Anlage 2 - Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO i.V.m. Art. 5 Abs. 1, Abs. 2 DS-GVO

1. Vertraulichkeit

1.1. Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der ihm übertragenen Leistungen genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Dokumentation der Vergabe von Schlüsseln oder RFID-Chipkarten
- Gesonderte Zutrittskontrolle für Räume mit kritischer IT-Infrastruktur
- Rückgabe von Schüsseln oder RFID-Chipkarten nach Austritt von Mitarbeitern
- Schutz des Firmengeländes (Pforte, Zaun etc.)
- Verwendung einer Zutrittskontrolle (schlüsselbasierte oder Zutrittssysteme)
- Verwendung sicherer Türen und Fenster

Ergänzender Hinweis: Die physische Absicherung der SaaS-Hostingumgebung erfolgt durch zertifizierte Rechenzentrumsbetreiber in Deutschland gemäß der beiliegenden Zusatzerklärung zum Hosting-Standort.

1.2. Zugangskontrollen

Es ist zu verhindern, dass die zur Erbringung der in der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt
werden können.
Beim Auftragnehmer umgesetzte Maßnahmen:

- Anwendung von Maßnahmen zur Verschlüsselung von lokalen Daten (z. B. Festplatten)
- Automatisches Sperren von PCs/Macs nach 5 Minuten
- Verwendung personalisierter Logins im Unternehmensnetzwerk
- Verwendung sicherer und individueller Passwörter

1.3. Zugriffskontrolle

Es ist sicherzustellen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Dokumentation eingerichteter Zugänge für Mitarbeiter
- Einführung von Benutzer- und Rollenkonzepten für interne Systeme
- Sperrung von Zugängen nach Austritt von Mitarbeiter
- Zentrale Verwaltung von Benutzerzugängen und -rechten

1.4. Weitergabekontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Nutzung SSL-verschlüsselter Übertragungswege im Internet
- Sicherung von Dokumenten beim Versand auf dem Postweg
- Verschlüsselter Versand von E-Mails (TLS)
- Verwendung von VPN-Systemen zum Login in das Firmennetzwerk

1.5. Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Einführung von Zugriffsberechtigungen für interne Systeme
- Trennung von internem WLAN und Gäste-WLAN
- Verbot der Nutzung von privaten Endgeräten im Firmennetzwerk

1.6. Pseudonymisierung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, 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.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Trennung von Kontaktdaten und weiteren nutzerbezogenen Daten

1.7. Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Verwendung verschlüsselter Übertragungswege für den Datenaustausch
- Verwendung von SSL-Zertifikaten für Hostingumgebungen

Die logische Sicherheit der Hostingumgebung wird durch ein nach ISO/IEC 27001 zertifiziertes Managementsystem des Infrastruktur-Partners gewährleistet.

2. Integrität

2.1. Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene
Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Einführung von Benutzer- und Rollenkonzepten für interne Systeme
- Einführung individueller Zugänge für interne Systeme
- Protokollierung von Zugriffen im Firmennetzwerk
- Verwendung personalisierter Logins im Unternehmensnetzwerk

2.2. Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem. 1.4 dienen auch der Sicherstellung der Integrität.

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Regelmäßige Aktualisierung der Virendefinitionen
- Regelmäßige Durchführung von Datensicherungen
- Regelmäßige Durchführung von Updates (Windows, Mac, Linux,
- Desktopanwendungen) Regelmäßige Überprüfung der erstellten Datensicherungen
- Verwendung einer Firewall (z. B. Barracuda, Check Point, Cisco, Sophos)
- Verwendung eines Virenscanners (z. B. AVG, Bitdefender, Kaspersky, Symantec)
- Verwendung einer unterbrechungsfreien Stromversorgung (USV) für interne Systeme
- Verwendung eines Überspannungsschutzes für interne Systeme
- Verwendung von RAID-Systemen (z. B. für lokale File- und Entwicklungsserver)

3.2. Rasche Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall raschwiederherzustellen.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Dokumentation und Test von Datenwiederherstellungen
- Erstellung von Notfallplänen zu kritischen Prozessen

4. Weitere Maßnahmenbereiche

4.1. Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Dokumentation von datenschutzrelevanten Zwischenfällen
- Löschen nicht mehr benötigter Daten (z. B. veraltete Daten, Testumgebungen)
- Sichere Entsorgung defekter/nicht mehr benötigter Hardware
- Sichere Entsorgung von Dokumenten (z. B. Aktenvernichter, Reisswolf)

4.2. Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

4.3. Fernwartung und Support

- **Support-Zugriff:** Der Support erfolgt ausschließlich browserbasiert über gesicherte HTTPS-Verbindungen. Ein direkter Zugriff auf die Client-Infrastruktur mittels Fernwartungssoftware (z. B. TeamViewer) findet nicht statt.
- **Kommunikation:** Zur Abstimmung mit dem Kunden werden etablierte Videokonferenzsysteme (Microsoft Teams / Zoom) eingesetzt. Dabei erfolgt die Übertragung der Audio- und Videodaten verschlüsselt (TLS).
- **Bildschirmfreigabe:** Eine Einsichtnahme in personenbezogene Daten des Kunden erfolgt nur nach expliziter Freigabe des Bildschirms durch den Kunden während einer aktiven Sitzung.

Beim Auftragnehmer umgesetzte Maßnahmen:

- Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden
- Auswahl geeigneter Dienstleister und Partner unter Datenschutzaspekten
- Benennung eines Datenschutzbeauftragten, sofern gesetzlich erforderlich (aktuell ab 10 Personen mit regelmäßiger Datenverarbeitung)
- Durchführung von stichprobenartigen Überprüfungen bei Dienstleistern
- Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter
- Regelmäßige Unterweisung und Fortbildung der Mitarbeiter zum Thema Datenschutz
- Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter