Anhang 1

Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers:

Name Auftragnehmer _____

Postanschrift _____

Name Datenschutzbeauftragter _____

Telefon _____

Telefax _____

E-Mail _____

Technische und organisatorische Maßnahmen zur Daten- und IT-Sicherheit

1. Vertraulichkeit der IT-Systeme und Datenverarbeitung (Art. 32 Abs. 1 lit. b) DSGVO)

a) Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ☐ personalisiertes elektronisches Zutrittskontrollsysteme: Ausweisleser, Magnetkarte, Transponder, Chipkarte etc. bzw. Schlüssel / Schlüsselvergabe
- ☐ bauliche Schutzmaßnahmen zur Außen- und Innensicherung der Gebäude, des Rechenzentrums und sonstiger Räume bzw. Sicherheitszonen, wie z. B. Schranken, Vereinzelungsanlagen, Sicherheitsschlösser, Türsicherungen, Fenstersicherungen etc.
- ☐ Gebäudeüberwachung und Überwachung der Sicherheitszonen durch geschultes Personal, wie z. B. Werksschutz, Pförtner etc.
- ☐ Zutrittsregelungen für externe Personen; Begleitung betriebsfremder Personen durch Mitarbeiter oder den Werksschutz, Wachdienst etc.
- ☐ Überwachungseinrichtungen, wie z. B. Alarmanlagen, Videoüberwachung etc.
- ☐ Mehrfach-Zutrittsschutz (z. B. Zutrittskarte zzgl. Token oder Zahlenschloss ggf. zzgl. mechanischem Schloss) für besonders sensible Zonen (z. B. Server, Telekommunikationsanlage, Netzwerkknoten, Backups etc.)
- ☐ Sonstiges: _____

b) Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (insbesondere technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung).

- ☐ Einrichtung eines Benutzerstammsatzes pro User
- ☐ Identity-Management-System zur Administration der Berechtigungen für die Systeme
- ☐ Zwei-Faktor-Authentifizierung
- ☐ Automatische oder manuelle Sperrung der Systeme (z. B. Pausenschaltungen, Bildschirmsperren etc.)
- ☐ Verschlüsselung von Datenträgern
- ☐ Kennzeichnung eigener und fremder Datenträger, separate Aufbewahrung etc.

- ☐ Sicherheitsrichtlinien (Berechtigungsvergabe, Passwortsicherheit, Netzwerksicherheit, Sicherheit der Serversysteme, Sicherheit der Arbeitsplatzrechner, Datensicherheit etc.)
- ☐ Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- ☐ Sonstiges: _____

c) Zugriffskontrolle

Maßnahmen, die geeignet sind zu gewährleisten, 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, verändert oder entfernt werden können.

- ☐ Einrichtung, Pflege und Kontrolle differenzierter Berechtigungen (Nutzerprofile, Rollen, Transaktionen und Objekte)
- ☐ Die Verarbeitung und Nutzung von personenbezogenen Daten ist ausschließlich im Rahmen der zugewiesenen Berechtigungen / Nutzerprofile möglich
- ☐ Einrichtung von Berechtigungen / Nutzerprofils nur für berechtigte Personen und nur nach eindeutiger Identifizierung dieser Person
- ☐ Verwaltung der erlaubten Zugriffsberechtigungen im Berechtigungskonzept / in den Nutzerprofilen
- ☐ Regelmäßige Kontrollen der Zugriffsberechtigungen
- ☐ Einsatz von Verschlüsselungsverfahren bei Systemen
- ☐ Protokollierungen von Auswertungen, Kenntnisnahmen, Veränderungen, Löschungen etc.
- ☐ Sonstiges: _____

d) Trennungskontrolle

Maßnahmen, die geeignet sind zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☐ Maßnahmen der physikalischen Trennung der Daten, z. B. Speicherung auf getrennten Servern, Datenträgern etc.
- ☐ Maßnahmen der logischen Trennung der Daten, z. B. softwareseitige Mandantentrennung; Dateiseparierung bei Datenbankprinzip; Zugriff auf Datensätze nur über Anwendungen, in der die Logik festgelegt wurde; Berechtigungskonzept mit Zugriffsregelungen; Festlegung von Rollen; unterschiedliche Verschlüsselung der Datensätze; Versehen der Datensätze mit Attributs-Signaturen etc.
- ☐ Sandboxing
- ☐ Trennung von Testdaten und produktiven Daten
- ☐ Sonstiges: _____

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a) DSGVO; Art. 25 Abs. 1 DSGVO)

Maßnahmen, die geeignet sind zu gewährleisten, dass die personenbezogenen Daten in einer Weise verarbeitet werden, 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.

