Dittmeier
Versicherungen für Busunternehmen

Technische und organisatorische Maßnahmen (TOM)

der Dittmeier Versicherungsmakler GmbH

Inhalt

1. Einleitung und Rahmenbedingungen

Die nachfolgenden Festlegungen repräsentieren die Prozess- und Verfahrensübergreifenden technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO der Dittmeier Versicherungsmakler GmbH.

2. Allgemeine Regelungen zum Datenschutz und zur Nutzung der Unternehmens-IT

- Das Datenschutzverfahren ist etabliert und ein Datenschutzhandbuch ist vorhanden
- Es existiert ein IT-Sicherheitskonzept
- Die private Nutzung des Internets ist mit Einschränkungen erlaubt
- Die private Nutzung betrieblicher, mobiler Kommunikationseinrichtungen ist erlaubt
- Mit Auftragnehmern erfolgt die Zusammenarbeit auf der Basis von vertraglichen Regelungen, gem. Art. 28 DSGVO

3. Vertraulichkeit

3.1. Zutrittskontrolle

Die Geschäftsräume befinden sich in den Stockwerken 2-4 der Kaiserstraße 23/25, 97070 Würzburg. Die Zugangstüren zu den Geschäftsräumen sind stets geschlossen und können von außen nur mit einem Schlüssel geöffnet werden. Jedem Mitarbeiter steht ein Schlüssel zur Verfügung. Die Schlüsselvergabe wird dokumentiert. Ein Verlust muss umgehend gemeldet werden. Nach Beendigung des Arbeitsverhältnisses muss der Schlüssel zurückgegeben werden.

Im Rahmen der Zutrittskontrolle wurden Maßnahmen ergriffen, die verhindern, dass unbefugte Personen den physikalischen Zutritt zu Datenverarbeitungsanlagen erhalten. Dazu zählen im weitesten Sinn Computer jeder Art - Server, PC, Notebook, Smartphone, Kopierer und andere Geräte, die sich zur Verarbeitung personenbezogener Daten eignen. Aber auch händische Unterlagen gehören zu den schützenswerten Dokumenten. Diese sind nach Geschäftsschluss durch die einzelnen Mitarbeiter datenschutzkonform aufzuräumen oder zu verschließen.

Unbefugte Personen sind all jene, welche sich aufgrund der ihnen zugewiesenen Aufgaben oder als Besucher nicht bei den entsprechenden Geräten aufhalten müssen. Die o. g. Datenverarbeitungsanlagen werden entsprechend mit Passwörtern, Schlössern oder sonstigen Sperren gesichert.

Besucher melden sich bei Betreten der Geschäftsräume am Empfang an und werden dort registriert. Von einem Mitarbeiter werden die Besucher zum Konferenzraum oder zur Besprechungslounge geleitet und dort betreut bis der oder die Gesprächspartner des Hauses eingetroffen sind.

Alternativ werden die Besucher am Empfang von einem Mitarbeiter abgeholt und während ihres Aufenthaltes in den Geschäftsräumen von diesem begleitet. Nach Beendigung des Besuchs werden die Gäste zur Tür geleitet und dort verabschiedet. Die Fenster sind nach Geschäftsschluss stets zu schließen. Sonstige Absicherungen des Gebäudes, Fenster und Türen sind zu beachten.

Der Zutritt in bestimmte Sicherheitsbereiche der Büroräume (z.B. Serverraum) nur für autorisierte Mitarbeiter gestattet. Für das Schließen und Absperren der Gebäudezugänge ist ein Schließdienst engagiert.

Die gesamten Büroräume sind mit einer Alarmanlage ausgestattet, die bei Verlassen der Büroräume durch den letzten Mitarbeiter aktiviert werden.

3.2. Zugangskontrolle

Durch die nachfolgenden Maßnahmen wird sichergestellt, dass Datenverarbeitungssysteme nicht von Unbefugten genutzt werden können.

- Serversysteme mit abgestuftem und/oder rollenbasiertem Berechtigungskonzept (MS-Domänenkonzept)
- Eindeutige Zuordnung von Benutzerkonten und Kennwörtern - jeder Benutzer hat im Netzwerk ein eigenes, nur ihm bekanntes, Passwort
- Passwortrichtlinien in Bezug auf Passwortsicherheit und Gültigkeitsdauer
- Bildschirmsperre mit Passwortschutz bei Reaktivierung
- Protokollierung der Nutzung der IT-Systeme und Auswertung der Protokolle
- Verschlüsselte Verbindungen (SSL) für externe Zugriffe mittels VPN
- Einsatz von gesicherten WLAN-Verbindungen (WPA2)
- Einsatz von Virenscanner mit ständig aktuellem Virenpattern
- Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware und Virenscanner-Pattern, Betriebssystem-Patches sowie Betriebssystem-Sicherheitspatches
- Einsatz von Firewall-Systemen
- Einsatz eines Fernwartungsprogramms mit ausreichender Verschlüsselung
- Richtlinie für Einarbeitung neuer Beschäftigter und für den Fall eines Ausscheidens aus dem Unternehmen
- Nutzung von verschlüsselten USB-Datenspeichern, die nur durch berechtigte User entschlüsselt werden können
- Automatische PIN-/Passwortsperren für mobile Endgeräte

