SoftBCom Berlin GmbH
Schiffbauerdamm 19,
10117 Berlin
030 51302118
www.softbcom.com

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) gemäß Art. 32 DSGVO, die die SoftBCom Berlin GmbH (SoftBCom) zum Schutz personenbezogener Daten ihrer Kunden umgesetzt hat. Diese Zusammenfassung dient der Transparenz gegenüber Vertragspartnern, insbesondere im Rahmen der Auftragsverarbeitung.

Zutrittskontrolle

Die Zutrittsregelungen für den Officebereich der SoftBCom Berlin GmbH werden durch folgende Maßnahmen umgesetzt:

- Aufenthalt von Fremden im gesamten Officebereich ist nur in Anwesenheit von Mitarbeitern der SoftBCom Berlin GmbH möglich.
- Die zutrittsberechtigten Personen für die Rechnerräume sind festgelegt.
- Es existiert eine Schlüsselregelung (verschlossene Türen; Schlüsselausgabe nur an Befugte)
- Maßnahmen zur Objektsicherung: Es gibt Sicherheitstüren im Eingangsbereich mit codierten Schlüsseln. Die Schlüsselausgabe erfolgt nur an Befugte.

SoftBCom Berlin GmbH
Schiffbauerdamm 19,
10117 Berlin
030 51302118
www.softbcom.com

Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu IT-Systemen und Datenverarbeitungseinrichtungen erhalten. Folgende Maßnahmen sind bei der SoftBCom Berlin GmbH umgesetzt:

Benutzerauthentifizierung:

- Die Identifizierung der Benutzer gegenüber dem Datenverarbeitungssystem erfolgt über individuelle Benutzerkennung und Passwort;
- Die Bildschirmarbeitsplätze werden nach 5 Minuten Inaktivität automatisch gesperrt (Passwortschutz für Bildschirmschoner);
- Das interne Netzwerk am Office-Standort ist durch eine Hardware-Firewall gegen Zugriffe von außen geschützt.

Passwortrichtlinien:

- Persönliches Passwort, erstellt durch den Nutzer selbst;
- Mindestens 8 Zeichen, inklusive Sonderzeichen und Zahlen (gemäß interner Arbeitsanweisung);
- Keine Weitergabe von Passwörtern an Dritte (verpflichtend geregelt durch Arbeitsanweisung).

Berechtigungsmanagement:

- Die Vergabe von Zugangsrechten erfolgt rollenbasiert nach dem Prinzip der minimalen Rechtevergabe;
- Die Gültigkeit bestehender Berechtigungen wird regelmäßig überprüft;
- Beim Ausscheiden von Mitarbeitenden werden deren Zugänge umgehend deaktiviert.

SoftBCom Berlin GmbH
Schiffbauerdamm 19,
10117 Berlin
030 51302118
www.softbcom.com

Zugriffskontrolle

Es ist ein Berechtigungskonzept erstellt worden für:

- die Verwaltung der Zugriffsrechte durch Systemadministrator.
- Zuordnung der Zugriffsberechtigungen hinsichtlich personenbezogener Daten
- Zugriffsberechtigungen sind nach Aufgabenbereich und Anforderungen angelegt.
- Es gibt differenzierte Berechtigungen für Lesen, Verändern oder Löschen von Daten.
- Nicht mehr benötigte Datenträger oder Dokumente werden datenschutzgerecht entsorgt.

Weitergabekontrolle

Ein Zugriff auf die personenbezogenen Daten des Auftraggebers oder deren Weitergabe an Dritte darf nur von Fall zu Fall nach schriftlicher Zustimmung des Auftraggebers erfolgen.

- Die Datenempfänger, der Transport- / Übermittlungsweg, die zur Übermittlung von Daten befugten Personen und die zu übermittelnden Daten sind in der IT-Dokumentation
- Müssen personenbezogene Daten über einen nicht gesicherten Übertragungsweg weitergegeben werden (E-Mail) erfolgt die Übertragung als verschlüsseltes Dokument.

SoftBCom Berlin GmbH
Schiffbauerdamm 19,
10117 Berlin
030 51302118
www.softbcom.com

Eingabekontrolle

Die Zugriffsberechtigungen wurden schriftlich erteilt und dokumentiert.

