Anlage 3 - Technische und organisatorische Maßnahmen

Die hier beschriebenen technischen und organisatorischen Maßnahmen entsprechen dem aktuellen Stand der Software-Driven UG. Das Unternehmen befindet sich im Prozess der Erstellung eines Datenschutzkonzeptes.

Vertraulichkeit

Zutrittskontrolle

Speicherung und/oder Verarbeitung von personenbezogenen Daten des Auftraggebers

☐ In den Büroräumen des Auftragnehmers

☐ Im Rechenzentrum bzw. in Serverräumen des Auftragnehmers

☒ Bei folgendem IT-Dienstleister (z.B. Cloud-Anbieter): Hetzner Online GmbH

Oder

☐ Nicht zutreffend

Gebäude sind mit folgenden Maßnahmen gesichert

	Alarmanlage	Videoüberwachung	Sonstiges	Nicht zutreffend
Bürogebäude	☐	☐	Klicken oder tippen Sie hier, um Text einzugeben.	☒
Rechenzentrum	☒	☒	Siehe TOMs bei Hetzner	☐

Zutritt zu den Räumlichkeiten ist mit folgenden Maßnahmen gesichert

	Manuelle Schließanlage	Chipkarten-zugangssystem	Sonstiges	Nicht zutreffend
Bürogebäude	☐	☐	Klicken oder tippen Sie hier, um Text einzugeben.	☒
Serverräume	☐	☒	Siehe TOMs bei Hetzner	☐
Rechenzentrum	☐	☒	Siehe TOMs bei Hetzner	☐

Dokumentation der Zutrittsberechtigungen erfolgt namensscharf

☒ Ja ☐ Nein ☐ Nicht zutreffend

Regelungen zum Gebäudezutritt von Firmenfremden/Gästen/Besuchern

	Namensscharfe Dokumentation		Zutritt und Aufenthalt nur in Begleitung von Aufsichtspersonal	Nicht zutreffend
	Ja	Nein		
Bürogebäude	☐	☐	☐	☒
Serverräume	☐	☐	☒	☐
Rechenzentrum	☐	☐	☒	☐

Regelungen zum Gebäudezutritt von Reinigungs- und Wartungspersonal

	Namensscharfe Dokumentation: Ja	Namensscharfe Dokumentation: Nein	Zutritt und Aufenthalt nur in Begleitung von Aufsichtspersonal	Nicht zutreffend
Bürogebäude	☐	☐	☐	☒
Serverräume	☐	☐	☒	☐
Rechenzentrum	☐	☐	☒	☐

Regelungen bzgl. der Entziehung von Gebäudezutrittsberechtigungen und Zugriffsrechten zu Computersystemen inkl. Dokumentation für Mitarbeiter bei Beendigung des Arbeitsverhältnisses

☒ Ja ☐ Nein

Zugangskontrolle

Firmennetzwerk ist gegen das öffentliche Netzwerk durch eine Firewall geschützt

☐ Ja ☒ Nein

Wenn ja:

Typ: Kein Firmennetzwerk

Aktualisierungsverfahren und -häufigkeit: BITTE ERGÄNZEN

Regelmäßige Penetrationstests aller zum Internet geöffneten IP-Adressen durchgeführt

☐ Ja ☒ Nein

Mitarbeiter werden auf folgende Passwortvorgaben verpflichtet

☒ Individuell geheim zu haltendes Computerkennwort für jeden Mitarbeiter

☒ Mindestlänge, wenn zutreffend (Anzahl Zeichen/Komplexität): 8-16 Zeichen, Klein- und Großbuchstaben, Zahlen und Symbole

☐ Wechselrhythmus, wenn zutreffend: BITTE ERGÄNZEN

☒ Automatische Verriegelung des Bildschirms nach: 5 Min.

An folgenden Übergängen zum Firmennetz werden Virenscanner eingesetzt

☐ E-Mail-Account ☐ FTP ☐ Web

Virenscanner auf allen Servern

☐ Ja Aktualisierungsverfahren und -häufigkeit: BITTE ERGÄNZEN

☒ Nein Angabe von Betriebssystem und Begründung: ausschließlich Ubuntu Linux LTS 22.04, Einschätzung BSI (BSI-CS 009 | Version 2.0 vom 11.07.2018): "Die Installation eines Virenschutzprogramms ist, basierend auf dem aktuellen Stand der Bedrohungslage in Bezug auf Schadsoftware für Linux, unter Ubuntu nicht notwendig."

