ablefy GmbH

Technical and Organizational Measures

Content

Foreword....3
Data protection and data security concept....3
1.Physical Access Controls....4
2.Logical Access Control....4
3.Data Access Control....5
4.Storage Device Control....5
5.Communication Control....5
6.Transmission Control....5
7.User Control....6
8.Service Provider Control....6
9.Storage Control....6
10.Availability control....7
11.Reliability....7
12.Data Recovery....7
13.Operating system....7
14.Software....7

Foreword

This document describes the binding technical and organizational measures in connection with the processing activities carried out between the data controller and processor. The measures described in this document describe the data protection and data security concept at the site.

Data protection and data security concept

The following catalog of measures describes the individual technical and organizational measures to be taken within the scope of the processing activities pursuant to Art. 24(1) GDPR. The GDPR requires companies to secure the processing of personal data by appropriate technical and organizational measures, and to anonymise or pseudonym use personal data wherever possible. The measures taken must take into account the risk of the respective data processing activities and correspond to the current state of the art. The controller meets these requirements through the effective interaction between data protection management and information security management and has taken appropriate measures to safeguard the processing of personal data. These data protection principles should also be carefully considered: availability, confidentiality, integrity and resilience. The data protection principles are based on the following definitions relevant to information security:

- Confidentiality: Data, information and programs shall be protected from unauthorized access and disclosure.
- Integrity: The term integrity refers to the correctness of the information and data processed.
- Availability: The term availability refers to information, data, applications and systems and refers to their functionality and retrievability.
- Load-bearing capacity: As a special aspect of availability, load-bearing capacity requires systems to be designed to be as robust as possible, even in the event of a malfunction, failure or high load.

1.Physical Access Controls

Unauthorized persons must be denied physical access to data processing equipment with which personal data are processed or used.

Access Control System:

- A centrally managed access control system is used for the company.

Access Control System - Administration:

- The access control system is managed in the following way:
    - Electronic

Access Control System - Technical means:

- The access control system is based on the following technical means:
    - Token/Transponder
    - Key

Access Control Systems - Lockable rooms:

- All rooms in which access to personal data is possible are lockable.
- Securing the premises / buildings of the company:
    - The company premises / building is secured from public ground by:
        - Office in a larger building complex
        - Lockable door
        - Porter

Security at the Company Premises - Alarm System:

- The company premises or parts of it are safeguarded by an alarm system:
    - Server - External Use:
        - External servers are rented in the company.
    - Server - Internal Use:
        - No servers are used on the company premises.

2.Logical Access Control

Unauthorized persons shall be denied access to data processing equipment with which personal data are processed or used.

Access to Personal Data in Visitor Areas:

- It is ensured that personal data in the company is not freely accessible in visitor areas.
    - Password Manager:
    - A password manager is used in the company.
        - The following password manager is used: 1Password

Password Manager - Access Control:

- The used password manager offers sufficient access control and encrypted storage.

Passwords Complexity:

- The system enforces a minimum password length of 8 characters.
- Passwords must contain a mix of uppercase letters, lowercase letters, numbers, and special symbols.

Single Sign-On Procedure:

- A single sign-on procedure is used in the company.

Storage of Sensitive Information:

- Employees were instructed to lock personal data up when leaving their workplace in the company (so-called Clean-Desk-Policy).

Two-Factor-Authentication:

- Two-factor authentication is used in the company.

3.Data Access Control

It must be ensured that persons authorized to use a data processing system can only access the data according to designated access permissions.

Departing Persons - Withdrawal of Authorisations:

- All access authorisations and access rights of a departing person are blocked/deleted promptly.

IT-Security - Firewall:

- One or more firewalls are used against unwanted network access in the company.

The following firewalls are used in the company:

- AWS Web Application Firewall
- Watchguard Firewall

4.Storage Device Control

Storage devices should not be read, copied, changed or removed without authorisation.

