Technische und organisatorische Maßnahmen nach § 28 DSGVO und Anlage

Folgende technische und organisatorische Maßnahmen sind in unserem Hause umgesetzt:

1. Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle

- Besucher erhalten erst nach Türöffnung durch einen Mitarbeiter oder des Sicherheitspersonals Zutritt zum Eingangsbereich
- Ein Sicherheitspersonal garantiert eine 24/7 Überwachung des Gebäudes
- Besucher haben nur Zutritt durch vorherige Anmeldung bzw. durch Eintrag einer internen Zutrittsliste
- Die interne Zutrittsliste wird von einem Mitarbeiter verwaltet.
- Schlüssel-, Schlüsselvergabe werden durch einen Mitarbeiter bzw. durch das Sicherheitspersonal nach einem definierten Prozess ausgehändigt
- Türen im Gebäude sind durch entsprechende Sicherheitstechnik vor unbefugten Personen geschützt
- Eine interne Überwachungseinrichtung erfasst den Ein-, Ausgangsbereich, Sicherheitsschleusen sowie Serverräume
- Eine interne Alarmanlage kann von jedem Mitarbeiter auf Funktion eingesehen werden. Ausschalten ist nur durch einen autorisierten Mitarbeiter gegeben
- Durch einen Videomonitor kann von den Mitarbeitern der Ein-, Ausgansbereich, Sicherheitsschleusen sowie Serverräume eingesehen werden.
- Jeder Besucher muss sich in ein elektronisches Besucherprotokoll eintragen
- Jeder Besucher erhält zur Kennzeichnung einen Besucherausweis, der ersichtlich getragen werden muss
- Es dürfen sich keine Besucher ohne Begleitung in den Büroräumen bewegen/aufhalten

1.2 Zugangskontrolle

Bei „Dedicated Server“, „Cloud Server” obliegt die Verantwortung beim Auftraggeber:

- Server Passwörter werden zur einmaligen Nutzung erteilt und müssen sofort vom Auftraggeber geändert werden. Das neu gesetzte Passwort ist der aixit GmbH nicht bekannt.

Bei „Managed Server“ obliegt die Verantwortung bei der aixit GmbH:

- Die Zugänge sind Passwortgeschützt
- Der Zugriff besteht nur für berechtigte Mitarbeiter
- Die Remote-Zugriffe erfolgen nur über verschlüsselte Verbindungen
- Alle Server sowie Client-Systeme werden durch eine regelmäßig gewartete Firewall geschützt
- Verwendete Passwörter müssen eine Mindestlänge haben und werden in regelmäßigen Abständen erneuert

- Alle Mitarbeiter sind angewiesen, ihre Endgeräte bei nicht Nutzung zu sperren.

1.3 Zugriffskontrolle

Bei „Dedicated Server“, „Cloud Server“ obliegt die Zugriffskontrolle bei dem Auftraggeber.

Bei „Managed Server“ obliegt die Zugriffskontrolle bei der aixit GmbH

- Durch regelmäßige Sicherheitsupdates stellt die aixit GmbH sicher, das unberechtigter Zugriff verhindert wird.
- Berechtigungen erhalten nur Mitarbeiter die diese IT-Systeme warten und pflegen.
- Für übertragene Daten/Software ist einzig der Auftraggeber in Bezug auf Sicherheit und Updates zuständig.

- Interne IT-Systeme werden durch regelmäßige Sicherheitsupdates vor unberechtigte Zugriffe geschützt.
- Alle Mitarbeiter müssen nicht mehr benötigte, ausgedruckte Informationen mit personenbezogenen Daten und/oder Informationen über Projekte in die hierfür ausgewiesenen Vernichtungsgeräte einwerfen.
- Den Mitarbeitern ist es untersagt, nicht genehmigte Software auf den Endgeräten zu installieren.
- Festplatten werden nach Kündigung nach einem definierten Prozess mehrfach überschrieben. Defekte Festplatten werden zerstört.

2. Gewährleistung der Vertraulichkeit

Die Gewährleistung der Vertraulichkeit wird unter Punkte 1.1 bis 1.3. geregelt.

3. Gewährleistung der Integrität

3.1 Weitergabekontrolle

- Alle Mitarbeiter sind unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen, sowie eine nach Auftragsbeendigung Datenschutzgerechte Löschung.
- Soweit möglich werden Daten (je nach Stand der Technik) verschlüsselt übertragen.

3.2 Eingabekontrolle

Bei „Dedicated Server“ „Cloud Server“ obliegt die Verantwortung beim Auftraggeber

Bei „Managed Server“ obliegt die Verantwortung bei der aixit GmbH

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst
- Änderungen an Daten durch die aixit GmbH werden protokolliert.

3.3 Auftragskontrolle

- Die Verarbeitung der Datenhaltung erfolgt ausschließlich in der Europäischen Union.
- Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben jeweils ein Auftragsverarbeitungsvertrag durch den Datenschutzbeauftragen abgeschlossen.
- Mitarbeiter der aixit GmbH werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen.
- Die aixit GmbH hat einen externen Datenschutzbeauftragten sowie einen betrieblichen Datenschutzverantwortlichen.
- Die aixit GmbH ist durch ISO 27001 zertifiziert und aktualisiert diese regelmäßig.

3.4 Trennungskontrolle

Zu gewährleisten ist, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden:

- Interne Mandantenfähigkeit/Zweckbindung
- Funktionstrennung

4. Gewährleistung der Verfügbarkeit

4.1 Verfügbarkeitskontrolle

- Für alle internen Systeme ist eine Prozesskette definiert, die genau beschreibt wer im Fehlerfall zu informieren ist, um die Systeme schnellstmöglich wiederherzustellen. Alle relevanten Server unterliegen einem Monitoring sowie einem dauerhaft aktiven DDoS-Schutz, das im Falle von Störungen unverzüglich Meldungen an einen beauftragten Mitarbeiter auslöst. Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung.
- Die aixit GmbH verwaltet Backups auf unterschiedlichen Systemen die getrennt voneinander an unterschiedlichen Brandschutzabschnitten zu finden sind. Die Backups werden durch ein Monitoringsystem überwacht.
- Bei „Dedicated Server“ „Cloud Server” obliegt die Datensicherung beim Auftraggeber.

5. Pseudonymisierung

- Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.
- Darüber hinaus werden Daten auf Server- und Clientsystemen auf verschlüsselten Datenträgern gespeichert. Es befinden sich entsprechende Festplattenverschlüsselungssysteme im Einsatz.
- Die Hardware im Serverraum wird ausschließlich durch ID Nummern anstelle von Klarnamen beschriftet.
- Datensätze werden nach Stand der Technik verschlüsselt (siehe 4.1)

7. Gewährleistung der Belastbarkeit der Systeme

- Daten auf Serversystemen von aixit GmbH werden mindestens täglich inkrementell und wöchentlich „voll“ gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Brandschutzbereich verbracht.
- Das Einspielen von Backups wird regelmäßig getestet.
- Die IT-Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Serverraum befindet sich eine Brandmeldeanlage.
- Alle Serversysteme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.
- Es gibt bei aixit GmbH einen Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

8. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

- Die aixit GmbH verwaltet Backups auf unterschiedlichen Systemen die getrennt von einander an unterschiedlichen Brandschutzabschnitten zu finden sind. Die Backups werden durch ein Monitoringsystem überwacht.

9. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

- Es ist ein Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt.
- Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
- Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort
- untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.
- Bei der Verarbeitung von Daten für eigene Zwecke wird im Falle des Vorliegens der Voraussetzungen des Art. 33 DSGVO eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Kenntnis von dem Vorfall erfolgen.