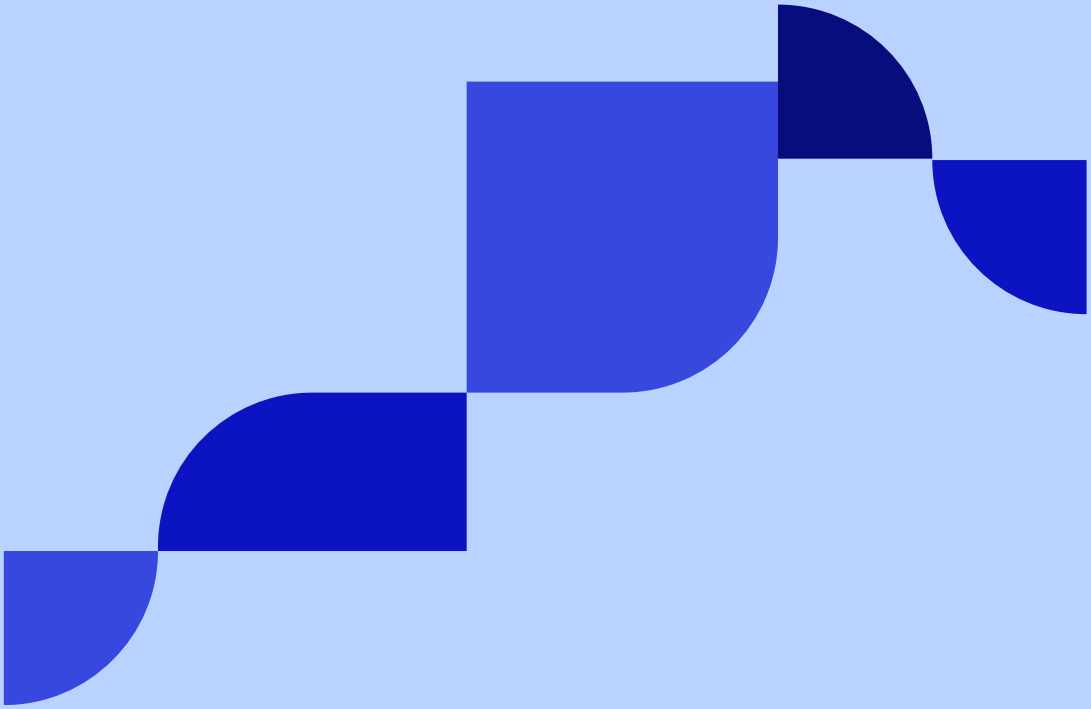
zvoove
Germany

06.2025

TOM Auskunft



Auskunft zu den technischen und organisatorischen Maßnahmen der zvoove Software Germany GmbH im Rahmen der Auftragsverarbeitung gem. Art 28 DSGVO.

Die zvoove Software Germany GmbH wird regelmäßig als **Auftragsverarbeiter i.S.d. Art 28 DSGVO** für ihre Kunden tätig. Die DSGVO verlangt von unseren Kunden insoweit, den Auftragsverarbeiter mit Bedacht auszuwählen und während der Vertragslaufzeit die Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen (kurz: TOM) beim Auftragsverarbeiter zu kontrollieren.

Um für zvoove-Kunden eine möglichst effektive Kontrolle zu ermöglichen, stellen wir dieses Dokument zur Verfügung, welches die jeweils aktuellen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der uns anvertrauten Daten zusammenfasst und weitere Informationen für die datenschutzrechtliche Bewertung der zvoove-Leistungen enthält.

Grundsätzlich gilt, dass zvoove natürlich dauerhaft an die mit den Kunden geschlossenen Auftragsverarbeitungs- verträge und in dessen Anlage definierten TOM gebunden ist; d.h. es findet während der Vertragsdauer keine Änderung in den technischen und organisatorischen Maßnahmen statt, die die vereinbarten Sicherungsstandards unterschreiten, ohne hierfür vorher das ausdrückliche Einverständnis des Kunden einzuholen. Die Einhaltung der vertraglich definierten Maßnahmen ist somit dauerhaft gewährleistet.

