



Privacy Statement on the protection of personal data in relation to Access control to premises

All personal data are processed in accordance with the provisions of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002.

Identity of controller:

The controller for this data processing activity is Cedefop. Department for Resources and Support. Email: facilities@cedefop.europa.eu

Identity of processor:

- Security Officer and Deputy Security Officer
- External security company (currently G4S)
- Human Resources staff

Purpose of processing:

- Security and safety purposes (control the access of officials, temporary agents, contract agents, contractors, trainees, visitors to the CEDEFOP premises at any time);
- Time recording and Flexi-time administration (for Cedefop staff)
- Unlock offices (for Cedefop staff)
- Prevent, deter, and if necessary, investigate unauthorised physical access, including unauthorised access to secure premises, offices and protected rooms, administration documents, IT infrastructure, or operational information.

Data processed:

- Processed data for security guards' logbook for visitors: data subject's first name, last name, ID number, car plate number (where applicable), entry-exit time in premises.
- Processed data for staff access / clock-in/out: access card number, time of event (entry-exit time in premises, entry time in offices), identification of access location.
- The cards themselves do not store any personal data other than the access card number which is linked (in the security system) to the card holder.

Legal basis / lawfulness:

- Article 5 (a). of Regulation (EU) 2018/1725 i.e. the processing is necessary for the performance of a task carried out in the public interest
- Staff Regulations – art.1.e) 2)
- Cedefop's Security Policy

Recipients of data:

- Processed data for security guard's logbook for visitors: Cedefop security staff (security Officer and backup), External security company (currently G4S).
- Processed data for key cards data: Cedefop security staff (security Officer and backup), External security company (currently G4S).
- Processed data for staff access (clock-in/out): Cedefop security staff (security Officer and backup), External security company (currently G4S) and Human Resources Staff.

Recipients outside Cedefop may include:

1. Local police will be given access if needed to investigate or prosecute criminal offences.
2. Access will be given to the European Anti-fraud Office ("OLAF") in the framework of an investigation carried out by OLAF.
3. Investigators appointed by the AIPN/AHCC in the context of a disciplinary investigation under the rules set out in Annex IX of the Staff Regulations of Officials of the European Communities.

The retention period of the collected personal data:

For security purposes, data are kept for 15 months. The Guards' visitor logbooks are kept for 13 months.

Data subject's rights:

Data subjects have the right to access and rectify (under specific circumstances) their information and request their erasure.

Queries and concerns regarding the processing of your personal data may also be addressed to Cedefop's Data Protection Officer at the following email: data-protection-officer@cedefop.europa.eu

Data subjects are also entitled to have recourse at any time to the European Data Protection Supervisor: <http://www.edps.europa.eu>

LAST UPDATED: 22 September 2021