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

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Inkrafttreten: 21. April 2026

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

Zutrittskontrolle

Zur Sicherung des physischen Zugangs zu den Büroräumen von SoftBCom gelten folgende Maßnahmen:

- Dritte dürfen sich nur in Begleitung eines SoftBCom-Mitarbeiters in den Bürobereichen aufhalten.
- Berechtigte Personen für Serverräume werden gesondert bestimmt.
- Der Zugang zu abgeschlossenen Bereichen wird über eine Schlüsselregelung verwaltet; Schlüssel werden nur an berechtigte Personen ausgegeben.
- Die Räumlichkeiten sind durch gesicherte Eingangstüren mit codierten Schlössern geschützt, die nur an autorisierte Mitarbeiter ausgegeben werden.

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

Zugangskontrolle

Die Zugangskontrolle dient dazu, unbefugten Personen den Zugang zu IT-Systemen und Datenverarbeitungseinrichtungen zu verwehren. Bei der SoftBCom Berlin GmbH wurden hierzu folgende Maßnahmen umgesetzt:

Benutzerauthentifizierung:

- Benutzer werden gegenüber dem Datenverarbeitungssystem durch eine individuelle Benutzerkennung und ein Passwort identifiziert;
- Bildschirmarbeitsplätze werden nach 5 Minuten Inaktivität automatisch gesperrt (Passwortschutz des Bildschirmschoners);
- Das interne Netzwerk am Bürostandort ist durch eine Hardware-Firewall gegen externen Zugriff geschützt.

Passwortrichtlinien:

- Persönliches, vom Benutzer erstelltes Passwort;
- mindestens 8 Zeichen, einschließlich Sonderzeichen und Zahlen (gemäß interner Arbeitsanweisung);
- keine Weitergabe von Passwörtern an Dritte (geregelt durch verbindliche Arbeitsanweisungen).

Berechtigungsmanagement:

- Zugriffsrechte werden rollenbasiert nach dem Prinzip der minimalen Rechtevergabe vergeben;
- die Gültigkeit bestehender Berechtigungen wird regelmäßig überprüft;
- beim Ausscheiden von Mitarbeitern werden deren Zugänge unverzüglich deaktiviert.

Zugriffskontrolle

Für die Zugriffskontrolle besteht eine formalisierte Richtlinie für:

- die Verwaltung von Zugriffsrechten durch Systemadministratoren;
- die Vergabe von Berechtigungen zur Verarbeitung personenbezogener Daten;
- die Einrichtung von Zugriffsberechtigungen entsprechend Aufgabenbereich und Erfordernissen;
- differenzierte Rechte zum Lesen, Ändern oder Löschen von Daten;
- die datenschutzkonforme Entsorgung nicht mehr benötigter Datenträger oder Dokumente.

Weitergabekontrolle

Der Zugriff auf personenbezogene Daten durch Dritte oder deren Übermittlung an Dritte erfolgt nur, soweit dies für die Erbringung der vereinbarten Leistung erforderlich ist und auf Grundlage der anwendbaren Vertragsdokumentation, einschließlich der Auftragsverarbeitungsvereinbarung (DPA), der vereinbarten Servicekonfiguration und der aktuellen Liste zugelassener Subprozessoren oder Dienstleister.
Für traditionelle SoftBCom-Produkte (Contact Center, Service Desk, Managed Outbound, WFM) bleibt eine solche Übermittlung auf das für die Erbringung der vereinbarten Leistung erforderliche Maß beschränkt und unterliegt den in diesem Dokument beschriebenen strengen regionalen und Vertraulichkeitsanforderungen.

- Empfänger, Übermittlungswege, berechtigtes Personal und Kategorien der übermittelten Daten werden dokumentiert.
- Bei Übermittlungen über ungesicherte Kanäle (z. B. E-Mail) wird Verschlüsselung eingesetzt.

Eingabekontrolle

Die Vergabe von Zugriffsberechtigungen wird dokumentiert.

Die Eingabe, Änderung und Löschung personenbezogener Daten ist auf autorisiertes Personal beschränkt, das im Rahmen seiner zugewiesenen Verantwortlichkeiten handelt.
Soweit technisch machbar und angemessen, werden relevante Verarbeitungsvorgänge protokolliert, um Nachvollziehbarkeit und Rechenschaftspflicht zu unterstützen.
Eine Verarbeitung personenbezogener Daten von Kunden außerhalb des Zielsystems des Kunden erfolgt nur, soweit dies für die vereinbarte Leistung erforderlich ist und im Einklang mit der anwendbaren Vertragsdokumentation, Servicekonfiguration und den Datenschutzanforderungen steht.

Auftragskontrolle

Die Einhaltung der Vorschriften zur Datensicherheit wird vom Auftragnehmer überwacht, und der Kunde wird informiert, wenn Verstöße vorliegen oder der Verdacht besteht, dass die Datensicherheitsanforderungen des Kunden unzureichend sind.

- Alle Mitarbeiter des Auftragnehmers sind zur Vertraulichkeit verpflichtet und in den anwendbaren Datenschutzpflichten unterwiesen.
- Alle Mitarbeiter wurden im Datenschutz geschult.

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle stellt sicher, dass personenbezogene Daten auch im Falle technischer Störungen oder außergewöhnlicher Ereignisse zuverlässig und zeitnah verfügbar sind. Bei der SoftBCom Berlin GmbH wurden hierzu folgende Maßnahmen umgesetzt:

- regelmäßige Datensicherungen 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);
- der Zugriff auf Daten ist nur über verschlüsselte Verbindungen möglich (z. B. HTTPS, VPN);
- es besteht ein formalisiertes Freigabeverfahren für neue Datenverarbeitungsverfahren und wesentliche Änderungen bestehender Prozesse. Datenschutzanforderungen werden vor der Einführung geprüft und dokumentiert.

Datenstandort und Verarbeitung

- Die personenbezogenen Daten des Kunden werden in dem im Vertrag oder Produkt festgelegten geografischen Bereich verarbeitet und gespeichert.
- Für traditionelle SoftBCom-Produkte, einschließlich SoftBCom Contact Center, SoftBCom Service Desk, SoftBCom Managed Outbound und SoftBCom WFM, werden personenbezogene Daten ausschließlich innerhalb des vereinbarten geografischen Bereichs verarbeitet und gespeichert, sofern in der anwendbaren Vertragsdokumentation nicht ausdrücklich etwas anderes vereinbart ist.
- Für Kunden mit Sitz in Deutschland: ausschließlich in Deutschland (z. B. auf Servern der Hetzner Online GmbH), sofern nichts anderes vereinbart ist.
- Für Kunden aus anderen EU-Mitgliedstaaten: ausschließlich innerhalb der Europäischen Union, sofern nichts anderes vereinbart ist.
- Für Kunden aus Drittländern: in der vertraglich festgelegten Region (z. B. EU-Rechenzentrum), soweit technisch verfügbar und sofern nichts anderes vereinbart ist.

- Für AI-spezifische SoftBCom-Produkte, einschließlich QAWacht und SoftBCom AI Agents, werden personenbezogene Daten primär in dem im Vertrag, in der Produktkonfiguration oder in der anwendbaren Service-Dokumentation festgelegten geografischen Bereich verarbeitet und gespeichert. Soweit technisch machbar und wirtschaftlich vertretbar, bemüht sich SoftBCom nach besten Kräften um die Nutzung von Hosting-Umgebungen, Subprozessoren und regionalen Endpunkten innerhalb dieser Region.
- Für solche AI-spezifischen Produkte garantiert SoftBCom nicht, dass alle Verarbeitungsstufen ausschließlich innerhalb der vereinbarten Primärregion stattfinden, insbesondere dann nicht, wenn aktivierte Funktionalitäten externe Anbieter, verteilte Infrastruktur oder Subprozessoren einbeziehen.
- Soweit die Verarbeitung Anbieter oder Infrastruktur außerhalb der vereinbarten Primärregion oder außerhalb der EU/des EWR umfasst, wird die jeweilige Verarbeitungskette durch angemessene vertragliche, technische und organisatorische Schutzmaßnahmen abgesichert, einschließlich Data Processing Agreements (DPAs), Standardvertragsklauseln (SCCs) und, soweit anwendbar, Maßnahmen wie Anonymisierung, Pseudonymisierung, Minimierung und anderer produktspezifischer Schutzmechanismen.

Einsatz von Drittsystemen

- Wenn Drittsysteme (z. B. AI-gestützte Tools, sprachbezogene Technologien oder damit verbundene Infrastrukturdienste) als Teil des Services eingesetzt werden, wendet SoftBCom den für das jeweilige Produkt geltenden Schutzansatz an.
- Für traditionelle SoftBCom-Produkte (Contact Center, Service Desk, Managed Outbound, WFM) und sofern nichts anderes festgelegt ist, werden für eine solche externe Verarbeitung nur anonymisierte oder aggregierte Daten

verwendet, und es findet keine Übermittlung personenbezogener Daten an solche Drittanbieter statt.

- Für AI-gestützte Services, einschließlich QAWacht und SoftBCom AI Agents, ist der jeweils geltende produktspezifische Schutzansatz in der einschlägigen Service-Dokumentation festgelegt. Je nach Service und Konfiguration kann dies Anonymisierung, Pseudonymisierung, Fragmentierung, Minimierung, kontextuelle Begrenzung und die Nutzung regionaler Endpunkte, soweit verfügbar, umfassen.
- Soweit externe Anbieter beteiligt sind, werden nur die für die jeweilige Funktion erforderlichen Daten offengelegt, und die jeweilige Verarbeitungskette unterliegt angemessenen vertraglichen, technischen und organisatorischen Schutzmaßnahmen.

Trennungsgebot

Die bei SoftBCom umgesetzten Maßnahmen zur Sicherstellung der Trennung sind: softwareseitige Trennung im Sinne der Mandantentrennung, Trennung von Test- und Produktivprogrammen, Trennung durch Zugriffsregelungen sowie Dateitrennung. So müssen beispielsweise alle Produktivsysteme getrennt von Entwicklungs- und Testsystemen betrieben werden.

- Technisch wird dies durch segmentierte Netzwerke mit aktivierten Firewall-Regeln umgesetzt.
- Produktivdaten dürfen nicht als Kopie für Testzwecke verwendet werden.
- Testdaten dürfen nicht in einer Produktivumgebung verwendet werden.
- Einzelheiten sind in den internen Sicherheitsrichtlinien für den sicheren Betrieb geregelt.