Vertrag zur Auftragsverarbeitung
gemäß Art. 28 DS-GVO

Vereinbarung

zwischen dem/der

Firmenname:
Straße Hausnummer:
PLZ Ort:

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der
SKIT GmbH
Dresdner Straße 6
74613 Öhringen

sowie der

SKIT Dynamics GmbH
Am Frauwald 12
65510 Idstein
- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

[ggf.: Vertreter gemäß Art. 27 DS-GVO]

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Dienstleistungsvereinbarung

_____ vom _____,
auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: IT-Betreuung

1.2 Dauer

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum _____

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von einem Monat zum Folgemonat gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom _____

oder

☐ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:
☐ IT-Betreuung und Administration mit unbeaufsichtigtem Zugriff

☐ Webhosting
☐ Dienstleistungen bei Bedarf
☐ Prüfungsdienstleistungen
☐ Fehlerbehebung Software/Datenbank

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

Das angemessene Schutzniveau in _____

☐ ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

☐ wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);

☐ wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DS-GVO);

☐ wird hergestellt durch genehmigte Verhaltensregeln (Art 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);

☐ wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).

☐ wird hergestellt durch sonstige Maßnahmen: _____ (Art. 46 Abs 2 lit. a, Abs. 3 litt. a und b DS-GVO)

2.2 Art der Daten

☐ Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter:

_____

oder

☐ Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien bzw. der Auftragnehmer hat im Kontext seiner Dienstleistungen Zugriff auf folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):
  ☐ Personenstammdaten
  ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
  ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
  ☐ Kundenhistorie

☐ Vertragsabrechnungs- und Zahlungsdaten
☐ Planungs- und Steuerungsdaten
☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
☐ ...

2.3 Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:

_____

oder

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☐ Kunden
☐ Interessenten
☐ Abonnenten
☐ Beschäftigte
☐ Lieferanten
☐ Handelsvertreter
☐ Ansprechpartner
☐ Steuerberater
☐ Rechtanwälte
☐ IT Berater
☐ Bankangestellte
☐ Gesellschafter
☐ ....

3. Technisch-organisatorische Maßnahme

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser ein-vernehmlich umzusetzen.

3.2 Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [Einzelheiten in Anlage 1]

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren

4. Berichtigung, Einschränkung und Löschung von Daten

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen, Berichtigung, Daten Portabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) ☒ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art.28 und 29 DS-GVO ausübt.

☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

☒ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer bestellt:

Herr Gerd Rückert/GRCON
Erich-Sailer-Straße 50
74206 Bad Wimpfen
0177-6895806
rueckert@grcon.de

☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

b) ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail] benannt.

c) ☐ Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: [Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail].

d) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

e) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

h) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

6.1 Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der nachfolgenden Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Firma Unterauftragnehmer	Anschrift	Leistung
SKIT Systems GmbH	Dresdner Straße 6, 74613 Öhringen	IT-Dienstleistungen
C.O.B. GmbH	Kupfergasse 11, 73728 Esslingen am Neckar	IT-Dienstleistungen
2consult	Meierei 1e, 90547 Stein b. Nürnberg	IT-Dienstleistungen
LogistikMeiLe GmbH	Frankenbacher Str. 47, 74078 Heilbronn	IT-Dienstleistungen

c) ☒ Die Auslagerung auf Unterauftragnehmer
oder
☒ der Wechsel des bestehenden Unterauftragnehmers
ist zulässig, soweit:
- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

6.3 Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.4 Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

6.5 Eine weitere Auslagerung durch den Unterauftragnehmer

- ☐ ist nicht gestattet;
- ☒ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrecht des Auftraggebers

7.1 Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftrag-nehmer in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftrag-nehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- ☒ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftraggebers

8.1 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragsnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

9.2 Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

10.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Ort		Ort	Idstein
Datum		Datum	
Name		Name	Guido Sterzing
Unterschrift		Unterschrift	

Anlage – Technisch-organisatorische Maßnahme

Diese Anlage darf nur nach vorheriger Rücksprache und Genehmigung durch GRCON weitergegeben, kopiert, weiterverarbeitet oder für andere Zwecke genutzt werden.

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

Zutrittskontrolle	
Technische Maßnahmen	Organisatorische Maßnahmen
☐ Sicherheitsschlösser ☐ Magnet- oder Chipkarten ☒ Transponder ☐ Schließsystem mit PIN ☒ Manuelles Schließsystem ☒ Elektrischer Türöffner ☐ Biometrische Zugangssperren ☐ Elektronisches Zutrittskontrollsystem ☐ Lichtschranken/Bewegungsmelder ☐ Alarmanlage ☐ Videoüberwachung ☒ Extra Zugangskontrolle zu Rechnerräumen ☐ Absicherungen am Gebäude	☒ Personenkontrolle beim Pförtner ☐ Wachpersonal ☒ Besucherregelungen (z. B. Klingel, Ausweise, Begleitung durch Mitarbeiter) ☒ Schlüsselregelung ☐ Hausausweise ☐ Sicherheitspersonal ☒ seriöses Reinigungspersonal ☐ Videoüberwachung Dokumentation ☐ Protokollierung von Zutritt

