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: 08/2023

Inhaltsverzeichnis

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

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

2. Datenschutzbeauftragter (ab 01.01.2023)

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. Jährlich werden die mit zvoove-Kunden vertraglich vereinbarten TOM von unserem externen Datenschutzbeauftragten auditiert und hierüber ein schriftlicher Bericht gefertigt. Der aktuelle Bericht vom 28.08.2023 bestätigt die Durchführung/Einhaltung der im AV-Vertrag (Anlage TOM) vereinbarten Maßnahmen (s. auch Ziff. 4. ff. dieses Dokuments).

g. Werden personenbezogene Daten von zvoove-Kunden im Rahmen des Auftragsverarbeitung ins außereuropäisches Ausland transferiert?

Die Datenverarbeitung durch zvoove erfolgt ausschließlich innerhalb der EU.

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

Subunternehmer werden nur 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.

i. 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:

Organisationskontrolle

- Datenschutz-Management (Richtlinien, Betriebsvereinbarungen, Verfahrensanweisungen, etc.)
- Verpflichtung der Beschäftigten zur Vertraulichkeit
- Verpflichtung der Beschäftigten auf das Fernmeldegeheimnis
- Verpflichtung von externen Dienstleistern auf das Datengeheimnis, sofern es sich nicht um Auftragsverarbeiter handelt
- Benennung eines Datenschutzbeauftragten
- Regelmäßige Auditierung der technischen und organisatorischen Maßnahmen zum Datenschutz durch unabhängige Instanz (externer Datenschutzbeauftragter)

Zutrittskontrolle

Sicherungsmaßnahmen des Gebäudes:

- Einfriedung/Einzäunung des Grundstücks
- Toranlage
- Einbruchmeldeanlage/Alarmanlage
- Wachdiens
- Tragepflicht von Berechtigungsausweise
- Zu- und Ausgänge des Gebäudes sind von außen nicht zu öffnen
- Sicherung der Fenster, Kellerfenster, Lichtschächte
- Besondere Sicherung der Türen
- Zentraler Empfangsbereich mit Personenkontrolle
- Besucherüberwachung (Elektronisches Besuchermanagementsystem, Begleitung durch Mitarbeiter etc.)
- Dokumentiertes Zutrittskontrollkonzept mit einer Festlegung und Dokumentation der berechtigten Personen
- Elektronisches Zutrittskontrollsystem für das Gebäude
- Kartendokumentation
- Sichere Verwahrung von Ersatzkarten / Dongles
- Prozess zur Aufhebung nicht mehr benötigter Zutrittsrechte

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

- Einbruchmeldeanlage/Alarmanlage
- Wachdienst
- Tragepflicht von Berechtigungsausweisen
- Zu- und Ausgänge der besonders sensiblen Räume sind von außen nicht zu öffnen
- Besondere Sicherung der Türen
- Closed-Shop-Betrieb
- Dokumentiertes Zutrittskontrollkonzept mit einer Festlegung und Dokumentation der berechtigten Personen
- Elektronisches Zutrittskontrollsystem für besonders sensible Räume und zusätzlich Sicherheitsschloss
- Karten-/Dongledokumentation
- Schlüssel-/Dongledokumentation
- Sichere Verwahrung von Ersatzkarten/Ersatzschlüsseln
- Prozess zur Aufhebung nicht mehr benötigter Zutrittsrechte
- Protokollierung des Zutritts zu einem besonders sensiblen Raum
- Beaufsichtigte Wartung
- Reinigung RZ-/Serverraum durch Mitarbeiter der IT-Abteilung

Zugangskontrolle (Datenverarbeitungsanlagen auf Netz- und Serverebene)

- Identifikation und Authentifikation von Benutzern (User-ID und Passwort etc.)
- Passwortregeln vorhanden
- 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
- Sperre von Endgeräten beim Verlassen (Bildschirmschoner mit Passwortschutz automatisch nach Zeitablauf)
- Firewall
- Updates für Firewall werden regelmäßig manuell installiert
- Anti-Virus-Software
- Updates für Anti-Virus-Software werden regelmäßig automatisch installiert
- 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 (WPA2 und 3, Standardeinstellungen, Standardbenutzernamen und Standardpasswörter durch sichere individuelle Einstellungen ersetzt, Verschlüsselungsverfahren etc.)
- Sicherungsmaßnahmen bei Zugang von extern zum Firmennetz (Virtual Private Network (VPN) etc.)
- Verschlüsselung von mobilen Datenträgern

Zugriffskontrolle (Datenverarbeitungsanlagen)

- Aktive Netzkomponenten (Switches etc.) sind zugriffssicher untergebracht
- Deaktivierung nicht benötigter Anschlussdosen/elektronischer Zugriffsschutz
- Richtlinie zur sicheren Nutzung mobiler Datenträger
- Verhinderung unzulässiger mobiler Datenträger durch Sperrung der Ports
- Transparenter User-Help-Desk (Explizite Freigabe durch Nutzer, Beendigung der Help-Desk-Sitzung erkennbar etc.)
- Rollenbasierte Berechtigungen wie Kategorien von Rollen und Rechte der Rollen
- Prozess zur Aufhebung nicht mehr benötigter Rollen und Rechte

Weitergabekontrolle

- Sensible Daten/Dokumente werden verschlüsselt übertragen/weitergegeben
- Identifizierung und Authentifizierung der Beteiligten bei der Datenübertragung (Benutzerkennung/Passwort etc.)
- Regelmäßiges automatisches Einspielen von Sicherheitspatches und/oder -updates bei E-Mail-Programmen
- Kein Einsatz von Web-Mail-Angeboten
- Protokollierung des E-Mail-Verkehrs
- Geeignete Sicherungsmaßnahmen für den Transport von Datenträgern (Verschlüsselung etc.)
- Prozess zur sicheren Löschung/Vernichtung von Datenträgern (Protokollierung der Vernichtung etc.)
- Sichere und vertrauliche Sammlung von Datenträgern/Unterlagen vor der Vernichtung
- Einsatz von Aktenvernichtern

Eingabekontrolle

- 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
- Admin-Zugänge sind individualisiert und werden protokolliert

Auftragskontrolle

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich des Datenschutzes)
- Vorherige Prüfung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen
- Abschluss eines Vertrages oder eines anderen Rechtsinstruments nach Art. 28 DSGVO und Einhaltung dieser Regularien
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vertraglich festgelegte Verantwortlichkeiten

Verfügbarkeitskontrolle

- 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 (inklusive Dieselaggregat)

- Regelmäßige Tests der unterbrechungsfreien Stromversorgung nach Herstellervorschrift auf Funktionsfähigkeit und Dokumentierung der Tests
- Redundante Klimaanlage mit Überwachung der Temperatur
- Rauchmeldeanlage (mit Alarmierung Wachdienst)
- Wassermelder
- Brandschutzkonzept
- Feuerlöscher mit geeignetem Löschmittel vorhanden
- Brandschutztüren
- jährliche Brandschutzübungen
- Regelmäßige Überprüfung des räumlichen Umfeldes des RZ/der Serverräume auf eventuelle Risiken
- Administratorenpasswort/Notfallpassworte sicher hinterlegt
- Notfallhandbuch
- Alarmierungsplan
- Notfallarbeitsplätze
- Dokumentation der Netztopologie
- Test- oder Entwicklungsumgebung vorhanden

Trennungskontrolle

- Logische/Physikalische Trennung von verschiedenen speichernden Stellen (Unternehmen)
- Trennung von Test- und Produktionsdaten

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. Vor-Ort-Kontrollen bei Mitarbeitern im Home-Office erfolgen unregelmäßig durch Mitarbeiter der Personalabteilung gemeinsam mit dem QM-Beauftragten des Unternehmens.