☐ Nicht zutreffend Trifft nicht zu, weil: BITTE ERGÄNZEN

Virenscanner auf allen Einzelarbeitsplatzcomputern

☒ Ja Aktualisierungsverfahren und -häufigkeit: Automatische Sicherheitsupdates des Herstellers

☐ Nein Angabe von Betriebssystem und Begründung: BITTE ERGÄNZEN

☐ Nicht zutreffend Trifft nicht zu, weil: BITTE ERGÄNZEN

Sicherheitsrelevante Updates werden regelmäßig und automatisiert in die vorhandene Software eingespielt

☒ Ja ☐ Nein

Mitarbeiter mit lokalen Administrationsrechten auf Einzelarbeitsplatzcomputer

	Ja	Nein
Administratoren, Entwickler, Techniker	☒	☐
Anwender	☐	☒

Mitarbeiter haben Internetzugangsberechtigung

☒ Ja ☐ Nein

Wenn ja:

restriktive, von Mitarbeitern nicht änderbare Browserkonfiguration eingerichtet

☐ Ja ☒ Nein ☐ Nicht zutreffend

Zugriffskontrolle

Berechtigungskonzepte vorhanden und dokumentiert

☒ Ja ☐ Nein

Organisation der Berechtigungsvergabe wird namensscharf dokumentiert (insb. wer darf welche Rechte vergeben)

☒ Ja ☐ Nein

Berechtigungen werden nach dem Need-To-Know-Prinzip vergeben und namensscharf aktualisiert und dokumentiert

☒ Ja ☐ Nein

Anzahl der Administratoren mit Berechtigung, Datenbestände des Auftraggebers ganz oder in großen Mengen zu kopieren/extrahieren

2

Anzahl Mitarbeiter (keine Administratoren!) mit Berechtigung, Datenbestände des Auftraggebers ganz oder in großen Mengen zu kopieren/extrahieren

0

Formate, in denen der Export erfolgen kann (csv, xlsx etc.)

Klicken oder tippen Sie hier, um Text einzugeben.

Komponenten der Arbeitsplatzcomputer wurden verriegelt/deaktiviert, damit keine Datenexporte extern gespeichert werden können

☐ USB-Ports

☐ CD-/DVD-/Blu-ray-Brenner

☐ Speicherkartenslots

☐ andere mobile Datenträger, wenn zutreffend, welche: BITTE ERGÄNZEN

Oder

☒ Es erfolgte keine Deaktivierung von Komponenten

Fernwartungs-/Fernzugriffszugänge sind vorhanden für

☐ weitere Dienstleister

☒ Mitarbeiter

Oder

☐ Es sind keine Fernwartungs-/Fernzugriffszugänge vorhanden

Wenn Fernwartungs-/Fernzugriffszugänge vorhanden sind, bitte folgende Angaben ergänzen

Art der Authentisierung (z.B. Passwort, oder PIN und Token)	Passwort oder Zertifikat
Bei Passwort Authentisierung (nur bei Abweichungen zu Passwort-Policy)	siehe oben
Verwendete Protokolle bzw. Mechanismen (z.B.: SSH, VPN, RDP)	SSH, SFTP bzw. SCP
Zusätzliche Sicherheitsmaßnahmen (z.B. individuelle Sitzungsfreigabe)	keine

Beim Auftragnehmer existieren Regelungen für mobiles Arbeiten (z.B. im Home-Office), um Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Datenverarbeitung sicherzustellen

☒ Ja ☐ Nein ☐ Nicht zutreffend

Unterweisung der Mitarbeiter zum mobilen Arbeiten inkl. namensscharfer Dokumentation erfolgt

☒ Ja ☐ Nein ☐ Nicht zutreffend

Trennungskontrolle

Separierung der Daten des Auftraggebers

☐ eigener, extra für den Auftrag vorgesehener Mandant

☐ netzwerktechnische Separierung durch folgende Maßnahmen: Klicken oder tippen Sie hier, um Text einzugeben.

