

Employee Privacy Policy

SimCorp A/S

May 2018

Employee Privacy Policy

SimCorp A/S

1. Introduction

SimCorp is committed to maintain the confidentiality, accuracy and security of the personal data of our employees. This policy describes what personal data SimCorp collects from employees, how we use it, how we store it, and who we share it with. Further, the policy describes the security measures set out to protect the personal data.

This policy covers employees in SimCorp A/S. If you have any questions with regard to the policy, please reach out to HR.

2. Which personal data does SimCorp collect and why?

SimCorp collects different types of personal data about employees in order to manage the employee relationship and to run the daily operation of the company. The information may include:

- Name, address, telephone number, gender, date of birth, CPR no., account no.
- Copy of passport
- Criminal record
- Emergency contact details
- Application and CV
- Personality test
- Salary and benefit information
- Sick leave and other absence
- Health
- Pension and insurance information
- Photo
- Education and training
- Former employment
- Time registration
- EPR data
- Expenses
- Office access log
- Warning and termination
- E-mails and internet (as further described in the Information Security Policy)

The information will primarily be collected directly from you. If we collect information from third parties, we will make sure that this has the necessary legal basis, and we may ask your consent, if necessary.

Personal data will only be collected and processed to the degree necessary and relevant for the purposes for which they are processed. Some information is necessary for fulfilment of the employment relationship between you and SimCorp. It may also be set out by law that an employer has to collect certain information, or SimCorp may process certain information in order to comply with legal obligations. Further, SimCorp may base processing on a consent from the employee.

Employee Privacy Policy

SimCorp A/S

SimCorp keeps the information above only for the period necessary to fulfil the purposes mentioned. This means that we will normally keep your information for the duration of your employment at SimCorp and for 6 years after your resignation or dismissal. Some information may be deleted earlier than this if there is no longer a need to keep it.

The legal basis for processing your data can be found in the General Data Protection Regulation (GDPR) and in the Danish Data Protection Act (DDPA):

- GDPR article 6.1(a): Consent
- GDPR article 6.1(b): Processing is necessary for the performance of a contract
- GDPR article 9.2(a): Consent to the processing of special categories of data (such as health)
- DDPA article 8.3: Consent to the processing of criminal records

3. When does SimCorp disclose your personal data?

SimCorp may be legally obliged to share personal data of employees with certain public authorities like SKAT, Danmarks Statistik and municipalities.

As part of the compulsory pension and insurance schemes, SimCorp will share relevant information with the broker and the pension and insurance provider.

If you are outplaced to or from another Market Unit, SimCorp A/S may share information with that Market Unit if necessary for tax or salary reasons or for other necessary purposes.

SimCorp may use suppliers who get access to employee personal data, e.g. IT or hosting providers, external consultants, vetting providers etc. SimCorp will make sure to have agreements with such third parties that ensures protection of personal data. SimCorp will enter into data processing agreements that defines how personal data may be processed, what kind of security measures must be established by the supplier, and the confidentiality obligations imposed on the supplier. If personal data is transferred out of the EU, SimCorp will ensure that appropriate measures are taken to protect personal data in accordance with applicable data protection law. This may be in the form of EU standard contractual clauses, binding corporate rules or the EU/US privacy shield.

4. Security

SimCorp maintains appropriate technical and organisational measures to protect employee personal data against unauthorised or unlawful processing, accidental loss, destruction or damage or other violation of the provisions of GDPR and local law.

Personal data regarding employees will be subject to SimCorp's Information Security Policy, which among other things lays down rules on physical and electronic access to buildings and IT systems. Physical employee files are stored in locked cabinets and when no longer in use, they are securely shredded.

Employee Privacy Policy

SimCorp A/S

Moreover, at SimCorp access to personal data is based on the principle that access to data should be restricted to those who have a legitimate need for the data and the principle that as few people as possible have access to such data. In other words, we operate on the need-to-know and nice-to-know principle. Only employees who have a need-to-know business need for personal data may gain access to such data. This applies both to electronically stored data and to data we store in physical form.

5. Your rights and who to contact

You have a right to know what personal data is processed about you. Also, if any information processed is inaccurate, you have the right to get the information rectified. In certain situations, you may request to have information about you deleted. However, this right does not apply if SimCorp still needs the information for the purposes mentioned above.

Please reach out to HR if you want to request access or has questions to the processing of your personal data.

If you feel the need to lodge a complaint about SimCorp's processing of your personal data, this can be done by contacting Datatilsynet (please go to datatilsynet.dk for further information).

6. Updates of the policy

This policy may be updated from time to time. Please go to SimLink for the most recent version.

The current version was last updated May 2018.