ANLAGE

Technische und organisatorische Maßnahmen (TOM)

der Convento GmbH im Zusammenhang mit myconvento
gem. Art. 28, 29, 32 DSGVO

myconvento

Anlage: Technische und organisatorische Maßnahmen (TOM)

DER CONVENTO GMBH IM ZUSAMMENHANG MIT MYCONVENTO GEM. ART. 28, 29, 32 DSGVO

Vorbemerkung: Die myloc managed IT AG ist das von der Convento GmbH ausgewählte Rechenzentrum. Ausschließlich hier werden die personenbezogenen Daten ihrer Kunden verarbeitet. myloc ist vom deutschen TÜV nach ISO 27001 zertifiziert, und zwar für alle Bereiche und Funktionen eines Rechenzentrums, und weist dies gegenüber Convento kontinuierlich nach. Auf Wunsch können wir unseren Kunden das ISO-Zertifikat von myloc und deren TOMs zur Verfügung stellen.

Convento speichert die Daten seiner Kunden am Arbeitsplatz des betreuenden Mitarbeiters nur sehr kurzfristig und nur aus besonderem Anlass. So ist vor der Inbetriebnahme von myconvento manchmal eine Vorbereitung der vorhandenen Daten zum Import nötig, für die der Kunde dann einen besonderen Auftrag erteilt.

a) Verwehrung des Zutritts zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zutrittskontrolle): Die Zutrittskontrolle erfolgt bei unserem zertifizierten Rechenzentrum über ein protokolliertes Zutrittssystem mit Schließanlage und Kartenleser. Darüber hinaus ist das Rechenzentrum gegen Einbruch mehrfach gesichert.
Convento hat seinen Serverraum durch ein Sicherheits-Schlüsselsystem gesichert. Ausgabe der Schlüssel nur an wenige autorisierte Mitarbeiter.

b) Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Zugriffskontrolle): Bei der myloc managed IT AG ist die Zugriffskontrolle über die ISO-Zertifizierung geregelt.
Convento bearbeitet Kundendaten - wenn überhaupt - nur auf fest installierten Desktop Rechnern in eigenen Büros. Es erfolgt keine Verarbeitung auf Notebooks oder anderen mobilen Endgeräten. Da das Büro auch mit einem speziellen Schlüsselsystem gesichert ist, ist auch hierüber die Datenträgerkontrolle gewährleistet.

c) Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Zugriffskontrolle): Die Zugriffskontrolle ist durch eine vorhandene Authentifizierung gegeben. Jeder Anwender erhält nur Zugriff auf seine eigenen Daten. Änderungen, Löschungen und das Anlegen von Daten werden protokolliert und die Daten werden verschlüsselt übertragen (TLS 1.3).

d) Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Zugangskontrolle). Die Zugangskontrolle wird durch vorherige Authentifizierung von Username und Passwort mit erweiterten Möglichkeiten zur Passwortrichtlinie sichergestellt.

e) Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugriff haben (Zugriffskontrolle): Das myconvento System verfügt über eine Benutzerverwaltung, in der die Rechte einzelner Benutzer festgelegt werden können. Dazu gehören Rechte wie „Vollzugriff", „Nur lesen" und „Versteckt". Auch ganze Programmbereiche lassen sich für einzelne Anwender sperren.

f) Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle): Convento überträgt Kundendaten nur über einen Up- und Downloadbereich (Up-/Downloadcenter). Der hierfür benötigte Speicherplatz befindet sich bei myloc. Dieser dient einerseits der sicheren Datenübertragung und ermöglicht es andererseits, alle getätigten Datenübertragungen nachzuvollziehen.

g) Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (**Eingabekontrolle**): myconvento protokolliert automatisch und im Hintergrund, welcher Anwender wann welchen Personen- oder Mediendatensatz erfasst, geändert oder gelöscht hat. Diese Protokolle können auf Wunsch dem Kunden-Administrator zur Verfügung gestellt werden.

h) Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (**Transportkontrolle**): Die Verbindung vom Endgerät des Anwenders zum myconvento System wird mit einer SSL-Verschlüsselung über Port 443 aufgebaut und sichergestellt.

i) Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellbarkeit**): Convento überträgt die täglich gesicherten Daten der Kunden auf zwei Standorte. Darüber hinaus wird einmal wöchentlich von der myloc AG eine Offline-Sicherung vorgenommen und an einen separaten Ort verbracht.

j) Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (**Zuverlässigkeit**): Die myLoc AG verfügt über ein Monitoring System, das Hardwarefehler automatisch meldet. Das myconvento Versandsystem protokolliert und meldet Fehler, die während der Erstellung oder Durchführung von Versandaufträgen auftreten.

k) Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**): Innerhalb von myconvento werden die Daten von einem professionellen SQL Datenbankserver verarbeitet und gespeichert. Dieser verfügt unter anderem über Transaktionsmechanismen und andere Methoden der Datenspeicherung, mit denen die Datenintegrität gewährleistet wird.

l) Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**): Zugriff auf Kundendaten erhalten myconvento Mitarbeiter nur dann, wenn dies ausdrücklich vom Kunden gewünscht und initiiert wird. So muss der Kunde beispielsweise den Support-Mitarbeitern erst einen ausdrücklichen Zugang einrichten oder seinen Bildschirm im Online Webinar freischalten, bevor sie die Daten sehen können.

m) Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**): Personenbezogene Daten sind durch die o.g. Mehrfachsicherung in verschiedenen Rechenzentren von myloc vor Zerstörung und Verlust geschützt. Der hohen Verfügbarkeit des Systems dienen darüber hinaus viele Sicherungsmechanismen des professionellen Rechenzentrums.

n) Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (**Trennbarkeit**): Die Trennbarkeit der Daten erfolgt auf dem MS SQL-Server jeweils durch die Einrichtung separater Datenbanken. Auf den Web-Servern wird die Trennung der Daten über eine Verwaltungsdatenbank gewährleistet. Die Daten jedes Kunden sind von denen anderer Kunden und sonstiger Anwender in der Multimandantenumgebung logisch getrennt. Für eine weitergehende physikalische Trennung ist der Betrieb in der sogenannten „Hosted Appliance" möglich.

o) Die Convento GmbH implementiert und praktiziert u.a. folgendes Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen gem. Art. 32 Abs. 1 lit. d): Führende Mitarbeiter von Technik, Entwicklung, Kundenbetreuung und Geschäftsführung treffen sich regelmäßig (i.d.R. 14-tägig) zu einem sogenannten AET-Meeting. Der Datenschutzbeauftragte ist manchmal auch anwesend. Der erste Punkt der Agenda betrifft regelmäßig die Diskussion über aktuelle Vorkommnisse, potenzielle Gefahren, aktuell getätigte oder geplante Investitionen und Maßnahmen zur Stärkung der IT-Sicherheit des Convento Systems. Darüber hinaus geht es um die erwartete oder beobachtete Wirksamkeit von geplanten oder getätigten Investitionen und Maßnahmen. Über Inhalt und Ergebnis der Diskussion wird ein Protokoll angefertigt und archiviert.