

Anlage 2

Detaillierte Ausführungen zu den technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit im Sinne des Art. 32 DSGVO.

1. Vertraulichkeit

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Das Unternehmen hat zur Sicherstellung der Zutrittskontrolle folgende Maßnahmen ergriffen:

Büro des Auftragnehmers

- Schlüssel mit dokumentierter Schlüsselvergabe für:
 - Eingangstüren
 - Aufbewahrungsschränke
 - Server-Schränke
- Außentüren sind mit einem manuellen und technischen Schließsystem versehen und grundsätzlich verschlossen

Rechenzentrum Keyweb (coveto Installation)

- Verdeckte und standortgetrennte Rechenzentren
- Alarmanlage
- Zutrittskontrollsystem/Schließsystem über Chipkarte
 - Nur berechtigte Mitarbeiter erhalten Zugang
 - Die Vergabe der Zutrittsberechtigung erfolgt uhrzeitabhängig basierend auf den jeweiligen Dienstzeiten der Mitarbeiter
- Zutritt von Dritten nur mit Voranmeldung
- Protokollierung der Besucher
 - Ständige Begleitung von Besuchern durch einen Mitarbeiter des RZ-Betreibers
 - Tragepflicht von Besucherausweisen
- Sorgfältige Auswahl von Reinigungspersonal
- Videoüberwachung

- Überwachung besonderer Gefahrenbereiche wie Eingangsbereich, Standort wichtiger Netzwerkkomponenten
 - Aufzeichnung der Videoüberwachung mit Speicherung für 3 Monate
- Regelmäßige Kontrollgänge

Rechenzentrum Hetzner

- elektronisches Zutrittskontrollsystem mit Protokollierung
- dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren

1.2 Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Das Unternehmen hat zur Sicherstellung der Zugangskontrolle folgende Maßnahmen ergriffen:

Auftragnehmer intern

- Komplexe Kennwörter mit einer ausreichenden Länge pro Benutzer
- Regelmäßige Änderung der Kennwörter
- Einsatz von Zertifikaten statt Kennwörtern, wo möglich und sinnvoll
- Automatische Sperrung bei Inaktivität
- Verschlüsselung von Datenträgern bzw. Daten oder verschlüsselte Übertragung, die unseren Kunden übermittelt werden

Rechenzentrum Keyweb & Hetzner

- Zugang zum Serversystem nur mittels Usernamen und Passwort bzw. SSH Keys
- Änderung des Passworts durch den Auftraggeber nach Beendigung des Auftrags
- Eine Verbindung zum Server zwecks Wartung erfolgt ausschließlich direkt über die lokale Konsole oder über eine verschlüsselte Verbindung, z.B. SSH
- Besucher – und Zugangsprotokollierung

1.3 Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden

können. Das Unternehmen hat zur Sicherstellung der Zugriffskontrolle folgende Maßnahmen ergriffen:

Auftragnehmer intern

- Verschlüsselte Speicherung von Kennwörtern
- Differenzierte Zugriffsrechte pro Mitarbeiter
- Protokollierung der Zugriffe durch den Support

coveto Software

- Erzwingen einer verschlüsselten SSL/TLS Verbindung
- Für jede Maske existiert die Möglichkeit, die Rechte pro Benutzergruppe festzulegen
- Die Zugriffsrechte der Standard-Benutzerguppen (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den typischen aufgabenbedingten und datenschutzrechtlichen Erfordernissen. Es können individuelle Zugriffsrechte vergeben werden.
- Der Zugriff auf die Anwendung (Eingabe, Veränderung und Löschung) wird protokolliert und kann ausgewertet werden.
- In den Enterprise-Tarifen besteht zudem eine Multi-Mandanten-Fähigkeit, bei der auf Datensatz-Ebene der Besitzer festgelegt werden kann
- Dynamische Zeitverzögerung bei Falscheingabe

Rechenzentrum Keyweb

- Verpflichtungserklärung aller Mitarbeiter auf das Datengeheimnis
- Sorgfältige Auswahl der Mitarbeiter durch den RZ-Betreiber
- Zugriff erfolgt nur nach konkreter Beauftragung durch den Auftragnehmer über das Ticketsystem des RZ-Betreibers
- Bearbeitender Mitarbeiter auf Seiten des RZ-Betreibers ist durch eine persönliche Benutzerkennung im Ticketsystem identifizierbar
- Arbeiten erfolgen nur im Rahmen dessen, was zur Lösung des vom Auftragnehmer geschilderten Problems notwendig ist
- Weitergehende Arbeiten erfolgen nur in Abstimmung mit dem Auftragnehmer
- Daten auf Festplatten, welche endgültig aus einem Server entfernt werden, werden umgehend durch Verwendung der Gutmann Löschmethode (35-maliges Überschreiben) dauerhaft und unwiederbringlich entfernt.
- Protokollierung der Datenlöschung

1.4 Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Das Unternehmen hat zur Sicherstellung der Trennungskontrolle folgende Maßnahmen ergriffen:

- Trennung der einzelnen coveto Installationen pro Kunde. Jeder Kunde erhält eine eigene Installation.
- Innerhalb der coveto Software ab den Enterprise-Tarifen zusätzlich Multi-Mandanten-Funktion
- Trennung der coveto Produktions-, Test- und Entwicklungs-Installationen.

1.5 Verschlüsselung und Pseudonymisierung

Verschlüsselung meint einen Vorgang, mit dem eine klar lesbare Information durch ein kryptographisches Verfahren verändert wird und damit nicht mehr klar lesbar ist. Das Unternehmen hat zur Sicherstellung der Verschlüsselung folgende Maßnahmen ergriffen:

- Auftragnehmer intern und coveto Software
 - Verschlüsselte Verbindungen SSH, SSL/TLS

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO): Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. Das Unternehmen hat entsprechend dem Stand der Technik und dem angestrebten Schutzzweck entsprechend folgende Maßnahmen ergriffen:

- Nichtangabe: Bei dieser Methode wird die zu schützende Information vollständig entfernt. Unbefugte Aufhebung der Pseudonymisierung wird durch technische Trennung der Daten (Kein Zugriff auf die personenbezogenen Daten ohne eine entsprechende Freigabe durch den Verantwortlichen) gewährleistet.
- Die Grundsätze der Pseudonymisierung, Anonymisierung, Verschlüsselung und Datenminimierung werden in den für die Mitarbeiter verpflichtenden Datenschutzschulungen erklärt und die Wichtigkeit dieser Maßnahmen erläutert.

2. Integrität, Verfügbarkeit, Belastbarkeit

2.1 Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Das Unternehmen hat zur Sicherstellung der Weitergabekontrolle folgende Maßnahmen ergriffen:

Auftragnehmer intern und coveto Software

- Datenkommunikation unter Einsatz verschlüsselter Verbindungen (SSH, SSL/TLS)
- Protokollierung von Exporten
- Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet
- Datenschutzgerechte Löschung der Daten nach Auftragsbedingung

2.2 Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Das Unternehmen hat zur Sicherstellung der Eingabekontrolle folgende Maßnahmen ergriffen:

coveto Software

- Protokollierung der Erfassung, Veränderung und Löschung von Datensätzen
- Verschiedene Auswertungsmöglichkeiten (kumuliert oder detailliert)
- Die Zugriffsrechte der Standard-Benutzergruppen (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den typischen aufgabenbedingten und datenschutzrechtlichen Erfordernissen. Es können individuelle Zugriffsrechte vergeben werden.

3. Wiederherstellbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Das Unternehmen hat zur Sicherstellung der Verfügbarkeitskontrolle folgende Maßnahmen ergriffen:

Rechenzentrum Keyweb

- Feuerlöschgeräte in den Rechenzentren
 - CO2 Handfeuerlöscher
- Feuer- und Rauchmeldeanlage mit Brandfrüherkennungssystemen an Decke und Boden

- Direkte Aufschaltung zur Feuerwehr
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- Dieselnotstromaggregat
- Generatoren mit einer Spitzenleistung von 500kVA
- Klimaanlage in den Rechenzentren
 - Kühlinfrastruktur ist N+1 redundant
- Alarmmeldung bei unberechtigten Zutritten zu den Rechenzentren
- Spiegelung der Festplatten durch ein RAID Systeme
- Backup aller Daten und Einstellungen. Wird i.d.R. 3 Tage lang aufbewahrt.
- Redundanten Internetverbindung

4. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

4.1 Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Dieser Punkt wird durch die vertraglichen Vereinbarungen zwischen den Parteien, den Zustimmungsvorbehalt des Auftraggebers beim Einsatz von Subunternehmern und die entsprechenden Kontrollrechte des Auftraggebers gewährleistet.

4.2 Zertifizierungen

Rechenzentrum Keyweb: Die Rechenzentren sind vom TÜV-Saarland zertifiziert als TÜV-geprüftes Rechenzentrum hochverfügbar Stufe 2. Die Prüfungen werden in Anlehnung an BSI IT Grundschutz, BITKOM, TIA 942 sowie ISO 27001 und ISO 27002 auf Basis des vorliegenden TÜV Saarland Anforderungskatalog durchgeführt. Die Verifizierung erfolgt regelmäßig und bescheinigt die bauliche und technische Sicherheit sowie die optimale Organisation der Rechenzentren des Auftragnehmers.

Rechenzentrum Hetzner: Die Hetzner Online GmbH ist nach dem internationalen Standard ISO/IEC 27001:2013 zertifiziert.

4.3 Datenschutz-Management

- Etablierung eines Datenschutzmanagementsystems zur Umsetzung der Nachweispflichten der DSGVO

- Schulungen der Beschäftigten zum Datenschutz
- Schriftliche Verpflichtung aller Mitarbeiter zum vertraulichen Umgang mit personenbezogenen Daten
- Regelmäßige Sensibilisierung der Mitarbeiter – mindestens jährlich
- Benennung eines Datenschutzbeauftragten durch den Auftragnehmer

4.4 Datenschutzfreundliche Voreinstellungen

Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

- Arbeitsanweisungen und Schulungen zur Nutzung des Systems
- Differenziertes Berechtigungskonzept
- Definition der Speicherfristen