Anlage 1

Beschreibung der personenbezogenen Daten / Datenkategorien und Beschreibung der Kategorien Betroffener Personen

1. Verarbeitete Datenarten/-kategorien

Folgende Datenarten oder Kategorien von Daten sind Gegenstand der Auftragsverarbeitung
(Zutreffendes bitte ankreuzen, nicht aufgelistete Datenarten und Kategorien ergänzen)

- ☐ Personenstammdaten (z.B. Vorname und Nachname)
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Adressdaten
- ☐ IP-Adresse
- ☐ Bewerberdaten (z.B. Zeugnisse, Zertifikate, Referenzen)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Kundenhistorie
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ☐ Bankdaten
- ☐ Kreditkartendaten
- ☐ Zeiterfassungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ IT-Daten (z.B. IT-Benutzernamen, Logdateien, Zugriffsrechte)
- ☐ Support-Ticket-Daten (z.B. Help-Desk- oder Kundensupport-Ticket-System)
- ☐ biometrische Daten (z. B. auch **Fotos**)
- ☐ Gesundheitsdaten (z. B. **Krankenstand, Schwangerschaft**)
- ☐ Religions- und Gewerkschaftszugehörigkeit
- ☐ sonstiges

2. Beschreibung der Kategorien betroffener Personen

Folgende Kategorien von Personen (Inhaber/Eigentümer der Daten) sind von der Auftragsverarbeitung betroffen
(Zutreffendes bitte ankreuzen, nicht aufgelistete Kategorien von Personen ergänzen)

- ☐ Kunden
- ☐ Ansprechpartner
- ☐ Interessenten
- ☐ Abonnenten
- ☐ Handelsvertreter
- ☐ Lieferanten
- ☐ Beschäftigte (Art. 88 DSGVO; § 26 Abs. 8 BDSG-2018)
- ☐ Minderjährige
- ☐ ehemalige Beschäftigte
- ☐ Bewerber
- ☐ sonstiges

3. Umfang, Art und Zweck der Verarbeitung von personenbezogenen Daten

Folgende Leistungen werden im Rahmen der Auftragsverarbeitung erbracht
(Bitte Leistungen auflisten)

Anlage 2
Technische und organisatorische Maßnahmen des Auftragnehmers

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

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen ist zu reduzieren.

>> Zutrittskontrolle

Technische und organisatorische Maßnahmen:

- Alarmanlage
- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder- oder manuelles Schließsystem
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal

> Zugangskontrolle

Technische und organisatorische Maßnahmen:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Schlüsselregelung (Schlüsselausgabe etc.)
- Sorgfältige Auswahl von Reinigungspersonal
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall bei allen mobilen Arbeitsplätzen

> Zugriffskontrolle

Technische und organisatorische Maßnahmen:

- Erstellen eines Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

> Trennungskontrolle

Technische und organisatorische Maßnahmen:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystem

> Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Technische und organisatorische Maßnahmen:

- Im Rahmen der Dienstleistungserbringung, treffen wir zusätzlich zu Maßnahmen die durch den Verantwortlichen im Rahmen der Beauftragung vorgenommen werden, keine weiteren Maßnahmen zur Pseudonymisierung."

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

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren.

>> Weitergabekontrolle

Technische und organisatorische Maßnahmen:

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

>> Eingabekontrolle

Technische und organisatorische Maßnahmen

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Nichtverfügbarkeit von im Auftrag verarbeiteten Daten ist zu reduzieren.

>> Verfügbarkeitskontrolle

Technische und organisatorische Maßnahmen:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen

>> Belastbarkeit der Systeme

Technische und organisatorische Maßnahmen:

- Skalierende Systeme
- Denial of Service - Abwehrtechniken,
- RAID-Systeme
- Virenschutz
- Firewall.

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

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

>> Auftragskontrolle

Technische und organisatorische Maßnahmen:

- Es wird keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen durchgeführt.

>> Innerbetriebliche Organisation

Technische und organisatorische Maßnahmen:

a. <u>Datenschutzmanagement</u>

- Nur Mitarbeiter die auf die Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet wurden, dürfen die für ihren Aufgabenbereich entsprechenden Daten verarbeiten
- Es existieren interne Verhaltensrichtlinien sowie ein Datenschutz Handbuch
- Alle Mitarbeiter werden in regelmäßigen Abständen (min. Jährlich) zum Thema Datenschutz per E-Learning geschult und sensibilisiert.
- In einem Organigramm sowie in Stellenbeschreibungen sind Verantwortlichkeiten und Befugnisse der einzelnen Mitarbeiter festgelegt und im Unternehmen bekannt gemacht.
- Dieses wird in regelmäßigen Abständen von der obersten Leitung im Rahmen der ISO 9001 Zertifizierung überprüft.

b. <u>Störfallmanagement</u>

- Die Einhaltung der technisch- organisatorischen Maßnahmen werden jährlich (Audit) durch den Datenschutzbeauftragten überprüft und gegebenenfalls angepasst.

c. <u>Datenschutzes durch Technikgestaltung</u>

- Auswahl datenschutzfreundlicher Technologie

Anlage 3
Genehmigte Subunternehmer

Bei den folgenden Unternehmen handelt es sich um genehmigte Subunternehmer:

Anschrift des Subunternehmers	**Kontakt**	**Länder, in denen Daten verarbeitet werden**
Pascalstr. 10 10587 Berlin	Strato AG	Deutschland
Hafenstraße 32 48153 Münster	Raidboxes GmbH	Deutschland
South County Business Park, One Microsoft Place Carmanhall and Leopardstown Dublin, D18 P521	Microsoft Ireland	Irland
Am Beuel 4 51570 Windeck	One-A-Communication GmbH	Deutschland
Wilhelminenstr. 36 64285 Darmstadt	Martin Gerwens Consulting GmbH	Deutschland
Am Gierath 20d 40885 Ratingen	bluvo GmbH -Teil der teccle group	Deutschland

Anlage 4

Weisungsberechtigte und Weisungsempfänger sowie Kontaktdaten der Datenschutzbeauftragten

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner die Nachfolger bzw. die Vertreter mitzuteilen.
(Bitte Daten eintragen):

1. Weisungsberechtigte und Weisungsempfänger

(Auftraggeber)

Name	Telefon	E-Mail

(Auftragnehmer)

Name	Telefon	E-Mail

2. Datenschutzbeauftragter

(Auftraggeber)

Name	Telefon	E-Mail

(Auftragnehmer)

Name	Telefon	E-Mail
Stephan Hartinger Coseco GmbH	08232 80988-70	datenschutz@coseco.de