10117

SoftBCom Berlin GmbH
Schiffbauerdamm 19,
Berlin
+49 30 51302118
www.softbcom.com

Technical and organisational measures in accordance with Art. 32 GDPR

This document describes the technical and organisational measures (TOM) in accordance with Art. 32 GDPR that SoftBCom Berlin GmbH (SoftBCom) has implemented to protect the personal data of its customers. This summary serves the purpose of transparency towards contractual partners, in particular in the context of order processing.

Physical Access Control

To secure physical access to SoftBCom's office premises, the following measures apply:

- Third parties may only remain in office areas when accompanied by a SoftBCom employee.
- Authorized personnel for server rooms are specifically designated.
- Access to locked areas is managed through a key policy; keys are only issued to authorized individuals.
- The premises are protected by secure entrance doors with coded locks, issued only to authorized staff.

System Access Control

SoftBCom Berlin GmbH
Schiffbauerdamm 19,
Berlin
+49 30 51302118
www.softbcom.com

System access control is intended to prevent unauthorised persons from gaining access to IT systems and data processing facilities. The following measures have been implemented at SoftBCom Berlin GmbH:

User authentication:

- Users are identified to the data processing system by means of an individual user ID and password;
- The screen workstations are automatically locked after 5 minutes of inactivity (password protection for screen saver);
- The internal network at the office location is protected against external access by a hardware firewall.

Password guidelines:

- Personal password created by the user;
- At least 8 characters, including special characters and numbers (according to internal work instructions);
- No disclosure of passwords to third parties (regulated by mandatory work instructions).

Authorisation management:

- Access rights are assigned on a role-based basis according to the principle of minimum rights assignment;
- The validity of existing authorisations is checked regularly;
- When employees leave the company, their accesses are deactivated immediately.

SoftBCom Berlin GmbH
Schiffbauerdamm 19,
Berlin
+49 30 51302118
www.softbcom.com

Data Access Control

A formal access rights policy exists for:

- Administration of access by system administrators.
- Assignment of permissions for processing personal data.
- Access authorisations are created according to task area and requirements.
- Differentiated rights for reading, modifying, or deleting data.
- Data carriers or documents that are no longer required are disposed of in accordance with data protection regulations.

Data Transmission Control

Access to or transmission of personal data to third parties occurs only on a case-by-case basis with prior written consent of the customer.

- Recipients, transmission methods, authorized personnel, and categories of transmitted data are documented.
- In the case of transmission over unsecured channels (e.g. email), encryption is used.

Input control

The access authorisations were granted and documented in writing.

The entry, modification or deletion of personal data is only logged for the contractor's own data. In the area of the SoftBCom Berlin GmbH office, no logging shall take

SoftBCom Berlin GmbH
Schiffbauerdamm 19,
Berlin
+49 30 51302118
www.softbcom.com

place in relation to commissioned data processing. Personal data of the client will only be entered, changed or deleted outside the client's target system with the written consent of the client.

Order control

Compliance with data security regulations is monitored by the contractor and the client is informed if there are violations or if there is a suspicion that the client's data security requirements are inadequate.

- All employees of the contractor are bound to data secrecy (§5 BDSG).
- All employees have been trained in data protection.

Availability control

Availability control ensures that personal data is available reliably and promptly when required, even in the event of technical incidents or extraordinary events. The following measures have been implemented by SoftBCom Berlin GmbH:

- Regular data backups on redundant systems;
- Use of highly available cloud infrastructures with fail-safety;
- Use of monitoring tools for real-time monitoring of critical systems;
- Documented emergency plans for the recovery of data and systems (disaster recovery plan);
- Data can only be accessed via encrypted connections (e.g. HTTPS, VPN);

- There is a formalised approval procedure for new data processing procedures and for significant changes to existing processes. Data protection requirements are checked and documented prior to introduction.

Data Location and Processing:

- The client's personal data is always processed and stored in the geographical area specified in the contract or product:
    - For customers based in Germany: exclusively in Germany (e.g. on servers of Hetzner Online GmbH).
    - For customers from other EU member states: within the European Union.
    - For customers from third countries: in the contractually defined region (e.g. EU data centre), if technically available.
- Personal data is **not** transferred outside of this defined area. If processing outside this area is necessary for technical or functional reasons (e.g. to use external AI services), the data concerned is **completely anonymised beforehand** so that there is no longer any personal reference within the meaning of the GDPR.

Use of Third-Party Systems:

- If third-party systems (e.g. AI-supported tools such as ChatGPT) are used as part of the service, only anonymised or aggregated data is used so that there is no longer any personal reference.
- There is no transfer of personal data to such third-party providers.

10117

SOFT COM

SoftBCom Berlin GmbH
Schiffbauerdamm 19,
Berlin
+49 30 51302118
www.softbcom.com

Separation requirement

The measures taken at SoftBCom to control the separation are: software exclusion in the sense of client separation, separation of test and routine programmes, separation through access regulations and file separation. For example, all production systems must be operated separately from the development and test systems.

- Technically, this is realised by segmenting networks with activated firewall rules.
- Production data may not be used as a copy for test purposes.
- Test data must not be used in a production environment.
- Details are regulated in the internal safety guidelines for safe operation.

Place, date Signature of the responsible body