Storage Device Management - Authorisation for Creation:

- A process for the authorisation of storage device creation has been put in place.

Storage Device Management - Inventory List:

- Inventories for the following storage devices are kept in the company:
    - Laptops
    - Mobile phones
    - Tablets

Workplace - Sealable Containers:

- There are lockable containers available at every workplace to securely store documents and storage devices in the company.

5.Communication Control

It must be possible to determine and establish where personal data can be transmitted by data transmission equipment.

- Connection to the Telecommunications Provider:
    - The following method is used to connect to the telecommunications provider:
        - Regular DSL/fibre optic connection

6.Transmission Control

It is necessary to prevent unauthorized reading, copying, modification or deletion of data during the transfer of personal data or during the transport of data carriers.

Data Transmission - Storage Devices:

- No storage devices containing personal data are transferred within the company.

Encryption of Transmission:

- Data is encrypted during transmission using the following procedures/protocols:
    - SSL/TLS

7.User Control

It must be prevented that data processing systems can be used by unauthorized persons using data transmission devices.

Administrators - Consistent Accounts:

- Administrator accounts are used at the following level in the company:
    - Database
    - Application

Administrators - Special Accounts:

- Special administrator accounts are used in the company.

Data Protection for Teleworkers:

- Teleworkers were made aware of compliance with relevant data protection regulations.

Departing Persons - Reclaiming Company Owned Property:

- All company-owned property containing personal data is reclaimed by a departing person.

Employee Training:

- The following measures are taken to make employees aware of the importance of data protection and to oblige with them in accordance with the requirements:
    - Training of all employees with access rights
    - Informing employees about innovations on the subject of data protection
    - Commitment of employees to rules of conduct
    - Internal company data protection guidelines

    - Obligation of employees to maintain data secrecy

Employee Training - Regularity:

- Regular training sessions are held on the subject of data protection in the company.

8.Service Provider Control

It must be ensured that personal data processed under contract can only be processed according to the instructions of the client.

External Service Provider - Remote Maintenance:

- No remote maintenance is carried out by the company.

External Service Providers:

- The company works with external service providers.

9.Storage Control

Unauthorized entry into storage systems as well as unauthorized access to, modification or deletion of stored personal data shall be prevented.

Measures for Data Locking and Data Deletion:

- Data locking/deletion measures are in place, meaning data can easily be locked/deleted in all systems upon request.

Password Protection - Password List:

- No unencrypted password list is kept.

10.Availability control

It must be ensured that personal data are available at all times and are protected against accidental destruction or loss.

Archiving Concept - Legal Retention Obligation:

- There is a legal storage obligation for the archived documents.

IT Security - Malware in Encrypted Data:

- Encrypted data in the company is checked for malware as well.

IT Security - SSL/TLS Scanner:

- An SSL/TLS scanner is used to check encrypted data packets for malware as well.

IT Security - SSL/TLS Scanner Examination:

- The checking and classification of the scanned data packet in the company takes place automatically.

IT Security - SSL/TLS Scanner Name:

- The following TLS/SSL scanner is used:
    - AWS Cert Manager

11.Reliability

It must be ensured that personal data is secured against accidental loss or destruction.

Critical Systems - Redundancy:

- Critical systems and the infrastructure are designed redundantly.

IT Security - Network Monitoring:

- A software is used to check the network or the applications in the company.

The following software is used:

- NewRelic, AWS CloudWatch, Sentry

12.Data Recovery

It is necessary to ensure that personal data can be quickly restored in the event of a physical or technical incident.

Backups:

- Backups in the company are performed by:
    - Service providers
    - Cloud provider

13.Operating system

Unauthorized individuals must be prevented from gaining access to operating systems.

Password Protection - User Account:

- Each user account of the operating system in the company is protected by a password.

14.Software

Unauthorized individuals must be prevented from gaining access to any applications.

Software - Separation between Environments:

- Productive, test and development environments including the databases are separated from each other in the company.