3.3. Zugriffskontrolle

Folgende Maßnahmen wurden getroffen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, sowie dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Zur Vernichtung von sensiblen Dokumenten werden spezielle verschlossene Mülltonnen eingesetzt, die regelmäßig von einem Fachunternehmen – welches die fach- und datenschutzgerechte Entsorgung zusichert – abgeholt werden
- Zu entsorgende Datenträger werden entweder fach- und datenschutzgerecht von einem Fachunternehmen entsorgt, oder so formatiert, dass ein Wiederherstellen der Inhalte zum aktuellen Stand der Technik ausgeschlossen werden kann
- Systemzugriffe werden in Lese-/Schreib und Veränderungsrechte unterschieden
- Datenbanksysteme haben keine direkte Außenverbindung
- Datenbanksysteme mit abgestuftem Berechtigungskonzept
- Die Anzahl der Administratoren mit entsprechenden Zugriffsrechten ist auf das Notwendigste begrenzt

3.4. Trennungsgebot

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Logische Trennung von Entwicklungssystemen zu Produktivsystemen
- Nutzung eines Berechtigungskonzeptes für Mitarbeiter in der Domäne
- Nutzung eines Berechtigungskonzeptes für administrative oder Entwickler-Zugänge (Datenbankrechte etc.)

- Die Datensicherung erfolgt auf unterschiedlichen Sicherungsmedien (NAS)

4. Integrität

4.1. Weitergabekontrolle

- Anweisung, dass kein Versand von sensiblen/personenbezogenen Daten über unverschlüsselte Wege erfolgen darf
- Es erfolgt eine Verschlüsselung von Daten auf dem Transportweg (z.B. VPN, SFTP, HTTPS zum Dateitransfer)
- Verwendung sicherer Verschlüsselungsverfahren (AES, min. 256 Bit)
- Versand von sensiblen, insbesondere personenbezogenen Daten nur auf Basis von zuvor getroffenen, vertraglichen Vereinbarungen

4.2. Eingabekontrolle

- Zur berechtigten Dateneingabe sind Berechtigungsprofile bzw. –gruppen festgelegt
- Differenzierung des Zugriffs erfolgt durch differenzierte Lese-, Ändern- und Löschen-Berechtigung
- Eingaben im Kundenverwaltungssystem werden mit Art der Änderung, Bearbeiter und Zeitstempel protokolliert

4.3. Auftragskontrolle

- Es bestehen vertragliche Regelungen (gem. § 11 Auftragsdienstleistungen) mit entsprechenden Unternehmungen (Sub-Unternehmungen)
- Aufträge an Sub-Unternehmungen werden nur mit vorheriger schriftlicher Genehmigung eines Auftraggebers vergeben
- Die Einhaltung der Vorgaben zu den technischen und organisatorischen Maßnahmen zum Schutze der Daten gem. §9, Anlage BSDG wird – auch bei Sub-Unternehmungen – überprüft
- Bei der Auswahl von Auftragsdienstleistern wird mit Sorgfalt vorgegangen und insbesondere, entsprechend Wert auf Datensicherheit gelegt

5. Verfügbarkeit und Belastbarkeit

5.1. Verfügbarkeitskontrolle

- Vollständiges Backup- und Recovery-Konzept
- Aufbewahrung von Backups in getrennten Brandabschnitten
- Regelmäßige Tests der Datenwiederherstellung
- Einsatz von Schutzprogrammen und Schutzverfahren (z.B. Virenscanner)
- Einsatz von RAID-Systemen (Festplattenspiegelung) zur sicheren Datenvorhaltung
- Einsatz unterbrechungsfreier Stromversorgung
- Nicht destruktive Brandbekämpfungssysteme mit CO2-Feuerlöschern
- Notfallplan zur Datenwiederherstellung im Falle von versehentlicher Löschung, teilweisem Hardwaredefekt/-verlust und Totalverlust/Katastrophenfall
- Einsatz von vernetzten Brandmeldern in den Büroräumen mit Alarmfunktion auf dem Smartphone des Brandschutzbeauftragten und seiner Brandschutzhelfer
- Einsatz von Klimaanlagen, um die Temperatur im Serverraum auf einem konstanten optimierten Level zu halten

6. Schlusserklärung

Im Übrigen sorgt der Datenschutzbeauftragte durch die Datenschutzorganisation für die angemessene und effektive Einbindung der „technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO in die betrieblichen Prozesse. Insbesondere erfolgt dies durch Erstellen und Führen eines Datenschutzmanagementsystems und Kontaktaufnahme mit der zuständigen Landesaufsichtsbehörde für den Datenschutz.