Technische und organisatorische Maßnahmen

gem. Art. 32 Abs. 1 Datenschutz Grundverordnung (DSGVO)
für Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

Version 1.9

Auftragsverarbeiter

JT3 Software GmbH
Rieslingstrasse 23
65343 Eltville
Deutschland
Handelsregister: Amtsgericht Wiesbaden, HRB 35081

E-Mail: info@terminarena.de

Internet-Adresse: www.terminarena.de

1. Terminologie

Soweit in diesem Dokument nicht abweichend definiert, gelten die Begriffsbestimmungen der Datenschutz-Grundverordnung (DSGVO). Für die Zwecke dieses Dokuments bezeichnet:

- „Auftragnehmer“ den Auftragsverarbeiter;
- „Auftraggeber“ den Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO;
- „Software“ die durch den Auftragnehmer bereitgestellte Software-as-a-Service-Lösung.

2. Zweck und Anwendungsbereich

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM), die der Auftragsverarbeiter zum Schutz personenbezogener Daten im Rahmen der Bereitstellung seiner Software-as-a-Service-Lösung umsetzt.

Die Maßnahmen dienen insbesondere der Gewährleistung von:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Belastbarkeit der Systeme und Dienste
- Fähigkeit zur raschen Wiederherstellung im Falle eines Zwischenfalls

3. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Zutrittskontrolle durch den Hosting Anbieter

Die Hetzner Online GmbH betreibt viele Rechenzentren und ist Marktführer im Segment der Hosting-Anbieter. Tausende Unternehmen verwenden die Hosting-Dienstleistungen von Hetzner. Der Dienstleister bietet entsprechend hohe Sicherheitsstandards bei der Zutrittskontrolle zu den Rechenzentren, darunter:

- Physische Sicherung der Rechenzentren durch den Hosting-Anbieter
- Zugang zu Serverräumen nur für autorisiertes Personal
- Dokumentierte Zutrittsregelungen beim Infrastrukturbetreiber

3.2 Zutrittskontrolle durch den Auftragnehmer

Die Verarbeitung personenbezogener Daten des Auftraggebers erfolgt auf Servern innerhalb der Rechenzentren des eingesetzten Hosting-Anbieters. In den Büroräumlichkeiten des Auftragnehmers werden personenbezogene Daten grundsätzlich weder dauerhaft gespeichert noch verarbeitet.

Der Zugriff auf personenbezogene Daten erfolgt ausschließlich über gesicherte Arbeitsplatzrechner des Auftragnehmers im Rahmen der vorgesehenen Systemzugänge.

Die vom Auftragnehmer genutzten Arbeitsplatzrechner werden ausschließlich vom Arbeitgeber bereitgestellt. Der Einsatz privater Endgeräte der Mitarbeitenden (Bring Your Own Device – BYOD) ist nicht vorgesehen.

Der Zugriff auf die Systeme des Hosting-Anbieters erfolgt ausschließlich über gesicherte Verbindungen mittels aktueller TLS-/SSL-Verschlüsselung.

Der Zugriff auf die Systeme ist nur nach erfolgreicher Authentifizierung mittels individueller Benutzerkennung und Passwort möglich. Die Zugangsdaten werden ausschließlich autorisierten Mitarbeitenden des Auftragnehmers im Rahmen ihrer jeweiligen Berechtigungen bereitgestellt.

Zugangsdaten sind vertraulich zu behandeln und dürfen nicht unbefugt weitergegeben oder Dritten zugänglich gemacht werden.

Beim Auftragnehmer kommt eine zentrale Benutzer- und Rechteverwaltung zum Einsatz. Beim Ausscheiden von Mitarbeitenden werden die jeweiligen Benutzerkonten und Zugriffsrechte unverzüglich deaktiviert oder gelöscht. Jede Nutzerkennung ist eindeutig einer natürlichen Person zugeordnet.

Die vom Auftragnehmer eingesetzten Arbeitsplatzrechner verfügen über eine automatische Sperrfunktion, die bei Inaktivität nach einer definierten Zeitspanne eine Sperrung des Systems auslöst und eine erneute Authentifizierung erfordert.

Betriebssysteme und sicherheitsrelevante Software werden regelmäßig und automatisiert aktualisiert, um Sicherheitslücken zeitnah zu schließen.

Der Zugriff auf die Arbeitsplatzrechner ist ausschließlich nach erfolgreicher Authentifizierung mittels Benutzername und Passwort möglich.

Die eingesetzten Arbeitsplatzrechner verfügen über eine vollständige Festplattenverschlüsselung, sodass bei Verlust oder unbefugtem Zugriff kein Zugriff auf gespeicherte Daten oder Zugangsinformationen möglich ist.

Passwörter unterliegen einer definierten Passwort-Policy, die insbesondere Mindestlänge, Komplexität und regelmäßige Änderung berücksichtigt.

Die IT-Systeme sind durch geeignete Firewall-Systeme gegen unbefugte Zugriffe geschützt.

Die Konfiguration von Betriebssystemen und Anwendungssoftware erfolgt nach aktuellen Sicherheitsstandards, Herstellerempfehlungen sowie anerkannten Best Practices und wird regelmäßig überprüft und angepasst.