Stand: 06/2025

1. Auftragsverarbeiter i.S.d. Art 28 DSGVO

zvoove Software Germany GmbH,
von-Humboldt-Str.2, D-49835 Wietmarschen-Lohne

2. Datenschutzbeauftragter

Rechtsanwalt Dr. Thomas
Balzer bpc GmbH
Einigkeitsstraße 9, 45133 Essen

3. Allgemeine Informationen zur Datenschutz-Organisation

a. Wie werden zvoove-Mitarbeiter mit den Vorschriften zum Datenschutz und zur Datensicherheit vertraut gemacht?

zvoove-Mitarbeiter erhalten beim Eintritt in das Unternehmen eine ausführliche Unterweisung zum Thema Datenschutz, Datensicherheit sowie Wahrung von Fernmeldegeheimnis, Geschäftsgeheimnis usw.. Gleichzeitig verpflichten sie sich schriftlich/vertraglich zur Einhaltung der entsprechenden gesetzlichen Regelungen. Daneben bestehen ausführliche Richtlinien und Arbeitsanweisungen für Mitarbeiter, die den gesetzes- und vertragskonformen Umgang mit Kundendaten regeln. Das Team „IT-Sicherheit/Datenschutz“ stellt durch regelmäßige Schulungen für Mitarbeitereine permanente Sensibilität der Mitarbeiter im Umgang mit personenbezogenen Daten sicher. Dieses Team steht den Mitarbeitern jederzeit auch zur Klärung von alltäglichen Einzelfallfragen zur Verfügung.

b. Gibt es angemessene schriftliche Regeln und Arbeitsanweisungen zum Datenschutz und zur Datensicherheit?

Es bestehen ausführliche Richtlinien und Arbeitsanweisungen für Mitarbeiter, die den gesetzes- und vertragskonformen Umgang mit Kundendaten und die Einhaltung der Maßnahmen zur Gewährleistung der Datensicherheit regeln.

c. Existiert ein Verzeichnis der Verarbeitungstätigkeiten i.S.d. Art 30 (1) DSGVO.

Ja. Dieses Verzeichnis wird jedoch nach den Vorgaben der DSGVO nur intern bzw. zur etwaigen Vorlagen gegenüber Datenschutzaufsichtsbehörden geführt und nicht allgemein zugänglich gemacht.

d. Gab es in den vergangenen 6 Monaten im Rahmen der Auftragsverarbeitung Beschwerden oder Probleme mit Betroffenen?

Nein.

e. Haben in den vergangenen 12 Monaten Prüfungen, Kontrollen oder Beanstandungen durch Datenschutz-Aufsichtsbehörden stattgefunden?

Nein.

f. Wird die Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen (TOM) regelmäßig überprüft?

Ja. Die die mit zvoove-Kunden vertraglich vereinbarten TOM von unserem externen Datenschutz-beauftragten in regelmäßigen Abständen auditiert und die Prüfung dokumentiert. Der aktuelle Bericht vom 03.06.2025 bestätigt die Durchführung/Einhaltung der im aktuellen AV-Vertrag (Anlage TOM) vereinbarten Maßnahmen (s. auch Ziff. 4. ff. dieses Dokuments).

g. Werden im Rahmen der Auftragsverarbeitung für den Kunden Subunternehmer eingesetzt und welche sind dies?

Subunternehmer werden in Asbtimmung mit dem Kunden in die unmittelbare Auftragsverarbeitung für den Kunden eingebunden. Der ausdrückliche Hinweis auf den Einsatz eines Subunternehmers erfolgt in der Regel schon im Rahmen des Leistungsvertrages innerhalb der dort definierten Produktbausteine; die Liste der eingesetzten Subunternehmer ist permanent im Internet unter www.zvoove.com/privacy abrufbar.

h. Bestehen mit allen Subunternehmern Verträge i.S.d. Art 28 (4) DSGVO.

Ja.

4. Technische und organisatorische Maßnahmen

Aktuell unterhält die zvoove Software Germany GmbH am Standort in 49835 Wietmarschen-Lohne folgende technischen und organisatorischen Maßnahmen i.S.d. Art 32 DSGVO zur Gewährleistung eines angemessenen Schutzniveaus im Rahmen der Auftragsverarbeitung für Vertragskunden:

Allgemeine Organisation

- Benennung eines (Konzern-)Datenschutzbeauftragten
- Datenschutz-Management (Richtlinien, Betriebsvereinbarungen, Verfahrensanweisungen, etc.)
- Verpflichtung der Beschäftigten auf Vertraulichkeit/Datengeheimnis, Wahrung Fernmeldegeheimnis,
  Wahrung von Geschäftsgeheimnissen
- Verpflichtung von externen Dienstleistern auf strenge Vertraulichkeit, sofern es sich nicht um Auftragsverarbeiter handelt
- Auftragsverarbeitungsverträge gem. Art 28 mit externen Auftragsverarbeitern.
- Regelmäßige Auditierung der technischen und organisatorischen Maßnahmen zum Datenschutz durch unabhängige Instanz (externer Datenschutzbeauftragter)

Verschlüsselung / Pseudonymisierung

- Bereitstellung von SaaS-Lösungen über verschlüsselte Verbindungen (HTTPS/TLS)
- Verschlüsselung von mobilen Datenträgern
- Pseudonymisierung personenbezogener Kunden-Daten, wenn keine Legitimation für Speicherung von Klardaten mehr vorliegt.

