Stand: Mai 2018

# Technische und organisatorische Maßnahmen zur IT -Sicherheit- und Datenschutz

Dienstleistung: **SAAS** 'Software as a Service'.

---

**SEVENIT GmbH | Hauptstraße 40 | 77652 Offenburg**

ergreift bei der Erhebung, Verarbeitung und Nutzung personenbezogener Kundendaten die folgenden technischen und organisatorischen Maßnahmen.

## 1. Zutrittskontrolle

---

Der Auftragnehmer gewährleistet durch geeignete Maßnahmen, dass Unbefugten der Zugang zu den Datenverarbeitungsanlagen, auf der die personenbezogenen Daten verarbeitet o der genutzt werden, verwehrt wird. Dies geschieht durch:

- Persönliche Überwachung im Eingangsbereich
- Schlüsselvergabe ausschließlich an autorisierte Personen
- Zutritt zu m Gebäude und allen relevanten Räumen nur für Berechtigte, d.h. die jeweiligen Mitarbeiter, Besucher nur in Begleitung von berechtigten Mitarbeitern.
- Zutritt zum abgeschlossenen EDV-Verteiler und Router/Firewall ist nur für autorisierte Mitarbeiter

## 2. Zugangskontrolle

---

Der Auftragnehmer verhindert durch geeignete Maßnahmen, dass seine Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dies geschieht durch:

- autorisierte Mitarbeiter
- Einsatz einer HW Firewall und entsprechend konfiguriert
- Clientsysteme nur nach passwortgestützter Netzwerk -Authentifizierung nutzbar

## 3. Zugriffskontrolle

Der Auftragnehmer gewährleistet, dass die zur Nutzung seiner Datenverarbeitungssysteme Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten ohne Berechtigung nicht gelesen, kopiert, geändert oder entfernt werden können. Dies geschieht durch:

- Freigabe von Daten nur an berechtigte Personen
- Unterweisung unter Berücksichtigung der individuellen Zugriffsrechte auf personenbezogenen Daten
- Schutz gegen unberechtigte interne und externe Zugriffe durch Firewall bestehen.

## 4. Weitergabekontrolle

Der Auftragnehmer verhindert durch geeignete Maßnahmen, dass bei der Übertragung der personenbezogenen Daten sowie bei Transport von Datenträgern die Daten unbefugt gelesen kopiert, verändert oder gelöscht werden können. Dies geschieht durch:

- Einsatz von aktueller Firewall
- E-Mail Nachrichten bzw. sonstige Informationen werden verschlüsselt versendet
- Einsatz von Verschlüsselungstechnologien für Dokument e. VPN-Technologie (SSL/TLS) zur Datenkommunikation

## 5. Eingabekontrolle

Der Auftragnehmer ergreift geeignete Maßnahmen, um zu gewährleisten, dass überprüft und sichergestellt werden kann, dass keine personenbezogenen Daten in die Datenverarbeitungssysteme zusätzlich eingegeben oder aus diesen endgültig entfernt worden sind. Dies geschieht durch:

- Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles)
- Der Zugriff auf Datenbestände erfolgt anhand Berechtigungen. Das Verfahren gewährleistet, dass keine Datenveränderungen unbemerkt vorgenommen werden können.

## 6. Auftragskontrolle

Der Auftragnehmer sichert durch geeignete Maßnahmen, dass in Fällen der Auftragsdatenverarbeitung personenbezogene Daten im Einklang mit den Weisungen des Auftraggebers verarbeitet werden. Dies geschieht durch:

- Eindeutige Vertragsgestaltung
- Kontrolle der Vertragsausführung
- Klare Anweisungen an den Auftragnehmer hinsichtlich de s Umfangs der Verarbeitung personenbezogener Daten.
- Soweit eine Datenverarbeitung im Auftrag durchgeführt wird, wird der Auftragnehmer vor Aufnahme der Datenverarbeitung nach den Vorschriften der DSGVO auf die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen überprüft. Über jeden Auftrag wird ein Vertrag nach den Vorschriften der Datenschutz-Grundverordnung abgeschlossen. Dies gilt auch für Verträge über Wartungsarbeiten an den Datenverarbeitungssystemen und Softwarepflege je nach Bedarf und sonstige IT Service-Unterstützung, wenn dabei ein Zugriff auf personenbezogenen Daten nicht ausgeschlossen werden kann. Bei der Überprüfung der Auftragnehmer und der Vergabe von Aufträgen im Rahmen einer Datenverarbeitung im Auftrag wird unser Datenschutzbeauftragte hinzugezogen.

## 7. Verfügbarkeitskontrolle

Der Auftragnehmer verhindert durch geeignete Maßnahmen die unbeabsichtigte Zerstörung oder den
Verlust personenbezogener Daten. Dies geschieht durch:

- Im Rahmen der SAAS Dienstleistung ist das Rechenzentrum nach ISO/IEC 27001:2013 zertifiziert
- Feuerlöscher und Virenschutz bestehen

## 8. Trennung der Verarbeitung für verschiedene Zwecke

Der Auftragnehmer gewährleistet durch geeignete Maßnahmen, dass personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, getrennt verarbeitet werden können. Dies geschieht durch:

- Funktionstrennung/Produktions- und Testsystem
- getrennte Verarbeitung zweckgebundener Daten

## 9. Organisationskontrolle

Für die Verarbeitung von Daten im Unternehmen sind Prozesse und Arbeitsabläufe definiert, die Umsetzung und Einhaltung der Prozesse werden kontrolliert.
Unsere Mitarbeiter werden in folgenden Punkten geschult/verpflichtet:

- Grundsätze des Datenschutzes und der IT-Sicherheit
- Pflicht zur Verschwiegenheit über Betriebs- und Geschäftsgeheimnisse
- Ordnungsgemäßer und sorgfältiger Umgang mit Daten, Dateien, Datenträgern und sonstigen Unterlagen
- Bestellung eines externen Datenschutzbeauftragten
- Regelmäßige Kontrolle durch den Datenschutzbeauftragt en
- Die Datenschutzschulungen werden regelmäßig wiederholt, mindestens jedoch alle zwei Jahre.
- SEVENIT GmbH gewährleistet, dass die Leistungserbringung unter Beachtung des Datenschutzrechts erfolgt.