Die Protokollierung der Eingabe, Veränderungen oder Löschung personenbezogener Daten erfolgt nur bei eigenen Daten des Auftragnehmers. Im Bereich des Office der SoftBCom Berlin GmbH findet dabei keine Protokollierung bezogen auf die Auftragsdatenverarbeitung statt. Personenbezogene Daten des Auftraggebers werden außerhalb des Zielsystems des Auftraggebers eingegeben, verändert oder gelöscht nur mit schriftlicher Zustimmung des Auftraggebers.

Auftragskontrolle

Die Einhaltung von Datensicherheitsbestimmungen wird durch den Auftragnehmer kontrolliert und der Auftraggeber wird Informiert, wenn Verstöße vorliegen oder der Verdacht besteht, dass die Datensicherheitsvorgaben des Auftraggebers unzureichend sind.

- Alle Mitarbeiter des Auftragnehmers wurden auf das Datengeheimnis (§5 BDSG) verpflichtet.
- Alle Mitarbeiter wurden im Datenschutz geschult.

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle stellt sicher, dass personenbezogene Daten bei Bedarf zuverlässig und zeitnah verfügbar sind, auch bei technischen Zwischenfällen oder außergewöhnlichen Ereignissen. Folgende Maßnahmen wurden durch die SoftBCom Berlin GmbH implementiert:

- Regelmäßige Datensicherungen (Backups) auf redundanten Systemen;
- Einsatz hochverfügbarer Cloud-Infrastrukturen mit Ausfallsicherheit;
- Einsatz von Monitoring-Tools zur Echtzeitüberwachung kritischer Systeme;
- Dokumentierte Notfallpläne zur Wiederherstellung von Daten und Systemen (Disaster Recovery Plan);
- Zugriff auf Daten ist nur über verschlüsselte Verbindungen möglich (z. B. HTTPS, VPN);
- Es existiert ein formalisiertes Freigabeverfahren für neue Datenverarbeitungsverfahren sowie bei wesentlichen Änderungen bestehender Prozesse. Dabei werden datenschutzrechtliche Anforderungen vor Einführung geprüft und dokumentiert.

Speicherort und Datenverarbeitung:

- Personenbezogene Daten des Auftraggebers werden grundsätzlich in dem geografischen Raum verarbeitet und gespeichert, der vertraglich oder produktbezogen vorgesehen ist:
    - Für Kunden mit Sitz in Deutschland: ausschließlich in Deutschland (z. B. auf Servern der Hetzner Online GmbH).
    - Für Kunden aus anderen EU-Mitgliedstaaten: innerhalb der Europäischen Union.
    - Für Kunden aus Drittstaaten: in der jeweils vertraglich definierten Region (z. B. EU-Rechenzentrum), sofern technisch verfügbar.
- Eine Übertragung personenbezogener Daten außerhalb dieses definierten Raums findet **nicht** statt. Soweit aus technischen oder funktionalen Gründen (z. B. zur Nutzung externer KI-Dienste) eine Verarbeitung außerhalb dieses Raums notwendig ist, werden die betreffenden Daten **zuvor vollständig**

anonymisiert, sodass kein Personenbezug im Sinne der DS-GVO mehr besteht.

Nutzung externer Systeme:

- Sofern im Rahmen der Dienstleistung Drittanbietersysteme (z. B. KI-gestützte Tools wie ChatGPT) zum Einsatz kommen, werden ausschließlich anonymisierte oder aggregierte Daten verwendet, sodass kein Personenbezug mehr besteht.
- Eine Übermittlung personenbezogener Daten an solche Drittanbieter findet nicht statt.

Trennungsgebot

Die bei SoftBCom ergriffenen Maßnahmen zur Kontrolle der Trennung sind: softwaremäßiger Ausschluss im Sinne einer Mandantentrennung, Trennung von Test- und Routineprogrammen, Trennung durch Zugriffsregelungen und Dateitrennung. So müssen beispielsweise alle Produktivsysteme getrennt von den Entwicklungs- und Testsystemen betrieben werden.

- Technisch wird dies durch die Segmentierung von Netzwerken mit aktivierten Firewall-Regeln realisiert.
- Produktionsdaten dürfen nicht als Kopie für Testzwecke verwendet werden.
- Testdaten dürfen nicht in einer Produktionsumgebung verwendet werden.
- Details sind in den internen Sicherheitsrichtlinien für den sicheren Betrieb geregelt.

SoftBCom Berlin GmbH
Schiffbauerdamm 19,
10117 Berlin
030 51302118
www.softbcom.com

Berlin 26.05.2025

Ort, Datum Unterschrift der verantwortlichen Stelle