team; the Head of the A-Division. The report from the AACC system is necessary for evaluating the physical presence in the Agency building in the context of carrying out ex-post controls to monitor compliance with weekly presence and for general statistical purposes in accordance with EMA working time and hybrid working rules; the Head of Staff Relations and Support department may also grant access to line managers of the data subjects in the lists, for the correct implementation of trust-based management in cases of differentiated determination of working hours of their staff; the Head of Service or Office of the officially appointed contract managers (of the processors) or to the Central Information Office of the I-Division, for the purpose of verifying the physical presence in the building of contractors where the applicable contract requires physical presence in the building or if the contract specifies that <i>intra-muros</i> ('on-site') rates apply and verification is necessary to process the payment of services to the contractor; other EMA managers may also be given access to the access control data when requested in the framework of 	

		<p>administrative enquiries or disciplinary procedures following a formally established process where the data subject must be informed;</p> <ul style="list-style-type: none"> • the Executive Director and Assistants to Executive Director, the Deputy Executive Director, the Internal Audit Service, the Legal Department, the Data Protection Officer (DPO); • national law enforcement authorities or DG Security of the European Commission upon written request and duly authorized by the data controller in case of crime prevention or investigations regarding threats to EMA security. <p>The contractors responsible for the technical maintenance of the access control system have access to all the system components, including data, exclusively for maintenance purpose.</p> <p>Additionally, when hardware must be replaced due to end of lifespan or fault, these contractors need to copy data to the new piece of hardware installed in the system. This process is always overseen by EMA security staff, it is done in the EMA building, using EMA approved hardware and it is not possible to access the data remotely as neither the old nor the new hardware are connected to the internet and/or cloud in any form.</p> <p>Requests for access to documents under the provisions of Regulation 1049/2001 are handled under EMA's relevant Privacy Statement concerning requests for information or access to documents.</p> <p>Furthermore, we may share your personal data with the following external institutions, on a need-to-know-basis or when the Agency is required to do so by law, including for monitoring, auditing or inspection purposes in accordance with European Union law:</p> <ul style="list-style-type: none"> • the European Ombudsman; • the Court of Justice of the EU; • the European Court of Auditors; • the European Anti-Fraud Office (OLAF); • the European Public Prosecutor's Office (EPPO); and • the European Data Protection Supervisor.
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.	<p>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,</p> <ul style="list-style-type: none"> • 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. • The technical maintenance contractors responsible for technical maintenance of the access control system have access to all the system components, including data, exclusively for maintenance purposes. They don't process any data per se, but they do incidentally have access to data. Additionally, when hardware must be replaced, due to end of lifespan or fault, they need to copy data to the new piece of hardware installed in the system. This process is always overseen by EMA security staff, it is done in the EMA building, using EMA approved hardware, and it is not possible to access the data remotely as neither the old nor the new hardware are connected to the internet and/or cloud in any form. • Training is provided for new members of EMA staff and contractors explaining AACC data transfer process and data protection regulations.
13.	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable), see the relevant Data Protection Notice:	<p>Details concerning the processing of your personal data are available on the Agency's website at: Data protection and privacy at EMA European Medicines Agency (EMA) and in the specific Data Protection Notice for the operation of the Security Access Control System: EMA-A-035-DPN-Access Control System-Public</p>