Oder

☒ Nicht zutreffend

Es besteht ein Berechtigungskonzept für vorgenannte Mandanten bzw. Netzwerksegmente, das den Datenzugriff von Mitarbeitern ausschließt, die nicht für den Auftraggeber tätig sind

☐ Ja ☐ Nein ☒ Nicht zutreffend

Mitarbeiter werden schriftlich dazu verpflichtet, Informationen aus Datenbeständen des Auftraggebers nicht in andere Projekte/Zwecke mit einzubringen

☒ Ja ☐ Nein ☐ Nicht zutreffend

Integrität

Weitergabekontrolle

Daten, die mittels Datenträger (Papierdokumente, Festplatten, USB-Sticks, CDs etc.) zwischen Auftraggeber und Auftragnehmer übermittelt werden

Die per digitalem Datenträger übermittelten Daten werden verschlüsselt

☐ Ja ☐ Nein ☒ Nicht zutreffend

Wenn ja:

Verfahren bitte erläutern: BITTE ERGÄNZEN

Rückmeldeverfahren an den Auftraggeber bei Erhalt oder vermutetem Verlust: BITTE ERGÄNZEN

Oder

☒ kein Einsatz von Datenträgern

Daten, die auf elektronischem Wege zwischen Auftraggeber und Auftragnehmer übermittelt werden

Eingesetzte Verschlüsselungsart für Datenaustausch

☐	SFTP	
☐	S/MIME	
☒	HTTPS (z.B. Web-Schnittstelle, Cloud-Speicher), bitte erläutern	Web-Schnittstelle zur Nutzung des Bildungsangebots
☐	SSL-VPN oder Citrix, bitte erläutern	BITTE ERGÄNZEN
☐	Sonstige, Verfahren bitte erläutern	BITTE ERGÄNZEN

Oder

☐ keine elektronische Übermittlung von Daten

Speicherung personenbezogene Daten des Auftraggebers beim Auftragnehmer

☐ Ja, verschlüsselt ☒ Ja, unverschlüsselt ☐ Nicht zutreffend

Wenn Daten verschlüsselt gespeichert werden:

Erläuterung des Verfahrens: BITTE ERGÄNZEN

Schutz der in Backups enthaltenen Daten des Auftraggebers (gesicherte Aufbewahrung der Backupmedien, Verschlüsselung der Backups, etc.)

Erläuterung der Maßnahmen: Tägliche automatische Backups im Hetzner-Rechenzentrum

Oder

☐ keine Backups von Daten des Auftraggebers

Löschung der Daten des Auftraggebers

	Art der Löschung (Standard/Norm)	Lösch-/Entsorgungsfrist	Lösch-/Entsorgungsdokumentation
Elektronische Daten im System	siehe Löschkonzept	siehe Löschkonzept	siehe Löschkonzept
Elektronische Datenträger	nicht zutreffend	nicht zutreffend	nicht zutreffend
Papierdokumente	nicht zutreffend	nicht zutreffend	nicht zutreffend

Schutz von Daten (auch temporären) des Auftraggebers auf mobilen Geräten

	Maßnahmen (ggfs. Details zur Verschlüsselung angeben)	Keine Maßnahmen	Nicht zutreffend
Mobile Arbeitsplatzrechner, Datenträger etc. (Sichtschutzfolie auf Bildschirmen, Verschlüsselung etc.)	BITTE ERGÄNZEN	☐	☒
Smartphones, Tablets etc. (Mobile Device Management, Verschlüsselung etc.)	BITTE ERGÄNZEN	☐	☒

Eingabekontrolle

Log-Files für die Nachvollziehbarkeit der Löschung/Änderung von Daten des Auftraggebers (namensscharf je Mitarbeiter)

☒ Ja ☐ Nein ☐ Nicht zutreffend

Restriktives Zugriffskonzept für Log-Files

☒ Ja ☐ Nein ☐ Nicht zutreffend

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Datensicherung (Backups)

Häufigkeit der Backups (Intervall): Täglich

Anzahl vorgehaltener Generationen von Backups: 7 (Tage)

Oder

☐ Nicht zutreffend

Aufbewahrungsort Sicherungsdatenträger

☐ Safe

☐ Externe Auslagerung ≥ 5km (Luftlinie)

Oder

☒ Nicht zutreffend

Wiederanlaufzeit bei vollständiger Zerstörung des Rechenzentrums

Tage: 2

Oder

☐ Nicht zutreffend

Verträge zur Wartung von IT-Systemen durch Externe

☐ Ja, ausschließlich innerhalb der EU ☐ Ja, Zugriff aus Drittländern möglich ☒ Nicht zutreffend

