

EMPLOYEE PRIVACY NOTICE¹

This Privacy Notice explains how Ascendis Pharma processes your personal data in connection with your employment with Ascendis Pharma and what your rights are in relation to Ascendis Pharma collecting, processing and retaining your personal data. The notice is applicable to all Ascendis Pharma employees.

Data controller

The Ascendis Pharma Group consists of Ascendis Pharma A/S and its wholly owned subsidiaries. The data controller is the Ascendis Pharma company that employs you (as set out in your employment contract). For a list of Ascendis Pharma companies please follow this [link](#).

Contact us

You can exercise your rights and direct any questions or complaints regarding the use of your personal data to dataprivacy@ascendispharma.com or by contacting your HR or Compliance team.

What personal data is collected and processed?

As an employer, we collect and process various categories of personal data about you such as name, bank account, position and title, absence information and competency and development information. In addition, we collect limited categories of confidential and sensitive personal data such as social security number and health information, if relevant and permitted by local law. A non-exhaustive list of personal data that we collect about you can be found in Annex 1.

Why do we need your personal data?

The purpose of processing your personal data is general personnel administration. This includes various tasks such as compensation administration, performance management (including appointments, promotions and demotions), recording and maintaining employment history, absence and disciplinary records, facility management including work environment and related security as well as IT security and provision and support of IT systems, user profiles, investigations etc. Also, handling of claims and disputes, and compliance with legal, regulatory and other obligations. In special circumstances, Ascendis Pharma may also need to process your sensitive personal data, such as health information e.g. to register accidents and to reduce the risk of exposure and spread of diseases.

What are our legal grounds for processing and from which sources do we obtain the personal data?

We will only collect and process personal data about you that is necessary in relation to your employment with Ascendis Pharma. The legal grounds we will use for processing your personal data will depend on the data we process. For most processing, the legal basis will be fulfillment of the employment contract² we have with you. We may, however, also need to process your personal data if Ascendis Pharma is under a legal obligation³ to do so, e.g. to report to tax authorities or to establish, exercise or defend a legal claim⁴. Ascendis Pharma may also process your personal data based on our legitimate interest⁵ in running our business in a certain way e.g. monitor online traffic to provide a safe IT environment or process information about your qualifications to ensure Ascendis Pharma is appropriately staffed. In very limited circumstances, Ascendis Pharma may process data based on your consent⁶ e.g.

in relation to using your photo.

Most of the data we collect and process will be obtained directly from you, but in some limited circumstances, we obtain information about you from other sources e.g. benefit providers or tax authorities.

Who will receive your personal data?

We will limit the sharing of your personal data as much as possible to what is necessary. This may include sharing your personal data with other relevant Ascendis Pharma companies for administrative purposes, business partners and vendors that support our business (such as internet, payroll or pension providers) or government authorities e.g. for tax reporting purposes. We may also disclose your personal data to third parties in the context of e.g., any potential sale, merger, acquisition, or corporate reorganization of Ascendis Pharma or to obtain legal advice.

In all cases where we share your personal data, we will ensure that the recipients of your personal data, where relevant, are bound by confidentiality and other contractual obligations, process the data only according to our instructions and only for legitimate business purposes. Besides this, we take appropriate steps to ensure that the recipients of your personal data implement appropriate technical and organizational measures, e.g. access control, to ensure a sufficient security level to protect your personal data.

Transfer of your personal data to third countries (countries outside EU/EEA)

Depending on the kind of processing we carry out, your personal data may be transferred to and processed in countries other than your home country. These countries may have data protection laws that are different to the laws of your home country (and, in some cases, may not be as protective).

No matter where we might need to transfer your data to, we will make sure that appropriate safeguards are in place regardless of whether the transfer is between Ascendis Pharma companies or to a third party. In Europe, this means that we will enter into what is known as EU Standard Contractual Clauses (SCC) for data transfer, a copy of which can be obtained by contacting your HR team.

For how long do we keep your personal data?

We will keep your personal data for as long as is necessary to carry out the task it was collected for. Once that purpose has been achieved, we will delete all information about you unless we are required by applicable laws to keep your data for a longer period. For further information about retention periods, please contact your HR team.

Your rights

You can, at any time, ask for information about our processing of your personal data, receive a copy of the data we keep about you, or ask us to send your personal data to somebody else. You can also ask us to rectify wrong or insufficient data about you or delete your data. In addition, you always have the right to complain about our processing of your personal data to the relevant data protection authority. A list of EU data protection authorities can be found here: [Our Members | European Data Protection Board \(europa.eu\)](#)

¹ GDPR article 12-14

² GDPR article 6(1)(b)

³ GDPR article 6(1)(c)

⁴ GDPR article 9(2)(f)

⁵ GDPR article 6(1)(f)

⁶ GDPR article 6(1)(a)

Annex 1

As part of your employment with Ascendis Pharma, we will process various types of personal data about you. The different categories are described in more detail below.

Individual details. Such as your name, address, email, date of birth, gender, photo (if you have provided one), emergency contact information, marital status (DE and US only), military status (US only).

Employment details. Such as employee ID, position, title, job description, employment date, office location, manager/employee competence and development conversations, time registration, absence information (vacation, PTO, illness, maternity/paternity leave etc.), business travel management, recording of internal meetings, training completion rate, results of personality and other tests, performance and disciplinary records, I-9 documentation and workers compensation classification (US only).

Educational background. Such as education, academic and professional qualifications, resume/CV, training/courses, certificates.

Financial information. Such as salary and other compensation, bank details, benefit plan enrolment election (US only), tax information, pension scheme information, employment benefits, employment expenses, reimbursements, canteen registrations (DK only), warrant and RSU management, company credit card details and use.

IT and Facilities information. Such as system and application access data (System ID, LAN ID, Email account, Instant messaging account, Mainframe ID, System passwords, Access logs, Activity logs, Country code, IP address (including the PC to which the IP address belongs), online traffic, employee access code, car registration (DK only).

Monitoring data. Such as CCTV data (where in operation), logging and control of IT use (including prompts), printer log, background and sanctions screenings (where permitted and required under local law).

Sensitive data. Such as health information (e.g. specific information about illness in connection with sickness absence (DK and US only)), vaccine status and related health information (e.g. symptoms, date of onset of symptoms) in the circumstances where this becomes relevant, permitted and required by local law, ethnicity (US only), disability status (DE and US only).

National identifiers. Such as national identification number (to the extent used in your country), work permits, visas, social security number (in Denmark: CPR number), copy of passport and/or driver's license.