



Record of processing activity

Physical Access Control System

Record of EBA activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 (EUDPR)

Nr	Item	Description
Part 1 - Article 31 Record (publicly available)		
1	Last update of this record	21/08/2023
2	Reference number	EBA/DPR/2023/4
3	Name and contact details of controller	Controller: European Banking Authority, Tour Europlaza, 20 avenue André Prothin, CS 30154, 92927 Paris La Défense CEDEX, France Contact: EBA-OfficeManagement@eba.europa.eu
4	Name and contact details of DPO	dpo@eba.europa.eu or you can send a letter to the postal address of the EBA (above address) marked for the attention of the DPO of the EBA
5	Name and contact details of joint controller (where applicable)	Not applicable
6	Name and contact details of processor (where applicable)	Europlaza Building Security Management: laura.enguixsignes@cbre.fr linda.gomez@cbre.fr Europlaza Canteen Management: europalaza@serenest.fr Proxyclick (for Visitor Management Tool): legal@proxyclick.com SE3M (Maintenance Provider): Marc.bourdon@se3m.fr
7	Short description and purpose of the processing	This record is to cover the processing of personal data that the EBA conducts as part of its physical access control system. This includes the following processing activities:

Nr	Item	Description
----	------	-------------

- **Visitor Badges and Proxyclick Visitor Management Tool:** The processing of data to register expected visitors into the Europlaza building and grant them visitor badges.
- **Staff Badge Creation Process (and set up of badges for the follow me printing service):** The process for granting new EBA staff and contractors with access badges for the Europlaza building, (and enrolling badges for use with printers) as well as the process followed where badges are lost or no longer required.
- **Biometric Fingerprint Processing:** The process by which biometric fingerprint data is captured for certain staff, allowing them to access restricted areas in the Europlaza building.
- **Badge Processing by Serenest Canteen:** The processing of badge data by Serenest Canteen which allows canteen staff to provide meal subsidies to qualifying staff.
- **Processing of Data Related to Car Park Access:** The processing of staff and visitor data for those authorized to use the Europlaza carpark and enabling them to access this carpark.
- **EBA Premises Security:** The processing of personal data to ensure only authorized visitors, staff and contractors can access EBA premises (within the Europlaza building and carpark) and ensuring that EBA assets remain secure. Please note that processing as part of the EBA video surveillance system is covered by a separate record and [privacy notice](#)

All these processing activities are part of the physical access controls for EBA premises (apart from the processing by the Serenest Canteen and the follow me printing service). These physical access controls help the EBA to ensure that only authorized EBA staff, contractors and visitors are able to enter the EBA premises (within the Europlaza building and carpark).

These access control functions support the reception and security staff and form part of the measures taken pursuant to the broader security policies. They ensure the safety and security of EBA staff, contractors, and visitors, as well as property and information within the premises. More specifically these measures allow the EBA to help prevent, deter and if necessary, investigate unauthorised physical access to premises, including unauthorised access to secure areas and protected rooms (areas containing IT infrastructure and operational information). The physical access control system helps prevent, detect and investigate theft of equipment and assets owned by the EBA as well as threats to the safety of personnel working within the premises.

With regards to the processing of badge data by Serenest Canteen this processing enables EBA staff members who qualify for meal subsidies, make use of this benefit.

The processing of data as part of the follow me printing service allows staff to make use of the EBA printing services.

Below is a short description for each of these processing activities.

Visitor Badges and Proxyclick visitor management tool:

