TECHNICAL AND ORGANIZATIONAL MEASURES (TOM) OF LUEDERS & PARTNER GMBH

Contents

1. Introduction and Framework

The following stipulations represent the technical and organizational measures across processes and procedures according to Art. 32 Para. 1 GDPR of Lueders & Partner GmbH.

2. General Regulations on Data Protection and the use of Company IT

- The data protection procedure is established and a data protection manual is available
- There is an IT security concept
- Private use of the Internet is permitted with restrictions
- The private use of company, mobile communication facilities is permitted
- Cooperation with contractors takes place on the basis of contractual regulations, in accordance with Article 28 GDPR

3. Confidentiality

3.1. Premises

The business premises are on the ground floor of Magdalenenstraße 11, 20148 Hamburg. The access doors to the business premises are always closed and can only be opened from the outside with a key. Each employee has a key. The allocation of keys is documented. A loss must be reported immediately. After termination of employment, the key must be returned.

As part of access control, measures have been taken to prevent unauthorized persons from gaining physical access to data processing systems. In the broadest sense, this includes computers of all kinds - servers, PCs, notebooks, smartphones, copiers and other devices that are suitable for processing personal data. However, manual documents are also among the documents worthy of protection. These are to be cleaned up or locked by the individual employees after the close of business in accordance with data protection regulations.

Unauthorized persons are all those who do not have to be at the corresponding devices due to the tasks assigned to them or as visitors. The above Data processing systems are secured accordingly with passwords, locks or other locks.

Visitors register at the reception when entering the business premises and are registered there. Visitors are guided to the conference room or meeting lounge by an employee and looked after there until the person or persons to be spoken to have arrived.

Alternatively, visitors can be picked up by an employee at reception and accompanied during their stay in the business premises. At the end of the visit, the guests are escorted to the door and said goodbye there. The windows must always be closed after business hours. Other safeguards for the building, windows and doors must be observed.

Access to certain security areas of the office (e.g. server room) is only permitted for authorized employees. A locking service is hired to close and block off the entrances to the building.

All offices are equipped with an alarm system, which is activated when the last employee leaves the office.

3.2. Authorization

The following measures ensure that data processing systems cannot be used by unauthorized persons.

- Server systems with graduated and/or role-based authorization concept (MS domain concept)
- Clear assignment of user accounts and passwords - each user has their own password in the network, which only they know
- Password policies related to password security and expiration
- Screen lock with password protection on reactivation
- Logging of the use of the IT systems and evaluation of the logs
- Encrypted connections (SSL) for external access via VPN
- Use of secure WLAN connections (WPA2)
- Use of virus scanners with constantly updated virus patterns
- Automated standard routines for regular updating of protection software and virus scanner patterns, operating system patches and operating system security patches
- Use of firewall systems
- Use of a remote maintenance program with sufficient encryption
- Policy for onboarding new employees and in the event of a departure from the company
- Use of encrypted USB data storage devices that can only be decrypted by authorized users
- Automatic PIN/password locks for mobile devices

3.3. Access

The following measures have been taken to ensure that those authorized to use a data processing system can only access the data subject to their access authorization, and that personal data cannot be read, copied, changed or removed without authorization during processing, use and after storage.

- Special, locked rubbish bins are used to destroy sensitive documents. These are regularly picked up by a specialist company that guarantees professional and data protection-compliant disposal

- Data carriers to be disposed of are either disposed of professionally and in accordance with data protection regulations by a specialist company, or are formatted in such a way that the content cannot be restored using the current state of the art
- System access is divided into read/write and change rights
- Database systems have no direct external connection
- Database systems with graduated authorization concept
- The number of administrators with the appropriate access rights is limited to what is absolutely necessary

3.4. Separation
The following measures ensure that data collected for different purposes are processed separately.

- Logical separation of development systems from productive systems
- Use of an authorization concept for employees in the domain
- Use of an authorization concept for administrative or developer access (database rights, etc.)
- The data is backed up on different backup media (NAS) 4. Integrity

4. Integrity

4.1. Data Transfer
- Instruction that no sensitive/personal data may be sent via unencrypted paths
- Data is encrypted during transport (e.g. VPN, SFTP, HTTPS for file transfer)
- Use of secure encryption methods (AES, min. 256 bit)
- Sending of sensitive, especially personal data only on the basis of previously made contractual agreements

4.2. Data Input
- Authorization profiles or groups are defined for authorized data entry
- Access is differentiated through differentiated read, change and delete authorization
- Entries in the customer management system are logged with the type of change, processor and time stamp

4.3. Contractors
- There are contractual regulations (according to § 11 contract services) with corresponding companies (sub-contractors)
- Orders to sub-contractors are only awarded with the prior written consent of a client
- Compliance with the specifications for the technical and organizational measures to protect data in accordance with Section 9, Annex BSDG is checked - also at sub-contractors
- When selecting order service providers, care is taken and, in particular, value is placed on data security

5. Availability and Resilience

5.1. Availability Control
- Complete backup and recovery concept
- Storage of backups in separate fire compartments
- Regular testing of data recovery
- Use of protection programs and protection methods (e.g. virus scanners)
- Use of RAID systems (hard disk mirroring) for secure data storage
- Use of uninterruptible power supply

- Non-destructive fire suppression systems using CO2 fire extinguishers
- Contingency plan for data recovery in case of accidental deletion, partial hardware failure/ loss and total loss/disaster
- Use of networked fire detectors in the offices with alarm function on the smartphone
- fire protection officers and their fire protection assistants
- Use of air conditioning to keep the temperature in the server room at a constant optimized level

6. Final Statement

In addition, the data protection officer ensures through the data protection organization that the “technical and organizational measures pursuant to Art. 32 GDPR are appropriately and effectively integrated into the operational processes. In particular, this is done by creating and maintaining a data protection management system and contacting the responsible state supervisory authority for data protection.

19.04.2023