Zotorn IT UG (haftungsbeschränkt)

Technische und organisatorische Maßnahmen nach Art.32 DSGVO

1. Zutrittskontrolle

Die Büroräume befinden sich in einem Bürohaus in Ottobrunn bei München. Die Zugänge zu den Büroräumen der Zotorn IT UG (haftungsbeschränkt) sind Tag und Nacht verschlossen. Zugang zu dem Bürohaus haben nur der Vermieter und die Mieter der Büroräume, sowie Besucher. An den Büroräumen kommt ein Schließsystem zum Einsatz, das vom der Zotorn IT UG (haftungsbeschränkt) selbst verwaltet wird.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch die Geschäftsführung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher erhalten freien Zutritt zum Bürohaus und werden in den Büroräumen der Zotorn IT UG (haftungsbeschränkt) empfangen. Jeder Besucher wird von einem Mitarbeiter zu seinem jeweiligen Ansprechpartner begleitet. Besucher dürfen sich nicht ohne Begleitung in den Büroräumen frei bewegen.

Die Eingänge und Fenster der Büroräume werden mit Dienstschluss verschlossen und kontrolliert.

2. Zugangskontrolle

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzer Berechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von der Geschäftsführung freigegeben wurde.

Der Benutzer erhält dann einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 14 Zeichen.

Remote-Zugriffe auf IT-Systeme der Zotorn IT UG (haftungsbeschränkt) erfolgen stets über verschlüsselte Verbindungen.

Alle Microsoft Windows basierten Server- und Client-Systeme verfügen über Virenschutzsoftware, bei der eine tagesaktuelle Versorgung mit Signaturupdates gewährleistet ist.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

3. Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen werden ausschließlich von Administratoren eingerichtet. Berechtigungen werden grundsätzlich nach dem Need-to-know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.

Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten. Der Antrag kann auch bei der Personalabteilung gestellt werden. Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Die Vernichtung von Papier erfolgt über Schredder.

4. Trennung

Alle für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die Trennung von Daten von verschiedenen Kunden ist stets gewährleistet.

5. Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

Daten mit hohen Schutzbedarfen werden nach aktuellem Stand der Technik mit verschlüsselten Verfahren analog der internen IT-Sicherheitsrichtlinie zur Kryptographie gesichert. Die eingesetzten Verschlüsselungsverfahren basieren auf Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Werden Daten anhand Datenträger ausgetauscht, wird dokumentiert, wer zu welchem Zeitpunkt zu welchem Zweck von wem einen Datenträger erhält. Datenträger, die nicht mehr zum produktiven Einsatz kommen, werden durch sichere Lösch- und Überschreib-Verfahren nach Empfehlungen des BSI entsorgt.

6. Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die im Auftrag verarbeitet werden, wird grundsätzlich protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten.
Benutzer-Accounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

7. Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten bei Zotorn (haftungsbeschränkt) im Zusammenhang mit Kundenprojekten untersagt.

Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

8. Verfügbarkeit und Belastbarkeit

Daten auf Serversystemen werden mindestens täglich inkrementell und wöchentlich ”voll” gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort verbracht.

Das Einspielen von Backups wird regelmäßig getestet.