3.1.2 Managers The division heads, department heads, and other managers of the COMPANY are internally responsible for ensuring data protection within their organizational unit in accordance with the relevant data protection regulations. They must inform the assigned positions and employees about the requirements of data protection and monitor compliance with the regulations. They ensure that their employees, especially temporary staff, are informed about this policy.

Within the assigned areas of responsibility, managers are particularly responsible for ensuring:

- Lawful and purpose-bound processing of personal data ("Lawfulness and Purpose Limitation", see sections 2.2.3 and 2.2.4)
- Processing that is appropriate and limited to what is necessary ("Data Minimization", see section 2.2.5)
- Regular awareness-raising and training of employees involved in processing activities about the essential provisions of data protection law and the regulations established for the COMPANY, considering specific training needs
- Identification and initiation of awareness measures
- Privacy-compliant process and technology design ("Privacy by Design" / "Privacy by Default", see section 2.4)
- Storing personal data only as long as necessary for the purposes for which they are processed, considering any statutory retention periods ("Storage Limitation"; deletion concepts, see section 2.2.5)
- Appropriate proof and necessary documentation, especially when introducing or modifying procedures involving personal data (e.g., the record of processing activities, see section 2.7), including regular review of the documentation's accuracy
- Conducting threshold analyses and data protection impact assessments (DPIAs) as necessary (see section 2.8)
- Early involvement of the designated data protection coordinator or IT compliance manager in the respective division (see section 3.2)
- Compliance with reporting obligations and further handling/documentation of reported data breaches according to the "Process for Reporting and Handling Data Breaches (GK102.2180P)" (see also section 2.9)
- Ensuring data subject rights (see section 2.6).

Managers may delegate tasks to employees, but the responsibility remains with them.

3.1.3 Employees Employees must be familiar with all measures and regulations concerning data protection that affect them or their activities and ensure that these are observed and implemented before any new or altered processing activity. Key measures and regulations described in this policy include, for example:

- Checking the lawfulness/legitimacy of data processing
- Documentation obligations (e.g., record of processing activities)
- Ensuring data subject rights
- Commissioning service providers (data processing agreements)
- Checking the lawfulness/legitimacy of data transfer to external parties (third parties)
- Obligation to delete data/data minimization principle

Employees must not make any changes to their own ACCOUNT. Likewise, handling cases as part of a mailing addressed personally to an employee is not permitted. The same applies to ACCOUNTS and mailing transactions involving relatives, friends, and acquaintances.

It is also prohibited to access ACCOUNTS or data of potential debtors or other third parties, regardless of the assigned processing tasks. Even read-only accesses are systemically logged and evaluated in case of suspected misuse.

Employees must handle (potential) data breaches according to the specifications in section 2.9 of this policy and the "Process for Reporting and Handling Data Breaches (GK102.2180P)