Vertraulichkeit

Zutrittskontrolle + Physikalische Sicherheit

- Einfriedung/Einzäunung des Grundstücks, Toranlagen
- Einbruchmeldeanlage/Alarmanlage, zusätzlich Wachdienst außerhalb Geschäftszeiten
- Tragepflicht von Berechtigungsausweisen
- Zu- und Ausgänge des Gebäudes sind von außen nicht zu öffnen
- Sicherung der Fenster, Kellerfenster, Lichtschächte, besondere Sicherung der Türen
- Zentraler Empfangsbereich / Personenkontrolle
- Dokumentiertes Zutrittskontrollkonzept mit einer Festlegung und Dokumentation der berechtigten Personen, elektronisches Zutrittskontrollsystem für die Gebäude
- Kartendokumentation, Prozess zur Aufhebung nicht mehr benötigter Zutrittsrechte
- Die Büroräume sind gesichert und der Zugang zu den Büros auf Mitarbeiter von zvoove sowie autorisierte Reinigungsdienste beschränkt. Mitarbeiter und Reinigungsdienste erhalten Zugangsmedien (wie Schlüssel und Key Card)

Zusätzliche Sicherungsmaßnahmen der besonders sensiblen Räume (RZ-/Serverraum, TK-Anlage, Verteilerräume, Archive, etc.):

- Zu- und Ausgänge der besonders sensiblen Räume sind von außen nur für speziell berechtigte Mitarbeiter zu öffnen
- Besondere Sicherung der Türen
- Closed-Shop-Betrieb
- Dokumentiertes Zutrittskontrollkonzept, Karten-/Schlüsseldokumentation
- Protokollierung des Zutritts zu einem besonders sensiblen Raum
- Beaufsichtigte Wartung
- Reinigung RZ-/Serverraum durch Mitarbeiter der IT-Abteilung

Authentifizierung / Berechtigung

- Identifikation und Authentifikation von Benutzern (User-ID und Passwort etc.)
- Rollenbasierte Berechtigungen wie Kategorien von Rollen und Rechte der Rollen
- Prozess zur Aufhebung nicht mehr benötigter Rollen und Rechte
- Passwortregeln, automatisierte Kontrolle der Passwortregeln
- Vorläufig vergebene Passwörter werden unverzüglich durch sichere Individualpasswörter ersetzt
- Automatische Kontrolle der unverzüglichen Vergabe von Individualpasswörtern
- Sperrung bei wiederholter Fehleingabe von Passwörtern, Freigabe nur durch Administrator
- Firewall + regelmäßige Updates d. Firewall
- Anti-Virus-Software + regelmäßige Updates d. Anti-Virus-Software
- Einsatz von Intrusion-Detection-Systemen
- Sicherheitseinstellungen der Browser werden gezielt angewendet
- Sicherheitseinstellungen der Browser sind für die Nutzer nicht veränderbar
- Regelmäßiges automatisches Einspielen von Sicherheitspatches und/oder -updates bei Browsern
- Protokollierung von Internetnutzung
- Trennung von Firmennetz und Gäste-WLAN
- Sicherheitsmaßnahmen WLAN (Standardeinstellungen, Standardbenutzernamen und Standard-passwörter durch sichere individuelle Einstellungen ersetzt, Verschlüsselungsverfahren etc.)
- Sicherungsmaßnahmen bei Zugang von extern zum Firmennetz (Virtual Private Network (VPN) etc.)
- Richtlinie über den sicheren Einsatz von mobilen Endgeräten

Zusätzliche Sicherungsmaßnahmen bei SaaS Applikationen in Public Cloud

- Analog zum Hosting ist der Zugriff auf Produktionsdatenbanken nur einem sehr eingeschränkten Administratorenkreis zugänglich, zusätzlich werden erweiterte Sicherheitsmaßnahmen über Automatisierung des Cloud-Anbieters genutzt und mittels 4-Augen Prinzip bzw. nur mit Zustimmung der Kunden eingestellt.
- Zwei-Faktor Authentifizierung für den Betrieb-/Administration-/Support der SaaS Anwendungen und deren berechtigter Benutzer.
- Für den 1st/2nd/3rd Level Supportzugriff auf alle Daten innerhalb einer Kundeninstanz muss die explizite Freigabe durch den Kunden für den Zugriff erfolgen.
- Administratorenrollen mit erweiterten Berechtigungen/Rollen werden ausschließlich an den minimal notwendigen Kreis von zvoove Mitarbeitern vergeben.

