Beschreibung der technischen und organisatorischen Maßnahmen

1. Allgemeine organisatorische Maßnahmen

Maßnahmen, die geeignet sind, eine Sensibilität für Datenschutz zu schaffen. Folgende allgemeine organisatorische Maßnahmen sind beim Auftragnehmer umgesetzt:

- Datenschutzbeauftragter wurde bestellt
- Beschäftigte erhalten Datenschutzschulung/-unterweisung (Art der Schulung: Präsenzschulung)
- Datenschutzschulungen werden wiederholt:
- Beschäftigte wurden/werden auf Betriebs-/Geschäftsgeheimnis verpflichtet
- Beschäftigte wurden/werden auf Datengeheimnis verpflichtet
- Beschäftigte unterschreiben Verschwiegenheitserklärung

---

2. Pseudonymisierung / Verschlüsselung

(Art. 32 Abs. 1 lit. a EU-DSGVO)

Maßnahmen, um den Schutz personenbezogener Daten zu gewährleisten, indem diese mittels Hilfsmechanismen in eine pseudonymisierte Form umgewandelt und verarbeitet werden oder mit einer dem Stand der Technik entsprechenden Verschlüsselung vor Zugriffen zu schützen:

- Speicherung erfolgt auf verschlüsselten Datenträgern und gesicherten Servern.
- Einsatz einer starken Verschlüsselung nach Stand der Technik (Bitlocker, FileVault)
- Verschlüsselte Speicherung personenbezogener Daten auf mobilen Datenträgern (Notebook, Smartphone, USB-Stick, etc.).

- Mobilgeräte (insbesondere Laptops) sind standardmäßig mit einer Festplattenverschlüsselung ausgestattet.
- Daten werden verschlüsselt an andere Bereiche oder Auftragsverarbeiter übertragen.
- Backups der Datenbank werden vor der Langzeitspeicherung AES-256 verschlüsselt.

---

3. Vertraulichkeit

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Maßnahmen, welche die Vertraulichkeit der Systeme und Dienste bei der Verarbeitung personenbezogener Daten sicherzustellen.

- **Angemessene Zugangskontrollen zu Gelände, Gebäude und Serverraum:**
  - Bereich kann nicht durch mehrere Türen unbemerkt verlassen werden (Notausgänge)
  - Sorgfältige Auswahl von Reinigungspersonal
  - Schließsystem zum Firmengelände/Büroräumen mit:
    - Schlüssel
    - Schlüsselausgabe wird protokolliert
  - Besucherregelung vorhanden
    - Besucher werden permanent in den Räumlichkeiten begleitet
- **Angemessene Datenträgerkontrollen:**
  - Führen einer Inventarliste sämtlicher Datenträger in der Infrastruktur
  - Regelmäßige Kontrolle, ob personenbezogene Datenspeicherung notwendig ist (Umfang und Zweck)
  - Ordnungsgemäße Vernichtung/Löschung von Daten/Datenträgern/Papier:
    - Physische Löschung von Datenträgern vor Wiederverwendung
    - Ordnungsgemäße Vernichtung von Papier (DIN 66399): Sicherheitsstufe P-4
- **Angemessene Benutzerverwaltung, sowie dediziertes Benutzer- und Berechtigungskonzept:**
  - Eindeutige Benutzerkennung
  - Zentrales Anlegen der Benutzer

- Beantragung im 4-Augen-Prinzip
- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Initialpasswort mit Änderungspflicht
- Schulung zu Passwörtern
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systeme
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert

- **Angemessene Benutzerkontrollmaßnahmen:**
  - Nur autorisierte Personen und Geräte erhalten Zugriff
  - Anwender müssen sich für Netzwerkanmeldungen authentifizieren
  - Es gibt ein gesichertes WLAN (mindestens WPA2):
  - Einsatz einer Software-Firewall
  - Regelmäßige Kontrolle der Firewall-Einstellungen
  - Fernwartungszugänge werden nur bei Bedarf freigegeben
  - Benutzerkonten von ausgeschiedenen Mitarbeitern werden unverzüglich gesperrt
  - Nutzung von privaten Mobilgeräten (u. a. Laptops, Tablet-PCs, Smartphones), z. B. im Rahmen einer Bring-Your-Own-Device-Regelung erlaubt
- **Sicherung bei Übermittlung personenbezogener Daten:**
  - Art der Sicherung der Daten zwischen Auftraggeber und Auftragnehmer: Verschlüsselung
- **Maßnahmen zur Auftragskontrolle**
  - Auswahl von Subauftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
    - Anhand der Vereinbarung zur Auftragsdatenverarbeitung
    - Anhand weiterer Dokumente: Standartvertragsklauseln, Privacy-Shield Zertifizierung
    - Dokumentation der Eignung ist einsehbar
  - Verträge mit den Dienstleistern enthalten:
    - Es gibt zu jedem Dienstleister eine Vereinbarung nach Art. 28 EUDSGVO
    - Es sind weitere Subdienstleister genehmigungspflichtig

- Auftragnehmer hat Datenschutzbeauftragten bestellt

Es sind Dienstleister im Einsatz für:

- Telefonanlage
- Lohnbuchhaltung

- **Weitere Maßnahmen der Zweckbindung/des Trennungsgebots:**
  - Festlegung von Datenbankrechten

---

4. Integrität

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Maßnahmen, die die Integrität der verarbeiteten personenbezogenen Daten sicherstellen.

