Data protection information on the Access Control System at the Mannheim campus

PHOENIX Pharma SE (PHX SE), PHOENIX International Holdings GmbH (PIH), PXG Pharma GmbH (PXG) PHOENIX Pharmahandel GmbH & Co KG including the Mannheim distribution centre (PPH), hereinafter jointly referred to as PHOENIX, operate an Access Control System (ACS) at the Mannheim campus as joint controllers within the meaning of Art. 26 GDPR.

The PHOENIX companies involved have determined that PHOENIX Pharma SE, Pfingstweidstraße 10-12, 61899 Mannheim, Germany, is the main contact for data protection enquiries. You can contact the data protection officer at the above address with the addition "To the data protection officer", or contact dataprotection@phoenixgroup.eu .

Purpose of processing and legal basis

With the Access Control System, PHOENIX is pursuing the goal of protecting the Mannheim employee location against unauthorised access. To this end, employee ID cards with dedicated access authorisations are issued to authorised persons.

If employee ID cards are issued to employees, the legal basis is Art. 6 para. 1 lit. b GDPR (employment relationship) in combination with regulatory requirements based on Art. 6 para. 1 lit. c GDPR and Art. 13 para. 1 lit c. EU Critical Resilience Directive. For other persons authorised to issue employee ID cards, the legal basis is the legitimate interest pursuant to Art. 6 para. 1 lit. f GDPR in combination with regulatory requirements based on Art. 6 para. 1 lit. c GDPR and Art. 13 para. 1 lit c. EU Critical Resilience Directive. The legitimate interest lies in safeguarding domiciliary rights and protecting the employee premises from unauthorised access in accordance with applicable EU law.

Scope of processing

The Access Control System covers the entire process of applying for an employee ID card, managing changes to access rights, handling the loss of employee ID cards and returning them.

As part of the application process, an authorized person within PHOENIX fills out a form via a workflow, which then goes through the appropriate approval process. Once approved, the employee ID card is created, and the employee entitled to receive it is notified of its completion via email. After the identity has been verified, the employee ID card is issued to the authorized employee, and the issuance is documented in the form of a handover log. The workflow is supported by Microsoft Office, and we have entered into a data processing agreement with Microsoft. The data is also stored in the administration system of the access control system, which we host ourselves.

The above workflow and the administration system are also used for access authorisation changes, employee badge losses and returns.

The process described above differs for employee ID cards issued to canteen visitors. Canteen visitors eligible for an employee ID card must check in at the front desk and, following verification of their identity, will receive a special employee ID card for canteen visitors. The issuance and return of the card are recorded in a handover log for canteen visitors.

The badges must be worn visibly at all times while on the employee premises.

Type of data processed

Depending on the type of employee ID card, different personal data is processed that is visible on the card:

- Uniquely assignable ID card number
- Full name (not for canteen visitors and external visitors)
- Photo (not for canteen visitors and external visitors)

The following data is also processed as part of the application and administration process for the employee ID card:

- Uniquely assignable ID card number
- Full name to assign to whom an ID card was issued
- Photo (not for canteen visitors and external visitors)
- E-mail address (not for canteen visitors)
- Additional information about the visit, such as company name, purpose of the visit, arrival date and time, and departure date and time (not applicable to employees and canteen visitors)
- Personal master data as part of handover and return protocols and as part of authorisation processes
- Identity documents (ID card or passport) when issuing employee ID cards for clear identity verification (no ID data is stored).

Storage period of the data

As part of the management of the employee ID card process, the photo for the creation of the employee ID card is stored until it is printed and then deleted. The other personal data relating to the employee ID card (personal data on the ID card, in the system and in the handover logs) is disabled after the employee ID card is returned and deleted within 30 days.

Your rights as a data subject

You can assert your rights listed below against the above-mentioned body at any time.

Right to information

You are entitled at any time to request information free of charge within the scope of Art. 15 GDPR about, among other things, your data processed by us, the purposes of processing, the categories of recipients, the planned storage period or, in the case of third country transfers, the appropriate guarantees.

Right to rectification, erasure, restriction of processing

If your data processed by us is incorrect, incomplete or its processing is unauthorised, you can demand that we correct or supplement your data, restrict processing or delete the data to the extent permitted by law, Art. 16, 17 and 18 GDPR.
The right to erasure does not exist, inter alia, if the processing of personal data is necessary (i) for exercising the right of freedom of expression and information, (ii) for compliance with a legal obligation to which we are subject (e.g. statutory retention obligations) or (iii) for the establishment, exercise or defence of legal claims.

Right to data portability

If you have provided us with your data on the basis of your consent or as part of an existing contractual relationship with us, we will make this data available to you in a structured, commonly

used and machine-readable format at your request or - if this is technically possible - transfer it to a third party designated by you.

Right of objection

If we process your data on the basis of a legitimate interest, you can object to this processing in accordance with Art. 21 GDPR for reasons arising from your particular situation. The right to object exists only within the limits provided for in Art. 21 GDPR. In addition, our interests may conflict with the termination of processing, so that we are authorised to process your personal data despite your objection.

Right of appeal

If you have any questions, suggestions or criticism, please contact our data protection officer (see above).
You are also entitled to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement, under the conditions of Art. 77 GDPR, if you consider that the processing of data relating to you infringes the GDPR. The right to lodge a complaint is without prejudice to any other administrative or judicial remedy.
The supervisory authority responsible for us is

The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg
P.O. Box: 10 29 32, 70025 Stuttgart, Germany
Phone: +49 (0) 711/615541-0
Fax: +49 (0) 711/615541-15
E-mail: poststelle(at)lfdi.bwl.de

However, we recommend that you always address a complaint to our data protection officer first.

Last updated: April 2026