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Auftragskontrolle

Schriftliche Verpflichtung zur Vertraulichkeit beim Umgang mit personenbezogenen Daten der Mitarbeiter des Auftragnehmers, die personenbezogene Daten des Auftraggebers verarbeiten oder Zugriff hierauf haben

☒ Ja ☐ Nein

Mitarbeiter werden schriftlich auf das Fernmeldegeheimnis verpflichtet (ePrivacy-Richtlinie oder -Verordnungen in ihrer jeweils gültigen Fassung i.V.m. nationalen Regelungen zum Fernmeldegeheimnis, z.B. § 88 TKG für Deutschland)

☒ Ja ☐ Nein

Schriftliche Zusatzerklärungen (im Zusammenhang mit Datenschutz/Datensicherheit und im Zusammenhang mit mobilem Arbeiten) bei Mitarbeitern des Auftragnehmers

Zusatzerklärungen: BITTE ERGÄNZEN

Subauftragnehmer, die Zugriff auf Daten des Auftraggebers haben

	Ja	Nein
Mit Subauftragnehmern (die Daten des Auftraggebers verarbeiten) bestehen Auftragsverarbeitungsverträge im Sinne der Art. 4 Nr. 8 i.V.m. Art. 28 DSGVO	☒	☐
Gewährleistung der Betriebssicherheit gemäß Artikel 4 RiLi 2002/58/EG i.V.m. RiLi 2009/136/EG (sofern zutreffend)	☒	☐
Es existieren Subauftragnehmer außerhalb der EU, mit Zugriff auf Daten des Auftraggebers	☐	☒
Subauftragnehmer (die Daten des Auftraggebers verarbeiten) halten die in dieser Checkliste vereinbarten technischen und organisatorischen Maßnahmen genauso wie der Auftragnehmer selbst ein und haben deren Einhaltung vertraglich zugesichert	☒	☐

Oder

☐ Es wurden keine Subauftragnehmer beauftragt, die Zugriff auf Daten des Auftraggebers haben

Namensscharf dokumentierte Schulungen der Mitarbeiter zum Datenschutz

☒ Ja ☐ Nein

Zertifikate/Datenschutzkonzepte des Auftragnehmers (bitte als Anhang übermitteln)

Titel und Datum: BITTE ERGÄNZEN

Bei Dienstleistungen, die unter Zuhilfenahme von Cloud-Services erbracht werden, wird ein Architekturbild mit eingereicht (IT-Komponenten, Orte der Speicherung, verwendeten Protokolle)

Titel und Datum: siehe Architekturbeschreibung

Sonstiges

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gem. Art. 32 (1) DS-GVO kommt beim Auftragnehmer zum Einsatz

☐	ISMS, nach folgendem Standard (ISO 27001/2 etc.)	BITTE ERGÄNZEN
☒	Alternatives Verfahren (bitte benennen)	BSI Grundschutz

Oder

☐ Nicht zutreffend, weil: BITTE ERGÄNZEN

Sofern Leistungen dieses Vertrages auch die Bereitstellung von Diensten bzw. die Entwicklung von Software umfassen (Software-as-a-Service etc.)

☒	Regelungen zu Datenschutz durch Technikgestaltung (Titel und Datum)	Netzplan und IT-Systeme, 17.02.2024
☐	Regelungen zur Verwendung personenbezogener Daten in der Softwareentwicklung (Titel und Datum)	BITTE ERGÄNZEN

Oder

☐ Nicht zutreffend

Es existieren Regelungen zum Umgang mit Sicherheitsvorfällen (Incident-Response)

☐	Regelungen zum Umgang mit Sicherheitsvorfällen (Titel und Datum)	BITTE ERGÄNZEN
☐	Verfahren zur unverzüglichen Meldung an den Auftraggeber (bitte erläutern)	BITTE ERGÄNZEN

Unterschrift

Wir versichern, dass die hier getätigten Angaben dem aktuellen Stand der bei uns umgesetzten technischen und organisatorischen Maßnahmen zum Datenschutzniveau und zur Datensicherheit entsprechen. Abweichungen der hier getätigten Angaben sind unmittelbar an den Auftraggeber zu melden.

Dr. Uwe Mayer

Name und Vorname der verantwortlichen Person

Dresden, 14.05.2024	
Ort, Datum	Unterschrift und Firmenstempel Auftragnehmer