Employee Data Processing Policy

Management in GF Inveco Group
Updated December 2024

This policy describes how we protect personal data and ensures that employees are aware of the rules governing the use of personal data they have access to as part of their work. This policy supplements our other policies on IT security, internet, email, etc.

As part of our personnel administration, the company processes information about our employees. This is done in compliance with data protection regulations, including data security requirements.

The company ensures that all personal data in personnel administration is protected so that no information is destroyed, lost, or degraded. At the same time, the company ensures that no information is disclosed to unauthorized persons, misused, or processed in violation of regulations.

All employees handling information about colleagues must comply with the following rules:

---

1. Data Controller

GF Inveco Group is the data controller for a range of personal data, including data we receive such as:

- Applications
- CPR number, name, address, phone number, bank account number, tax information, and pension details (payroll processing)
- Name and address (employment contracts)
- Passport, driver's license (for visa applications, powers of attorney, banking activities, etc.)
- Driver's license and forklift certificate (driving company vehicles and forklifts)
- Photos (for websites, brochures, etc. – consent form completed)
- Personnel administration information

The Danish Working Environment Authority may request information on forklift certificates. Regarding documents for banks, we are subject to the Financial Supervisory Authority.

---

2. Purpose of Processing

To manage personnel administration of employees within the company, including in accordance with applicable laws and regulations covering employees.

---

3. Unsolicited Applications & Applications in General

Applications are scanned and archived on the management drive, where they are stored for a maximum of 6 months. Only management has access.
Paper applications are shredded after scanning.

---

4. Employee Data Digitally

A digital folder is created for each employee on the management drive containing:

- Employment contracts
- Amendments to contracts
- Consent forms
- Passport, driver's license, and forklift certificate
- Photos
- Various personnel documents

When an employee leaves, all material is deleted after 6 months except for employment contracts, terminations, and any liability-related documents. These are stored for the current year + 5 years in accordance with the Accounting Act.

Paper documents are shredded after scanning.

Employees can request access to their own information from management at any time.
Rules regarding the storage of registered personal data are provided in the company's employee handbook.

---

5. Employee Data in Physical Folders

Payroll folders with pay slips and other payroll material (annual statements, holiday pay lists, etc.) must be kept in a locked cabinet accessible only to management.

---

6. Child Certificates

Not relevant for the company.

---

7. Deletion and Data Portability

Handled by company management.
We only process data for the stated purpose, and it is deleted when no longer needed. All confidential material is shredded upon disposal.

---

8. Data Protection

We have implemented technical and organizational security measures regarding the personal data we process to ensure that data is not altered, lost, or disclosed to unauthorized parties. Measures include firewall, web security, server, PC, and network equipment security updates, and protection against viruses and unwanted programs.

We also have authorization and access restrictions to ensure personal data is only accessible to relevant employees who are bound by confidentiality and instructed in handling personal data.

Management is responsible for data protection matters.

---

9. Data Breaches

Management is obliged to inform affected persons immediately and notify the relevant supervisory authority within 72 hours.

---

10. Disclosure to Third Parties

We only disclose or transfer personal data to third parties in accordance with the law and only for the purposes described.

We use external providers for IT operations and services such as payroll processing, and these providers have access to our personal data. In each case, we ensure data is protected through confidentiality or data processing agreements.

---

11. Special Sensitive Data

We do not process special sensitive data other than CPR number and bank account number. These two items are only held by the payroll bureau and in a physical folder in a locked cabinet, accessible only to management.

We do not consider our processing to be associated with particular risks.

---

12. Operations in Multiple Countries

We operate in several EU and EEA countries and rent server space in the cloud, thus following the regulations of the countries in which the companies are domiciled.