Anlage 1

Technische und organisatorische Schutzmaßnahmen gemäß Art. 32 DS-GVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft die PROWIS Automatisierung GmbH nachfolgend dargelegte technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die dargestellten Maßnahmen sind Maßnahmen innerhalb der Organisation der PROWIS Automatisierung GmbH. Einige der dargestellten Maßnahmen wirken ausschließlich innerhalb der Organisation der PROWIS Automatisierung GmbH und haben bei der Erbringung von technischen oder softwaretechnischen Dienstleistungen beim Auftraggeber vor Ort keine Relevanz.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**

  Arbeitsbereich:
  Sicherheitsschlösser; Schlüsselregelung (Schlüsselausgabe etc.); Personenkontrolle beim Empfang; Begleitung des Besuchers durch Mitarbeiter; Sorgfältige Auswahl von Reinigungspersonal

  Serverraum:
  Sicherheitsschlösser; Protokollierung der Zutritte; Begleitung des Wartungsarbeiters durch Mitarbeiter

  Besucherregelung:
  Begleitung des Besuchers durch Mitarbeiter; Trennung von Bearbeitungs- und Publikumszonen; Personenkontrolle beim Empfang

- **Zugangskontrolle**:

  Verwaltungssystem:
  Acitive Directory -Benutzerverwaltung

  Identifikation/Authentifizierung:

  Erstellen von Benutzerprofilen; Zentrales anlegen des Benutzers; Zuordnung von

Benutzerrechten; Authentifikation mit Benutzername / Passwort; Passwortvergabe durch den Benutzer; Schulung zu Passwortanwendung; Sperre ausgeschiedener Beschäftigter; Automat. Bildschirmschoner

Technischer Zugangsschutz:

Viren-Scanner für Server; Viren-Scanner für Clients; Einsatz von VPN-Technologie und TLS 1.2-Technologie; Einsatz einer Hardware-Firewall; Verschlüsselung von W-LAN; Einsatz einer Software-Firewall; Verschlüsselung von Datenträgern in Laptops / Notebooks; Fernwartungszugriffe nur durch Bestätigungscode oder Kundenfreigabe

- **Zugriffskontrolle**

Erstellen eines Berechtigungskonzepts; Verwaltung der Rechte durch Systemadministrator; Rechtevergabe benutzerspezifisch nach Aufgabe; Regelmäßige Überprüfung des Berechtigungssystems; Anzahl der Administratoren auf das „Notwendigste“ reduziert; Passwortrichtlinie inkl. Passwortlänge; Passwortwechsel; Sichere Aufbewahrung von Datenträgern; physische Löschung von Datenträgern vor Wiederverwendung; ordnungsgemäße Vernichtung von Datenträgern; Einsatz von Aktenvernichtern bzw. Dienstleistern; Protokollierung der Vernichtung; Verschlüsselung von Datenträgern; Fernwartungszugriffe nur durch Bestätigungscode oder Kundenfreigabe

- **Trennungskontrolle**

Trennung durch Berechtigungssystem; Eigenständige Datenbank; Trennung von Produktiv- und Testsystem; Mandantenfähigkeit

- **Pseudonymisierung und Verschlüsselung**

Anlassbezogene softwarebasierte Verschlüsselung bei Datenspeicherung; Anlassbezogene hardwarebasierte Verschlüsselung bei Datenspeicherung

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**

Einrichtungen von Standleitungen bzw. VPN-Tunneln; E-Mail-Verschlüsselung; Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger; Transportsicherung; Datenschutzgerechte Entsorgung Papierdokumente mit Papiertonne/Schredder mit der Sicherheitsstufe 3; Protokollierung; Beim physischen Transport: sorgfältige Auswahl von

Transportpersonal und –Fahrzeugen

- **Eingabekontrolle**
  Protokollierung der Eingabe; Änderung und Löschung von Daten auf Feldebene in Anwendungsprogrammen; Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen; Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes,

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**

  Unterbrechungsfreie Stromversorgung (USV); Klimaanlage in Serverräumen; Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen; Schutzsteckdosenleisten in Serverräumen; Feuer- und Rauchmeldeanlagen; Feuerlöschgeräte für Serverräum; Einsatz von Virtualisierungstechnologie; Erstellen eines Backup- & Recoverykonzepts; Testen von Datenwiederherstellung; Erstellen eines Notfallplans; Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort; Serverräume nicht unter sanitären Anlagen; Virenschutz / Firewall; Spiegeln von Festplatten, z.B. RAID-Verfahren

- **Belastbarkeitskontrolle**
  Die Verarbeitung der Daten soll tolerant gegenüber Störungen und Fehlern sein.

  Virenschutz/Anti-Malware/Anti-Ransomware; großzügig vorhandene Netzwerkkapazität; gehärtete Hardware gegen insbesondere DoS- und DDoS-Angriffe; IDS/IPS; geeignete Systemarchitektur/DMZ; Firewall

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

- Schriftlich fixierte Regelungen der Verantwortlichkeiten für Datenschutz
- Schriftlich fixierte Regelungen der Verantwortlichkeiten für Informationssicherheit
- Existenz eines angemessenen Informationssicherheitsmanagements
- Existenz eines angemessenen Incident Response Managements z.B. Ticketsystem
- Durchführung einer Informationsklassifizierung
- Regelmäßige Aufklärung und Sensibilisierung der Mitarbeiter und Führungskräfte
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle, um weisungsgemäße Auftragsverarbeitung zu gewährleisten:
  - Strikte Einhaltung der im vorliegenden Auftragsverarbeitungs-Vertrag festgeschriebenen Vereinbarungen und diesbezügliche Überprüfungen

- Konzept dahingehend, wie die regelmäßige Kontrolle des Auftragsprozesses erfolgt (z.B. Vorlage von Self-Assessments, Vorlage der Verträge mit Unterauftragnehmern, Durchführung von Kontrollen bei Subunternehmern durch den Auftragnehmer)
- Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z. B. anhand: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.