Zugangskontrolle (Login)	
Technische Maßnahmen	Organisatorische Maßnahmen
☒ Authentifikation mit Passwort ☐ Authentifikation mit biometrischen Daten ☐ Single-Sign-On ☒ Zugangssperren bei fehlerhaften Anmeldeversuchen ☐ RFID-, Chip-, Smart- oder Magnetkarten ☒ Zwei-Faktor-Authentifizierung ☐ USB-Dongel ☒ Protokollierung des Zugangs	☒ Erstellen von Benutzerprofilen ☒ Zuordnung von Benutzerrechten ☒ Zuordnung von Benutzerprofilen zu IT-Systemen ☐ Einsatz von zentraler Smartphone-Administrations-Software ☒ Verwaltung der Benutzerberechtigung ☒ Passwortvergabe (Erstanmeldeprozedur) ☒ Passwortrichtlinien (Komplexität, Mindestlänge 8 Zeichen, regelmäßiger Wechsel) ☒ Verfahren für Antrag bei neuen Benutzern und beim Ausscheiden von Mitarbeitern ☐ Vier-Augen-Prinzip ☐ Administrationsrichtlinien

Zugriffskontrolle	
Technische Maßnahmen	Organisatorische Maßnahmen
☒ softwareseitiges Berechtigungskonzept ☒ Rollen-/Gruppendefinition ☒ abgestufte Berechtigungen ☒ Ordnungsgemäße Vernichtung von Datenträgern ☒ Aktenvernichter nach DIN-Norm ☒ Akten in abschließbaren Schränken ☐ Sperrung von Laufwerken und Anschlüssen ☒ Automatische Sperren ☒ Verschlüsselung von Notebooks ☐ Verschlüsselung von Servern ☒ Datenschutzgerechte Löschung vor Wiedereinsatz von Datenträgern ☒ Protokollierung von Zugriffen	☐ schriftliches Berechtigungskonzept ☒ Richtlinien zur Aktenvernichtung ☒ Richtlinien zur Datenträgervernichtung ☒ Sichere Aufbewahrung von Datenträgern ☒ Protokollierung der Datenträger-vernichtung ☐ Einsatz von Dienstleistern bei der Vernichtung (nach sorgfältiger Auswahl) ☒ Nur die nötigste Anzahl an Administratoren

Trennungskontrolle	
Technische Maßnahmen	Organisatorische Maßnahmen
☒ Mandantenfähige Software ☒ Trennung der verarbeitenden Systeme ☒ Trennung der Nutzerkonten ☒ Verarbeitung auf unterschiedlichen Servern, Systemen, Datenbanken oder Tabellen ☒ Produktiv- und Testsystem	☒ Logische Mandantentrennung ☐ Zweckbindung ☒ Regelung und Maßnahmen zur Sicherstellung der Trennung von Daten unterschiedlicher Zwecke (z. B. Kunden- und Mitarbeiterdaten)

- **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) **und Anonymisierung**
  Die Verarbeitung personenbezogener Daten findet in einer Weise statt, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;
  - ☐ Pseudonymisierung
  - ☐ Anonymisierung

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

Weitergabekontrolle	
Technische Maßnahmen	Organisatorische Maßnahmen
☒ Verschlüsselung von Daten bei Übertragung ☒ Sichere Verbindungen (VPN, SSL) ☐ Sicherer Transportbehälter ☒ Verschlüsselung von E-Mail-Anhängen ☐ Verschlüsselung von E-Mails ☐ Elektronische Signatur ☐ Content-Filter, SSL-Scanner	☒ Protokollierung von Empfängern und hierzu relevante Daten ☒ Dokumentation regelmäßiger Abruf- und Übermittlungsvorgänge (Datenflussplan) ☐ Einsatz von verlässlichem Transportpersonal und Transportmitteln

Eingabekontrolle	
Technische Maßnahmen	Organisatorische Maßnahmen
☒ Protokollierung von Änderungen an Daten, Anwendungen und Systemen ☒ Erfassung gescheiterter Zugriffsversuche ☒ Dokumentenmanagement	☒ Protokollierung von Administration ☒ Auswertung von Protokolldaten ☐ Plausibilitätskontrollen ☒ Dokumentation, mit welchen Anwendungen welche Daten eingegeben, geändert, gelöscht werden können ☐ Festlegung, wer Daten bearbeiten darf

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

Verfügbarkeit und Sicherheit	
☒ Schutz vor Schadsoftware/Virenschutzkonzept ☒ Backup von Systemen, Komponenten und Datenbanken ☒ Backup-Konzept mit unterschiedlichen Brandschutzzonen ☒ Datenspiegelung ☒ Redundanz von Systemen, Komponenten und Netzwerken ☒ Quarantänenetzwerk ☒ Brandschutz im Rechnerraum ☒ Klimatisierter Rechnerraum ☐ Klima-, Temperatur- und Feuchtigkeitsüberwachung Rechnerraum ