Technische und organisatorische Maßnahmen (TOM) zur Datensicherheit (nach Art. 32 DSGVO)

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Maßnahmen sind nur insoweit erforderlich, wie ihr Aufwand und die Implementierungskosten in angemessenem Verhältnis zum angestrebten Schutzzweck steht.

Die Kanzlei Rechtsanwalt Werner Zehentmeier erfüllt diese Vorgabe durch die folgenden Maßnahmen:

A. Vertraulichkeit (Art. 32 Abs. (1) lit. a) DSGVO)

I. Zugangskontrolle

Maßnahmen zur Verhinderung des Zugangs von Unbefugten zu Datenverarbeitungsanlagen, mit denen die Verarbeitung personenbezogener Daten durchgeführt wird:

- Gesicherter Gebäude-Zugang mit Sicherheitsschlösserrn,
- Klingelanlage mit Sekretariatszugriff,
- In Büro-Kernzeiten besetzter Empfang,
- Gebäudeabsicherung durch Alarmanlage,
- Zugangsflur zum Serverraum bleibt auch zu Bürozeiten geschlossen,
- Zugangsflur zu Büroräumen außerhalb der Bürozeiten videoüberwacht,
- Computer mit personenbezogenen Daten in abgeschlossenen Serverschränken,
- Personen mit Zugangsberechtigung/ Schlüssel in Liste geführt,
- Sorgfältig ausgewählte Reinigungsdienste mit Verschwiegenheitsverpflichtungen.

II. Speicherkontrolle

Maßnahmen zur Verhinderung der Kenntnisnahme, der Veränderung oder Löschung von personenbezogenen Daten durch Unbefugte:

- Interner Zugriff auf Arbeitsplatz-Rechner nur nach kennwortgeschützter Anmeldung ,
- Externe Zugriffe auf das Netzwerk (über verschlüsseltes VPN) nur nach kennwortgeschützter Anmeldung mit besonders komplex gebildeten Kennwörtern,
- Zugriff auf Server-Systeme erst nach weiterer kennwortgeschützter Anmeldung,
- Zugriff auf das interne LawFirm System (Verwaltung von Interessenten und Kunden, Auftragsabwicklung, Support) erst nach weiterer kennwortgeschützter Anmeldung,
- Personenbezogene Daten sind ausschließlich auf den Server-Systemen gespeichert, sind also erst nach einer zweistufigen Anmeldung zugänglich.

- Im internen LawFirm System verwaltete Daten sind in einer verschlüsselten Datenbank abgelegt und sind erst nach der dritten Anmeldestufe zugänglich.
- Dokumente werden auf verschlüsselten Datenträgern abgelegt, d.h. gestohlene Datenträger sind für Unbefugte nicht lesbar.
- Sicherungskopien befinden sich auf verschlüsselten Datenträgern.
- Die Systemadministration aller internen Systeme erfolgt durch eine Person zzgl. Vertretung

III. Datenträgerkontrolle

Maßnahmen zur Verhinderung des Zugriffs von Unbefugten auf Datenträger, auf denen personenbezogene Daten gespeichert sind:

- Personenbezogene Daten sind ausschließlich auf den Server-Systemen gespeichert, die sich in abgeschlossenen Serverschränken befinden.
- Betriebssystem und Daten der Server-Systeme werden auf getrennten Datenträgern (Festplatten bzw. Partitionen) gespeichert.
- Datenträger mit personenbezogenen Daten sind verschlüsselt, d.h. gestohlene Datenträger sind für Unbefugte nicht lesbar.
- Zur Datensicherung eingesetzte externe Datenträger sind verschlüsselt und werden extern an einem sicher verschlossenen ausgelagerten Ort aufbewahrt.
- Vernichtete Papierakten-Inhalte mit personenbezogenen Daten werden geschreddert.
- Zur Vernichtung von Akten in größerem Umfang werden zertifizierte Dienstleister beauftragt.

IV. Benutzerkontrolle

Maßnahmen zur Verhinderung der Nutzung von automatisierten Verarbeitungssystemen durch Unbefugte:

- Zuordnung zugangsberechtigter Mitarbeiter/innen zu drei Anmeldestufen:
- Zugang zum Arbeitsplatz-PC/ Zugang von außen ins Netzwerk (verschlüsseltes VPN)
- Zugang zu den Server-Systemen
- Zugang zum internen LawFirm System (Verwaltung von Interessenten und Kunden, Auftragsabwicklung, Support)
- Für verschiedene Stufen von Zugangsberechtigungen existieren festgelegte Sicherheitsprofile:
- Windows Benutzergruppen sind entsprechend konfiguriert.
- Zugriffsberechtigungen im internen LawFirm System werden entsprechend zugeteilt.
- Zugriffsberechtigungen für den externen Zugriff (über verschlüsseltes VPN) werden nur einer sehr kleinen Benutzergruppe zugeteilt.
- Externe Zugriffe werden in den Windows Serverprotokollen aufgezeichnet.
- Die Zugangsberechtigungen ausgeschiedener Mitarbeiter/innen werden deaktiviert.

V. Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass berechtigte Nutzer von automatisierten Verarbeitungssysteme nur zu den ihrer Zugriffsberechtigung entsprechenden personenbezogenen Daten Zugang haben:

- Festlegung von Zugriffsberechtigungen für die folgenden Ebenen:
- Zugriffsberechtigungen für den externen Zugriff (über verschlüsseltes VPN): berechtigt/ nicht berechtigt.
- Windows Benutzergruppen: verschiedene Gruppen für verschiedene Bereiche von Daten; je Gruppe: nicht berechtigt/ nur lesend / lesend und schreibend.
- Zugriffsberechtigungen im internen LawFirm System: Das LawFirm Zugriffsberechtigungs-System erlaubt die Zuordnung zu verschiedenen Gruppen mit festgelegten Berechtigungsprofilen oder individuelle Einstellungen, Zugriffsberechtigungen auf einzelne LawFirm Fenster bzw. besondere Funktionen, Unterscheidung nach Befugnissen: Ansehen, neue Einträge, Ändern/Löschen, Listenabrufe, Auswertungen mit verschiedenen Zusammenfassungs-Graden
- Die Arbeit mit den o.g. Zugriffsberechtigungen ist nur nach erfolgreicher Anmeldung in den drei Anmelde-Ebenen möglich:
- Arbeitsplatz bzw. externer Netzwerk-Zugang über verschlüsseltes VPN,
- Server-Systeme,
- internes LawFirm System.
- Entwicklungs- und Testumgebungen für die Herstellung der Anwaltssoftware LawFirm sind getrennt von der Produktivumgebung mit der personenbezogene Daten verwaltet werden.
- Für die Durchführung von Tests auf den Server-Systemen werden separate Windows Benutzer und Benutzergruppen verwaltet.
- Die Verwaltung der Berechtigungsprofile erfolgt über einen Systemadministrator.

B. Integrität (Art. 32 Abs. (1) lit. b) DSGVO)

1. Übertragungskontrolle

Die Maßnahmen zur Übertragungskontrolle stellen sicher, dass überprüft und nachvollzogen werden kann, an welche Stellen personenbezogene Daten übermittelt oder zur Verfügung gestellt wurden:

- Übertragungen von personenbezogenen Daten der Kunden finden nicht statt.
- Übertragungen sonstiger personenbezogener Daten erfolgen nur an Empfänger, mit denen ein Auftragsverarbeitungsvertrag besteht oder wenn es sich um Berufsgeheimnisträger handelt (z.B. externe Lohnabrechnung), so dass die Vertraulichkeit gewährleistet ist.
- Personenbezogene Daten werden nicht auf Mobilgeräte synchronisiert.
- Für den externen Netzwerk-Zugang über verschlüsseltes VPN ist nur eine sehr kleine Benutzergruppe nutzungsberechtigt.
- Externe Zugriffe werden in den Windows Serverprotokollen aufgezeichnet.

- Über den externen Netzwerk-Zugang werden nur die internen Server-Systeme und dortigen Anwendungen (internes LawFirm System) genutzt. Eine Übertragung personenbezogener Daten zur Speicherung an einem anderen Ort findet nicht statt.

II. Transportkontrolle

Maßnahmen zur Sicherstellung, dass bei der Übermittlung von personenbezogenen Daten oder beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden:

- Soweit Übertragungen von personenbezogenen Daten auf digitalem Weg stattfinden, werden verschlüsselte Verbindungen genutzt:
- Zugang über verschlüsseltes VPN,
- Datenerfassung über mit SSL gesicherte Web-Formulare.
- Der Austausch von Daten mit Kunden zum Zweck des Supports findet über verschlüsselte Transportwege statt (mit dem SSL bzw. SFTP Protokoll).
- Zu diesem Zweck übertragene Inhalte befinden sich in verschlüsselten Datenbanken.

C. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. (1) lit. b) DSGVO)

1. Verfügbarkeitskontrolle

Maßnahmen zum Schutz personenbezogener Daten gegen Zerstörung oder Verlust:

- Das Büro ist mit Rauchmeldeanlagen ausgestattet.
- In der Nähe der Serverschränke befindet sich ein Feuerlöschgerät und eine Löschdecke.
- Stromanschlüsse für IT Geräte sind über separate Sicherungskreise abgesichert.
- Die IT Systeme sind mit Anti-Viren Software geschützt.
- Betriebssystem und Daten der Server-Systeme werden auf getrennten Festplatten bzw. Partitionen gespeichert.
- Die Partitionen mit Daten sind verschlüsselt.
- Mitarbeiter/innen werden in speziell zur Erkennung verdächtiger E-Mail Anhänge eingewiesen und dürfen solche im Zweifel nicht öffnen.
- Sicherungskopien werden in mehreren Ebenen erzeugt:
- Image-Sicherungen (Betriebssystem-Einrichtung/ Software) auf verschlüsselten externen Datenträgern,
- Bewegungsdaten (insbes. Datenbankinhalte, neue oder veränderte Dokumente) über Nacht auf separaten, verschlüsselten Datenträgern,
- Aktualisierung mehrerer vollständiger Sicherungskopien (reihum) mit Hilfe einer Synchronisationssoftware auf externen, verschlüsselten Datenträgern,
- Zur Datensicherung eingesetzte externe Datenträger sind verschlüsselt und werden extern an einem sicher verschlossenen ausgelagerten Ort aufbewahrt.
- Server-Systeme werden für den Fall eines Ausfalls redundant und fertig eingerichtet vorgehalten.
- Arbeitsplatz-Computer stehen ebenfalls als Reserve zur Verfügung.

II. Zuverlässigkeit

Maßnahmen zur Sicherstellung, dass alle Funktionen der zur Verarbeitung eingesetzten Systeme zur Verfügung stehen und dass Fehlfunktionen entdeckt werden:

- Die IT Systeme sind mit Anti -Viren Software geschützt.
- Die Anti-Viren Software wird regelmäßig aktualisiert.
- Betriebssystem-Updates und Software-Updates werden regelmäßig installiert.
- Windows Server-Protokolle zeichnen Fehlfunktionen auf.
- Redundant eingerichtete Server-Systeme sowie Reserve-Arbeitsplatz-Computer sichern schnelle Wiederverfügbarkeit im Fehlerfall.
- Das mehrstufige Datensicherungskonzept stellt schnelle Verfügbarkeit aktueller Sicherungskopien sicher. Auf extern aufbewahrte Datenträger muss nur im „ Katastrophenfall" zurückgegriffen werden.

III. Datenintegrität

Maßnahmen zur Sicherstellung, dass personenbezogene Daten nicht durch Fehlfunktionen der zur Verarbeitung eingesetzten Systeme beschädigt werden können:

- Die IT Systeme sind mit Anti-Viren Software geschützt.
- Die in der verschlüsselten Datenbank abgelegten Daten des internen LawFirm Systems sind für externe Einflüsse unzugänglich.
- Das mehrstufige Datensicherungskonzept stellt sicher, dass ggf. beschädigte Daten schnell wiederhergestellt werden können.

D. Wiederherstellbarkeit (Art. 32 Abs. (1) lit . c) DSGVO)

1. Wiederherstellbarkeit

Maßnahmen zur Sicherstellung, dass di e zur Verarbeitung personenbezogener Daten eingesetzten Systeme im Fehlerfall wiederhergestellt werden können:

- Redundant eingerichtet e Server-Systeme sowie Reserve-Arbeitsplatz-Computer sichern die Wiederherstellbarkeit bei Problemen mit den Geräten.
- Das mehrstufige Datensicherungskonzept stellt sicher, dass ggf. beschädigte Daten schnell wiederhergestellt werden können.
- Die Wiederherstellung beschädigter Daten per Rückgriff auf die Sicherungskopien wird bei jeder Datensicherung durch Probezugriffe getestet.

E. Regelmäßige Überprüfung (Art . 32 Abs. (1) lit. d) DSGVO)

Maßnahmen zur Sicherstellung, dass die zur Verarbeitung personenbezogener Daten eingesetzten Syst eme im Fehlerfall wiederhergestellt werden können:

- Quartalsweise werden die technischen und organisatorischen Maßnahmen durch Stichproben kontrolliert und das Ergebnis protokolliert ,
- Quartalsmäßige Überprüfung aller Sicherheitskonzepte auf Optimierungsmöglichkeiten.