Die Büroräume des Auftragnehmers sind durch geeignete Zutrittskontrollsysteme gegen den unbefugten Zutritt Dritter geschützt.

Kundenbesuche finden grundsätzlich nicht in den Büroräumlichkeiten des Auftragnehmers statt, da die Leistungserbringung ausschließlich über internetbasierte Systeme erfolgt und keine Vor-Ort-Termine angeboten werden. Kundentermine werden ausschließlich über elektronische Kommunikationsmittel durchgeführt. Sofern ausnahmsweise Besucher empfangen werden, erfolgt deren Zutritt kontrolliert und

dokumentiert. Besucher werden während ihres Aufenthalts durch autorisierte Mitarbeitende des Auftragnehmers begleitet.

3.3 Zugriffskontrolle

- Rollenbasiertes Berechtigungskonzept (Role-Based Access Control)
- Zugriff nur nach dem Need-to-know-Prinzip
- Verwendung individueller Benutzerkonten
- Verbot von geteilten Benutzerkonten

3.4 Zugriffssicherheit

- Authentifizierung mittels sicheren Passwortrichtlinien
- Optional: Multi-Faktor-Authentifizierung (MFA)
- Automatische Sperrung bei Inaktivität

3.5 Trennungskontrolle

- Logische Trennung von Kundendaten innerhalb der Anwendung
- Mandantenfähigkeit der SaaS-Plattform
- Trennung von Produktions- und Testsystemen

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

- Schutz vor unbefugter Änderung durch Zugriffskontrollen
- Protokollierung sicherheitsrelevanter Systemereignisse
- Datenübertragung ausschließlich verschlüsselt (TLS)
- Validierung von Eingaben zur Vermeidung von Manipulationen

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

5.1 Backup-Konzept

- Regelmäßige, automatisierte Backups
- Getrennte Speicherung von Backup-Daten
- Definierte Aufbewahrungsfristen für Backups
- Regelmäßige Überprüfung der Wiederherstellbarkeit

5.2 Systemverfügbarkeit

- Betrieb in professionellen Rechenzentren (EU/EWR)
- Monitoring der Systemverfügbarkeit
- Redundante Systemarchitektur (soweit technisch umgesetzt)

5.3 Wiederherstellbarkeit

- Definierte Prozesse zur Datenwiederherstellung
- Regelmäßige Tests von Restore-Prozessen

6. Pseudonymisierung und Verschlüsselung

- Verschlüsselung der Datenübertragung mittels TLS (HTTPS)
- Einsatz aktueller Verschlüsselungsstandards nach Stand der Technik
- Passwortspeicherung ausschließlich gehasht und gesalzen

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Regelmäßige Überprüfung der technischen Sicherheitsmaßnahmen
- Patch- und Update-Management für eingesetzte Systeme
- Sicherheitsupdates werden zeitnah eingespielt
- Dokumentierte Sicherheits- und Wartungsprozesse
- Incident-Response-Prozesse bei Sicherheitsvorfällen

8. Auftragskontrolle (Art. 28 DSGVO)

- Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung des Auftraggebers
- Verpflichtung aller Mitarbeiter auf Vertraulichkeit und Datenschutz
- Abschluss von Vertraulichkeitsvereinbarungen mit Beschäftigten
- Kontrolle von Unterauftragnehmern gemäß Subprozessor-Management

9. Eingabekontrolle

- Protokollierung von Zugriffen und Änderungen an Daten (Audit-Logs)
- Nachvollziehbarkeit, wer Daten wann geändert oder gelöscht hat
- Schutz der Logs vor unbefugter Veränderung

10. Transport- und Übertragungssicherheit

- Verschlüsselte Datenübertragung (TLS 1.2 oder höher)
- Keine unverschlüsselte Übertragung personenbezogener Daten
- Gesicherte API-Kommunikation

11. Organisationsmaßnahmen

- Datenschutzverpflichtung aller Mitarbeiter
- Schulung der Mitarbeiter zu Datenschutz und IT-Sicherheit
- „Need-to-know“-Prinzip
- Dokumentierte Sicherheitsrichtlinien
- Zentrale Datenschutzkontaktstelle

12. Subunternehmer-Management

- Einsatz von Unterauftragnehmern nur gemäß Art. 28 DSGVO
- Vorherige Prüfung und vertragliche Bindung aller Subprozessoren
- Führung einer aktuellen Subprozessor-Liste
- EU/EWR-basierte Verarbeitung (sofern nicht anders vertraglich geregelt)

13. Incident Management (Datenschutzverletzungen)

- Verfahren zur Erkennung und Meldung von Sicherheitsvorfällen
- Meldung von Datenschutzverletzungen innerhalb gesetzlicher Fristen
- Unterstützung des Auftraggebers bei Meldepflichten nach Art. 33 und 34 DSGVO
- Dokumentation aller Vorfälle

14. Stand der Technik

Alle Maßnahmen werden regelmäßig überprüft und an den Stand der Technik angepasst. Änderungen erfolgen unter Berücksichtigung von Risiko, Wirksamkeit und wirtschaftlicher Zumutbarkeit.