- ☐ Einsatz von sicheren und wirksamen Pseudonymisierungsverfahren
- ☐ Sonstiges: _____

2. Integrität der IT-Systeme und Datenverarbeitung (Art. 32 Abs. 1 lit. b) DSGVO)

a) Weitergabekontrolle

Maßnahmen, die geeignet sind zu gewährleisten, 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 welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ☐ Leitungen, Anschlüsse und Verteiler für die Datenfernübertragung in den Betriebsstätten liegen in nicht frei zugänglichen Sicherheitsbereichen
- ☐ Datenübertragungen laufen über gemietete Leitungen eines privaten Netzbetreibers; durch Filtermaßnahmen und Authentifizierungsmechanismen auf den Netzwerk-Komponenten sind die betriebenen Systeme vor Aufbau unberechtigter Datenfernübertragungsverbindungen geschützt
- ☐ Verschlüsselungsverfahren, Tunnelverbindungen (VPNs) etc.
- ☐ Festlegung und Dokumentation der Empfänger personenbezogener Daten, der Übertragungsverfahren und -wege
- ☐ Dokumentation der Abruf- und Übermittlungsprogramme
- ☐ elektronische Signaturen
- ☐ Protokollierungen der Datenübermittlungen, Empfänger etc.
- ☐ Abschottung der Systeme durch mehrstufige Firewalls
- ☐ mehrstufiges Virenschutzkonzept (Ports, Server, Arbeitsplatzrechner etc.)
- ☐ Sonstiges: _____

b) Weitergabekontrolle

Maßnahmen, die geeignet sind zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- ☐ Protokollierungs- und Protokollauswertungssysteme
- ☐ Sonstiges: _____

3. Verfügbarkeit, Belastbarkeit und rasche Wiederherstellbarkeit der IT-Systeme und Datenverarbeitung (Art. 32 Abs. 1 lit. b) und lit. c) DSGVO)

Maßnahmen, die geeignet sind zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, dass IT-Systeme belastbar sind und dass IT-Systeme und personenbezogene Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können

- ☐ Verteilung aller geschäftskritischen IT-Infrastruktur-Services auf verschiedene redundante Rechenzentren
- ☐ Getrennte Speicherung / Aufbewahrung von personenbezogenen Daten, z. B. in verschiedenen Brandabschnitten
- ☐ Hochverfügbarkeits-Maßnahmen
- ☐ Backup-Verfahren

- ☐ Spiegeln von Festplatten, z. B. RAID-Verfahren
- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Überspannungsschutz
- ☐ Wirksame Klimakontroll-Maßnahmen
- ☐ Firewall-Schutz
- ☐ Richtlinie zum Business Continuity Management (BCM)
- ☐ Notfallplan
- ☐ Sicherheitsrichtlinie
- ☐ Schulung der Mitarbeiter hinsichtlich Sicherheitsmaßnahmen
- ☐ Regelmäßige Tests der Rechenzentren auf Ausfallsicherheit, Hochverfügbarkeit etc.
- ☐ Sonstiges: _____

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

Verfahren und Maßnahmen, die geeignet sind zu gewährleisten, dass die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Sicherstellung der Daten- und IT-Sicherheit regelmäßig überprüft, bewertet und evaluiert werden

- ☐ Verfahren gemäß § 6 Abs. 3 dieser Vereinbarung zur regelmäßigen Überprüfung, Bewertung und Dokumentation der Umsetzung und Einhaltung der festgelegten technischen und organisatorischen Maßnahmen nach Anhang 3 zu dieser Vereinbarung und deren Wirksamkeit zur Gewährleistung der Daten- und IT-Sicherheit gemäß Art. 32 DSGVO
- ☐ Datenschutz-Compliance-Management-System
- ☐ Datenschutzrichtlinien
- ☐ Privacy by Design-Richtlinien
- ☐ Incident-Response-Management
- ☐ Maßnahmen der Auftragskontrolle, wie z. B. Kontrolle der Vertragsausführung, insbesondere mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere die Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags; eindeutige Vertragsgestaltung; strenge Auswahl der Subunternehmer etc.
- ☐ Sonstiges: _____

Anhang 2 - Subunternehmer

Kontaktdaten des Subunternehmers:

Name Subunternehmer _____

Postanschrift _____

Name Kontaktperson _____

Telefon _____

E-Mail _____

Kontaktdaten des Subunternehmers:

Name Subunternehmer _____

Postanschrift _____

Name Kontaktperson _____

Telefon _____

E-Mail _____

Kontaktdaten des Subunternehmers:

Name Subunternehmer _____

Postanschrift _____

Name Kontaktperson _____

Telefon _____

E-Mail _____

Kontaktdaten des Subunternehmers:

Name Subunternehmer _____

Postanschrift _____

Name Kontaktperson _____

Telefon _____

E-Mail _____