Beschreibung der bestehenden technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

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

1.1 Zutrittskontrolle

Maßnahmen, durch die Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- Lage der Gebäude ist risikoarm. Geringe Angriffswahrscheinlichkeit von außen.
- Auf- und Abschließen der Gebäude bei Arbeitsbeginn bzw. -ende. Protokollierte Schlüsselvergabe.
- Zutritt von Mitarbeitern und registriertem Reinigungspersonal zu Büroflächen nur mittels Schlüsseln.
- Zutritt von anderen Personen (Besucher, Dienstleister etc.) nur nach vorheriger Anmeldung und grundsätzlich ausschließlich in Begleitung von Mitarbeitern.
- Server- und Technikräume nur für Administratoren/Techniker zugänglich. Betrieb der Server in speziellen Sicherheitsräumen.

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Zugang zu Systemen und Applikationen durch persönliche Passwörter geschützt.
- Grundsätzlich Zwei-Faktor-Authentifizierung.
- Schutz des Netzwerks gegen unerlaubten Zugriff aus dem Internet und gegen Schadsoftware durch Firewall-Systeme, Proxy-Server und Antivirensoftware. Alle Zugriffsversuche, zulässige und unzulässige, werden protokolliert.
- Getrennte VPNs (z. B. für Telefonie, Computer, Cloud-Rechenzentrum).
- Zugriffe werden systemseitig oder durch Tätigkeitsnachweise dokumentiert.

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und personenbezogene Daten bei der Verarbeitung nicht unbefugt kopiert, verändert oder gelöscht werden können:

- Zugang zu Systemen und Applikationen durch persönliche Passwörter geschützt.
- Steuerung der Rechte der einzelnen Benutzer (Datenzugriffe, Funktionsumfang) durch dedizierte Rollen- und Berechtigungskonzepte.
- Systemseitige Schutzmaßnahmen gegen unbefugte Veränderung bzw. Löschung von Daten (Funktionsdeaktivierung, Protokollierung von Änderungen).

Beschreibung der bestehenden technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

1.4 **Trennungskontrolle**
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Logische Trennung der Daten in den Datenverarbeitungssystemen.
- Mitarbeiter sind angewiesen und geschult, Daten nur im Rahmen der Dienstleistungserbringung und unter Wahrung der Zweckbindung zu verarbeiten.

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

2.1 **Weitergabekontrolle**
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Weitergabe personenbezogener Daten nur über verschlüsselte Verbindungen oder Datenträger.
- Die Verschlüsselung erfolgt entsprechend dem Stand der Technik.
- Umfangreiche systemseitige Protokollierung von Datenweitergaben.

2.2 **Eingabekontrolle**
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

- Weitergabe personenbezogener Daten nur über verschlüsselte Verbindungen oder Datenträger.
- Die Verschlüsselung erfolgt entsprechend dem Stand der Technik.
- Umfangreiche systemseitige Protokollierung von Datenweitergaben.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)/Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Server-Räume sind grundsätzlich mit Brandmeldeanlagen ausgestattet.
- Betrieb der Server in speziellen Sicherheitsräumen mit umfangreichen Schutzmaßnahmen (unterbrechungsfreie Stromversorgung (USV), Zutrittsschutz, Brandschottung, automatische Löschanlage, Brandmeldeanlage).

Beschreibung der bestehenden technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

- Permanentes, automatisches Monitoring aller wesentlichen Systeme.
- Umfangreiche mehrstufige Datensicherungsmaßnahmen.
- Schutz gegen unerlaubten Zugriff aus dem Internet und gegen Schadsoftware durch doppelte Firewall, Proxy-Server, Netzwerksegmentierung, Antivirensoftware, Zugriffsprotokollierung.
- Notfallmanagementsystem und Notfallpläne sind eingerichtet und werden regelmäßig getestet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 2 DSGVO)

4.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kunden verarbeitet werden können:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit).
- Alle Mitarbeiter und sonstige Personen, die Zugriff auf personenbezogene Daten haben, sind schriftlich zur Einhaltung des Datenschutzes verpflichtet.
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart.
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten.

4.2 Datenschutz-Management

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung:

- Regelmäßige und anlassbezogene Sensibilisierung der Mitarbeiter zum Datenschutz.
- Bewertung aller Prozesse in einem Verfahrensverzeichnis, das regelmäßig und anlassbezogen aktualisiert wird.
- Prozesse zur Behandlung und Meldung von potenziellen/tatsächlichen Datenschutzverletzungen eingerichtet und kommuniziert.

4.3 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen Zweck erforderlich ist, verarbeitet werden:

- Zugang zu Systemen und Applikationen durch persönliche Passwörter geschützt.
- Steuerung der Rechte der einzelnen Benutzer (Datenzugriffe, Funktionsumfang) durch dedizierte Rollen- und Berechtigungskonzepte. Mitarbeiter erhalten grundsätzlich nur Zugriff zu den Daten, die für die Arbeit benötigt werden.