Integrität

- Protokollierung der Einrichtung und des Betriebes von IT-Systemen
- Protokollierung von Systemänderungen (Dokumentation von Versionsänderungen oder Änderungen der technischen Umgebung des IT-Systems, Änderungen der Dateiorganisation oder des Dateiverwaltungssystems etc.)
- Protokollierung von Eingaben und Veränderungen (unbefugte und abgewiesene Zugriffsversuche, wiederholte Eingabe von fehlerhaften Passwörtern zu einem Login, unbefugtes Einloggen und Überschreiten von Befugnissen, Benutzung von Admin-Accounts, Warnungen über unbefugtes Eindringen etc.)
- Systemüberwachung (Systemstart und -stopp, Anschluss und Entfernung von Ein- und Ausgabegeräten, Systemfehler etc.)
- Protokollierung von Verbindungsdaten
- Protokollierung der Entfernung von Datenträgern
- Protokollierung des Exports, Downloads und Versands von vertraulichen Dokumenten und Daten
- Gewährleistung der Sicherheit von Protokolldateien (Eingeschränkter Zugriff nur für Mitarbeiter der IT-Abteilung etc.)
- Regelmäßige manuelle Auswertung der Protokolle auf Normabweichungen, Sicherheitsverletzungen und Angriffe

Verfügbarkeit / Belastbarkeit der internen Systeme

- Ausfallschutz durch gespiegelte Plattenlaufwerke, RAID-System etc.
- Automatisierte Protokollierung der Entfernung von Datenträgern und Auswertung/Prüfung der Protokolle
- Backup-Konzept
- Regelmäßige automatisierte Datensicherungen
- Sichere Übertragung von Datensicherungen
- Überprüfung der Sicherungsdaten auf Vollständigkeit und Lesbarkeit
- Sichere Lagerung von Datensicherungen (anderer Brandabschnitt etc.)
- Unterbrechungsfreie Stromversorgung
- Regelmäßige Tests der unterbrechungsfreien Stromversorgung nach Herstellervorschrift auf Funktionsfähigkeit und Dokumentierung der Tests
- Klimaanlage mit Überwachung der Temperatur
- Rauchmeldeanlage (mit Alarmierung Wachdienst)
- Wassermelder
- Brandschutzkonzept
- Feuerlöscher mit geeignetem Löschmittel vorhanden
- Brandschutztüren
- Administratorenpasswort/Notfallpassworte sicher hinterlegt
- Notfallarbeitsplätze
- Dokumentation der Netztopologie

Zusätzliche Sicherungsmaßnahmen bei SaaS Applikationen in Public Cloud

- Rücksicherung der Daten (auch im Disaster Recovery Fall) durch Point-in-Time Recovery mit Granularität von 30min
- Pläne für verschiedene Szenarien sowie regelmäßige protokollierte Recovery Tests (Daten/Applikation/Infrastruktur)
- Nutzung der Reports und Logs des Cloud-Anbieters

Wiederherstellung nach physischem/technischem Zwischenfall

- Backup-Konzept, Notfallhandbuch, Alarmierungsplan
- Regelmäßige automatisierte Datensicherungen
- Sichere Übertragung von Datensicherungen
- Überprüfung der Sicherungsdaten auf Vollständigkeit und Lesbarkeit
- Sichere Lagerung von Datensicherungen (anderer Brandabschnitt etc.)

Regelmäßige Überprüfung, Bewertung und Evaluation der TOM

Regelmäßige Auditierung der technischen und organisatorischen Maßnahmen zum Datenschutz durch unabhängige Instanz (externer Datenschutzbeauftragter).

5. Home-Office

zvoove-Mitarbeiter, die Ihre Tätigkeit ganz oder teilweise von zuhause aus erbringen (Home-Office) verpflichten sich schriftlich zur Einhaltung strenger Auflagen im Umgang mit personenbezogenen Daten. Die im Home-Office eingesetzte Hardware wird den Mitarbeitern ausnahmslos von zvoove zur Verfügung gestellt und administriert. zvoove behält sich gegenüber Mitarbeitern im Home-Office das Recht vor, jederzeit die Einhaltung der Home-Office-Richtlinie vor Ort persönlich zu kontrollieren.