- Fernwartungszugänge werden nur bei Bedarf freigegeben
- Auswahl von Subauftragnehmern unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- **Maßnahmen zur Trennbarkeit**
  - Trennung von Produktiv- und Testsystem
  - Festlegung von Datenbankrechten

---

5. Verfügbarkeit

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Maßnahmen und Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

- **Maßnahmen zur Gewährleistung der Verfügbarkeit**
  - Erstellen eines Backup- & Recoverykonzepts
  - Umfang der Sicherung:
    - Datenbanken
    - Fileserver
  - Art der Sicherung:
    - Band

        - Festplatte
        - Auf einem anderen System
- **Maßnahmen zur Wiederherstellbarkeit**
    - Notfallpläne vorhanden / gepflegt
    - Testen von Datenwiederherstellung, Häufigkeit: jährlich
- **Maßnahmen zur Verfügbarkeitskontrolle**
    - Unterbrechungsfreie Stromversorgung (USV) ist installiert
    - Klimaanlage in Serverräumen
    - Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
    - Aufbewahrung von Datensicherung:
        - an einem sicheren, ausgelagerten Ort (Art der Datenübertragung: digital, verschlüsselt)
    - Nutzung von Cloud-Services
        - Amazon Cloud
        - Google-Docs

---

6. Belastbarkeit der Systeme

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Gewährleistung, dass IT-Systeme auch unter hoher Inanspruchnahmefrequenz ordnungsgemäß funktionieren (Performanz). Die Belastbarkeit der IT-Systeme ist grundlegend für die Aufrechterhaltung des Geschäftsbetriebs, also für die Business Continuity. In der englischen Fassung wird von „resilience“ gesprochen, so dass hier eher/auch die Begriffe Resilienz bzw. Widerstandsfähigkeit der Systeme bzw. Dienste gemeint sind.

Maßnahmen, welche die Belastbarkeit von Systemen und Diensten sicherstellen sollen:

- **Maßnahmen zur Belastbarkeit**
    - redundante WAN-Anschlüsse
    - Multi-Channel-Bonding (z.B. UMTS/LTE/Glasfaser/Kupfer)
    - Ausreichende Dimensionierung der Storage-Systeme
    - Ausreichende Dimensionierung der Arbeitsspeicher
    - Monitoring der Systeme

- Monitoring des Netzwerks
- Ausfallraten-Statistik
- Verfügbarkeits-Statistik
- Ticketsystem
- Mit Dienstleistern abgeschlossene Service-Level-Agreements (SLA)
- Unterbrechungsfreie Stromversorgung (USV) ist installiert
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Ausreichende Dimensionierung der Storage-Systeme
- Ausreichende Dimensionierung der Arbeitsspeicher

---

7. Verarbeitung auf Dauer

(Art. 32 Abs. 1 lit. b EU-DSGVO)

Maßnahmen, die sicherstellen, dass eine Verarbeitung auf Dauer integer gewährleistet wird und andererseits die Dauer der Verarbeitung nicht überschritten wird.

- Monitoring der Systeme
- Monitoring des Netzwerks
- Datensicherungsformate ermöglichen langfristige Sicherung und Rücksicherung
- Changemanagement vorhanden; Updates werden bspw. nur nach vorherigem Test eingespielt

---

8. Wiederherstellbarkeit

(Art. 32 Abs. 1 lit. c EU-DSGVO)

Maßnahmen, die sicherstellen, dass Systeme und Dienste zur Verarbeitung personenbezogener Daten im Störungsfall wiederhergestellt werden können.

- Backup-Prozeduren nach Kategorisierung und Ressourcen vorhanden.
- Erreichbarkeit von Administratoren geregelt (ggf. Rufbereitschaft)
- Vorhandensein von Ausweichrechenzentren (Hot site, warm site, cold site):
- Mit Dienstleistern abgeschlossene Service-Level-Agreements (SLA).

---

9. Speicherbegrenzung

(Art. 5 Abs. 1 lit. e EU-DSGVO)

Gewährleistung, dass personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“)

Folgende Maßnahmen der Speicherbegrenzung sind beim Auftragnehmer umgesetzt:

- Vorliegen Löschkonzept (insbesondere für CRM- und ERP-Systeme)
- Nachweis der Datenlöschung durch Systemprotokolle

---

10. Regelmäßige Evaluation der Wirksamkeit

(Art. 32 Abs. 1 lit. d EU-DSGVO)

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Folgende Maßnahmen zur regelmäßigen Evaluation der Wirksamkeit sind beim Auftragnehmer umgesetzt:

- Auswertung von Vorfällen
- Auswertung und Umsetzung von Verbesserungsvorschlägen
- Überprüfung der Managementsysteme durch die Geschäftsführung
- Überprüfung durch den DSB (mit Bericht)