Nr	Item	Description
		<p>The Proxyclick visitor management tool is software that allows the EBA to register visitors and contractors within the EBA premises. In order to register a visitor or contractor the EBA collects personal data from visitors via a meeting registration form. This meeting registration form can be completed by the visitors, contractors or their hosts. These forms can be obtained from the Extranet or from reception. These forms are then submitted to reception, who input the data from these forms to the visitor management tool.</p> <p>Once this data has been input into the visitor management tool, the tool will generate an e-mail invitation to the visitor with a unique QR code they can use to check-in/out using the tablets that are available at the EBA reception. Once visitors have checked in, they will be granted an access badge by reception.</p> <p>Where visitors do not have a QR code they have the option to sign in using a paper sign-in sheet, as part of this alternative sign in procedure, the reception staff may request to view ID documentation (such as a driving license or passport) as proof of identity. They will view these ID documents only for the purposes of verifying the visitor's identity. Once verified, visitors will be granted an access badge by reception.</p> <p>No personal data is stored on visitor's access badges. Personal data for visitors is stored within the Proxyclick visitor management tool. When a visitor leaves the EBA their data will be deleted from the visitor management tool. In cases where the visitor personal data is needed to reimburse visitors, data will be kept for up to 12 months to allow for the reimbursement process.</p> <p>Staff Badge Creation Process (and set up of badges for the follow me printing service):</p> <p>When a new member of staff is recruited by the EBA, HR send information regarding the new staff member to the EBA IT staff responsible for creating a staff profile. When the new staff member is onboarded, they will be given the option of sending a photo of themselves or of having a photo taken, to be used for their access badge (and other accounts). The IT staff will use the photo and the data they have been sent in order to create their profile.</p> <p>Once the profile has been created the Corporate Support Unit will use the details from the staff profile in order to create the access badge.</p> <p>So that the access badges can be used by staff to access the EBA printing facilities, the badges are configured to grant access to the printers within the EBA premises. To access this facility staff must provide their access badge and their password. For this activity no data is transferred elsewhere.</p> <p>Once the access badge has been created, an email is sent from the EBA corporate staff to the Europlaza security with the staff members full name and badge number. This is used to create a staff profile in the Europlaza security physical access control system.</p> <p>This personal data is stored locally in the Europlaza security server and access to this EBA staff personal data can only be made by strictly authorized users e.g., security guards or the Europlaza building manager.</p> <p>Where a member of staff leaves the EBA, their access badge will be deactivated, and the personal data contained within the badge and held by Europlaza security will be deleted. The badge will then go through a secure</p>

Nr	Item	Description
		<p>destruction process. It will be kept in a secure for up to a period of two months before it is securely destroyed. Where a staff member reports that they have lost a badge, their badge will be deactivated immediately.</p> <p>Where an EBA staff member forgets their access badge, the staff member will be required to write their name and signature on a sign in sheet and collect a temporary badge. Temporary badges do not contain any personal data.</p> <p>Biometric Fingerprint Processing:</p> <p>Certain areas within the EBA premises are restricted so that only staff that require access to these areas can enter. The EBA restricts access to these areas as they contain sensitive assets that EBA needs to protect. For this purpose, the EBA processes biometric fingerprint data, which is used to verify staff members identity, and ensure that they are authorized to enter these restricted areas.</p> <p>Where a staff member needs access to these restricted areas their line manager will send a request to the Corporate Support Unit who are responsible for processing these requests. The Corporate Support Unit will then take an electronic fingerprint from the staff member in order to add this data to their card. The fingerprint data is programmed on to the staff member's access badge using an internal tool. This tool is integrated with the badge readers so that the badge readers can recognise the fingerprints that have been programmed onto access badges.</p> <p>Data is only stored within access badges and within this internal tool in an encrypted format. This data is never stored on any IT platforms or databases and is not transferred over any networks. These access badges should remain in possession of the staff member or contractor for the duration of their visit.</p> <p>Where a member of staff leaves the EBA, data contained on the card will be deleted in line with the '<i>Staff Badge Creation Process</i>', detailed above. Where a staff member does not want their fingerprints to be taken an alternative procedure exists to enable access.</p> <p>Badge Processing by Serenest Canteen:</p> <p>Access badges are also used for the identification of EBA staff who qualify for the canteen subsidy and for cashless payments when using the canteen facilities.</p> <p>After the Corporate Support Unit have created an EBA staff member's access badge, in order to create a staff profile on the 'electronic IP Restobadge system' and register staff members as qualifying for meals subsidy, the Corporate Support Unit send the EBA staff members full name and badge number to Serenest Canteen via email.</p> <p>This personal data is stored locally in the canteen server. Access to EBA staff accounts can only be made by strictly authorized users e.g., serenest manager or cashiers. Where a member of staff leaves the EBA the data stored by Serenest Canteen will be deleted.</p> <p><u>Cashless Payments</u></p>

Nr	Item	Description
		<p>Serenest give staff members the option of registering their access badge via their online portal for cashless payments. This allows staff to add funds to their access badge using their credit/bank cards and then use their access badge to make payments. EBA staff can also use this service to see the available balance on their account. The processing is governed by separate terms and conditions and a separate privacy notice. For more information see: https://www.e-chargement.com/serenest/europlaza/.</p> <p>Processing of data related to Car Park Access:</p> <p>For security purposes, where staff members require access to the carpark facilities, staff members are asked to fill in a vehicle registration form. This form is used to facilitate the management of the Europlaza car parking places and to ensure that the carpark is kept secure from unauthorised vehicles. The vehicle registration form captures details about staff member's vehicles.</p> <p>Once completed these forms are submitted directly by the staff member via email to designated persons within the Corporate Support Unit who oversee the management of the carpark. The forms are stored in a restricted folder which can be accessed only by designated Corporate Support Unit members. When a staff member leaves the EBA their form is deleted immediately. If a staff member decides that they no longer require carpark access, then they will inform the Corporate Support Unit who will also delete their vehicle registration form immediately.</p> <p>Complete the vehicle registration form is not a mandatory requirement in order to access the carpark area. Where staff members prefer not to disclose the information captured on the form, access can be granted without the completion of the form (where there is a justified reason, and the request is accepted by EBA management).</p> <p>When staff members are granted access to the carpark facilities their access rights (which enable them to enter this area) are added onto their access badge.</p> <p>EBA Premises Security:</p> <p>In addition to the data that is shared with Europlaza Security as part of the '<i>Staff Badge Creation Process</i>' (detailed above) Europlaza Security may process data in order to protect the security of the building and the assets contained within. For this purpose, the following activities involving the processing of personal data may be conducted:</p> <ul style="list-style-type: none"> • Visual checks of badges, the photograph and details on these badges, where this is necessary to verify the identity of an individual (for example in instances where the badge is not recognised by the machine) • The electronic checks of the badges using the physical access control system. • Checking of legal or ID documents, may be required to verify the identity of visitors (for example where systems are unavailable). • Processing of paper-based forms for visitors, visit requests and authorisations, where systems are unavailable.

Nr	Item	Description
		<ul style="list-style-type: none"> • Where there is a security incident, data may be processed in order to safeguard the building, individuals within the building or assets within the building. • Data may also be processed in order to detect, prevent, investigate or prosecute a crime and data may be shared with authorities where this is required for these purposes. • Security staff will also be able to access data captured by the badge readers showing the time staff have entered or exited certain areas, this data will only be processed as is necessary for security purposes. • In certain instances, monitoring data may be processed where this is necessary for security purposes. This will involve flagging certain individuals that are considered a security risk. Where an individual is flagged, they would be put on a monitoring list and alerts would be sent to mandated staff where these individuals enter the premises. This processing will only be conducted where there is a justified and proportionate reason for doing so, and where the processing is a necessary security measure.

Storage of Data by EBA

Operational and active data are stored on dedicated servers with dedicated data storage. The physical access control system is hosted in the EBA data centre. All local security equipment (door controllers, badge readers, IP cameras, monitoring desk PCs) enforcing access control or used for monitoring, contain a copy of the required access permissions. These access permissions are stored locally.

This equipment is physically isolated, offline and protected from unauthorized access. After enrolment, fingerprint minutiae is stored exclusively on the data subject badge and an internal tool that is integrated with the badge readers, so that the badge readers can recognise the fingerprints. This is all contained in an isolated and dedicated system.

Some data (for example the data shared with Europlaza security when a staff badge is created) is stored on Microsoft Office documents such as Word, Excel, PowerPoint, Adobe PDF.

8	Description of categories of data subjects (persons whose data the EBA processes) and list of data categories	<p><u>Description of categories of data subjects</u></p> <p>The data subjects whose data is being processed as part of these activities are persons who needs to access the EBA premises at the Europlaza building, these data subjects may fall under the following categories:</p> <p>Data subject (s) Internal to the EBA</p> <ul style="list-style-type: none"> • EBA Statutory Staff (including permanent staff, contract and temporary agents) • Seconded National Experts • Trainees
---	---	--

Nr	Item	Description
		<p>Data subject (s)External to the EBA</p> <ul style="list-style-type: none"> • Staff of other EU institutions and EU agencies • Visitors to the EBA premises, • Consultants, experts and contractors <p>Data categories/fields</p> <p>Below, all data categories that are processed as part of each data processing activity are listed:</p> <p>Visitor Badges and Proxyclick visitor management tool:</p> <p>Data processed for EBA employees:</p> <ul style="list-style-type: none"> • Full name • E-mail address • Mobile phone number <p>Data processed for EBA visitors:</p> <ul style="list-style-type: none"> • Full name • All other fields are optional and can be activated (or not) by the EBA: e-mail address, phone number, picture, signature, company name etc.) <p>Staff Badge Creation Process (and set up of badges for the follow-me printing service), EBA Premises Security and Biometric Fingerprint Processing, processed by EBA and Europlaza security staff (if necessary):</p> <ul style="list-style-type: none"> • Full name • Photograph • Nationality • Badge number • Fingerprint minutiae (special category data) collected only in cases where a person needs to have access to more restricted areas e.g., IT server rooms. There is no centralised storage of such data, data will only be stored on the data subject's badge, encrypted to a highly advanced standard. Where collection of data is not possible, and an alternative procedure exists to enable access. • Identity documentation • Access rights • Staff roles and tasks associated with system privileges. <p>Badge Processing by Serenest Canteen:</p> <ul style="list-style-type: none"> • Full name

Nr	Item	Description
		<ul style="list-style-type: none"> • Badge number <p>Processing of Data Related to Car Park Access and Security:</p> <ul style="list-style-type: none"> • Full name • Badge number • Vehicle make, model and colour • Vehicle registration plate number
9	Time limit for keeping the data	<p><u>Data collected by the Serenest Canteen and Europlaza Security:</u></p> <ul style="list-style-type: none"> • Will be deleted immediately after employment. <p><u>Visitor data collected by ProxyClick or in EBA forms:</u></p> <ul style="list-style-type: none"> • Will be kept for 12 months to allow enough time for reimbursements of expenses or in case of any investigations. <p><u>Data collected by EBA in relation to access badges:</u></p> <ul style="list-style-type: none"> • General data captured, relating to access badges, will be retained by the EBA for six months after termination of the link between the data subject and the EBA. This retention period strikes a balance between still being able to investigate incidents (which may not be detected immediately, e.g., theft over a holiday period) and not keeping logs unnecessarily and for too long. Information on badge holders must be kept for the duration of badge validity. Keeping it for 6 months after expiry/revocation still allows incidents possibly involving staff who left recently to be investigated (otherwise the EBA would not know whom an expired badge related to). • Data retained in the local door controllers are stored for less than one week until transferred to the central system or overwritten in a round-robin mode. • On enrolment stations, fingerprint images and minutiae are temporarily stored on memory. Temporary storage space will be cleaned at start-up. • Fingerprint minutiae (if used) are stored on the data subject's access badge, for the badge validity period - this will generally be until termination of the link between the data subject and the EBA. <p>Data older than the defined retention periods will be:</p> <ul style="list-style-type: none"> • Copied to an alternate system to be made anonymous and aggregated for statistical purposes, or • Fully wiped from the IT operational systems.

Nr	Item	Description
10	Recipients of the data	<ul style="list-style-type: none"> • EBA designated Corporate Support staff for creating an access badge and following up on security incidents and investigations. • Europlaza building security management to create access right for EBA staff. • Proxyclick software to provide a platform for managing visitors' and contractors' visits to the EBA premises. • Proxyclick's sub-processors, only where providing a service that is necessary for Proxyclick to provide their service to the EBA. • Serenest Canteen: Who process data to enable EBA staff to qualify for meals subsidy. • EBA IT support staff: Who use personal data and a photo to create EBA staff profile. • EBA physical access control systems' maintenance provider (SE3M) when involved in maintenance of the system.
11	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	<p>Except for the data processed by Proxyclick for the visitor management tool, all personal data is processed and stored inside the EEA/EU.</p> <p>The data held by the Proxyclick for the visitor management tool is stored within the EEA/EU. Proxyclick may however allow access to the data by their sub-processors, some of which are located outside of the EEA/EU. Access will only be granted where this is necessary for Proxyclick to provide their service to the EBA. The sub-processors used by Proxyclick that are located outside of the EEA/EU, are located in the US and New Zealand. Proxyclick have standard contractual clauses in place for all sub-processors based in the US (as a transfer mechanism pursuant to Article 48 of the EUDPR). For the data processing conducted in New Zealand, New Zealand have been granted an adequacy decision by the European Commission (pursuant to Article 47 of the EUDPR), demonstrating that their legal framework provides an adequate level of protection for EU data subjects.</p>
12	General description of security measures, where possible	<p>All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored on the servers of the EBA or of its contractors. All processing operations are carried out pursuant to the EBA Decision (EBA/DC/138) of 29 October 2015 on the security of communication and information systems in the EBA. The EBA adopted Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.</p> <p>Processing is performed under the EBA Information Security Framework, published on the EBA intranet. The security measures in place include:</p> <ul style="list-style-type: none"> - Access controls and authentication procedures in place (on a need-to-know basis) - Backups of data - Audit trails

Nr	Item	Description
		<ul style="list-style-type: none">- A policy covering physical security and Information security- A policy covering patch management <p>Proxyclick security measures can be found here</p>
13	For more information, including how to exercise your rights to access, rectification, object and data portability (where applicable):	In order to exercise your data subject rights you can send your request to the EBA by post in a sealed envelope or via email using the below addresses: dpo@eba.europe.eu For the attention of the DPO of the EBA DEFENSE 4 – EUROPLAZA 20 Avenue André Prothin CS 30154 92927 Paris La Défense CEDEX