Anhang „Technisch-organisatorische Maßnahmen“

Nach § 9 BDSG bzw. Art. 32 DSGVO

§ 1. Technische und organisatorische Sicherheitsmaßnahmen
Gemäß § 11 Abs. 2 S. 2 Nr. 3 BDSG in Verbindung mit § 9 BDSG bzw. Art. 32 DSGVO sind die Vertragspartner verpflichtet, die technischen und organisatorischen Sicherheitsmaßnahmen festzulegen.

In anderen Worten,

sind wir als Cloud- und Hostingprovider dazu verpflichtet, ein Höchstmaß an Sicherheit für den Schutz von sensiblen, insbesondere personenbezogenen Daten zu gewährleisten.

§ 2. Innerbetriebliche Organisation des Auftragnehmers
Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

In anderen Worten,

wir werden zu jeder Zeit jede Maßnahme ergreifen, die den Schutz vertraulicher, persönlicher und personenbezogener Daten gewährleistet.

§ 3. Konkretisierung der Einzelmaßnahmen
Im Einzelnen werden folgende Maßnahmen bestimmt:

§ Vertraulichkeit (Art. 32 Abs. 1 lit. b. DSGVO)
• Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen. Die Sicherung von Räumlichkeiten erfolgt durch Zutrittsregelung (nur einzelnen Personen wird nach vorheriger Anmeldung Zutritt gewährt), persönliche RFID-Karten zzgl. eines persönlichen biometrischen Merkmals (Fingerabdrucks), elektrische Türöffner, Vereinzelungsanlagen, einen 24/7 Werkschutz, Alarmanlagen und Videoanlagen an allen Ein- und Ausgängen sowie in den Räumlichkeiten selbst;
• Zugangskontrolle
Keine unbefugte Systembenutzung. Jeder Benutzer hat persönliche Zugangsdaten. Es kommen ausschließlich sichere Kennwörter zum Einsatz. Zugänge werden automatisch gesperrt, wenn ein Verdacht auf Manipulation vorliegt. Eine Zwei-Faktor-Authentifizierung ist obligatorisch und sämtliche Datenträger werden verschlüsselt;
• Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems. Dazu kommen Berechtigungskonzepte zum Einsatz. Zugriffsrechte werden nach dem Deny-Allow-Prinzip erteilt und auf das nötigste beschränkt. Jeder Zugriff wird Protokolliert;
• Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B.: Mandantenfähigkeit, Sandboxing, Trennung von Test- und Produktumgebungen;
• Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
Die Verarbeitung personenbezogener Daten findet in einer Weise statt, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen;

In anderen Worten,

um die Vertraulichkeit zu sichern, schützen wir alle unsere Server und Datenspeicher vor unbefugtem, physischen Zugriff mit allen verfügbaren Mitteln. Die Nutzung unserer Systeme oder Services ist ohne persönliche Zugangsdaten ausgeschlossen. Niemand – auch nicht unsere Mitarbeiter – haben unmittelbaren Zugriff auf deine Daten. Grundsätzlich vergeben wir nur solche Benutzerrechte (ggf. temporäre Rechte), die unbedingt für die Arbeit unserer Mitarbeiter erforderlich sind und protokollieren jeden Vorgang.
Informationen, die wir zum Beispiel für unsere Entwicklungsprozesse benötigen, beinhalten niemals persönliche Daten. Wir gewährleisten, dass ein Datenexport vertraulicher Daten niemals möglich ist. Sollten wir doch irgendwann einmal personenbezogene Daten verarbeiten, werden wir diese Daten durch algorithmische Maßnahmen so anonymisieren, dass aus den Daten keine natürliche Person erkennbar ist.

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

• Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport. Dazu wird nach aktuellen wissenschaftlichen Erkenntnissen auf Verschlüsselung der Daten sowie Datenübertragung durch Virtual Private Networks (VPN) gesetzt. Daten werden vor Übertragung mit Prüfsumme versehen, um die Unveränderte Übertragung validieren zu können;

• Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dazu werden Änderungen und Eingaben von Daten protokolliert. Dokumente werden in einem Dokumentenmanagementsystem verwaltet.

In anderen Worten,

die Datenintegrität stellen wir sicher, indem wir stets mit starker Verschlüsselung arbeiten und eine ungewollte Veränderung von Daten über die Anwendung von Prüfsummen umgehend identifizieren.

Das Erstellen neuer oder Ändern bestehender Daten protokollieren wir für die bessere Nachvollziehbarkeit. Wir können also erkennen, „wer" „wann" „was" gemacht hat.

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

• Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch eine online Backup-Strategie (off-site), eine unterbrechungsfreie Stromversorgung (USV), redundanter Hardware, Netztrennungen und dem Einsatz von Firewalls sowie der Gewährleistung einer schnellen Wiederherstellung von Services im Fehlerfall.

• Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

In anderen Worten,

wir überwachen alle unsere Dienste und tun alles in unserer Macht stehende für die höchstmögliche Verfügbarkeit und höchstmögliche Sicherheit. Wir sichern zwar unsere eigenen Daten, nicht aber deine Daten.
Wir üben regelmäßig verschiedene Ereignisse, um uns auf eine große Störung vorzubereiten und um dann sofort zu wissen, was wir tun müssen.

§ Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)
• Datenschutz-Management;
• Incident-Response-Management;
• Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
• Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers. Dazu liegt eine eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement vor und etwaige Dienstleisters werden nach strengen Kriterien ausgewählt. Es finden angemessene Kontrollen und Nachkontrollen statt.

In anderen Worten,

wir stellen jederzeit einen sehr guten Datenschutz sicher und sorgen für einen datenschutzfreundlichen Betrieb. Niemals führen wir ohne deinen Auftrag eine Verarbeitung deiner vertraulichen oder persönlichen Daten durch. Außerdem gewährleisten wir, dass 24/7 erfahrene Ingenieure den Betrieb sicherstellen.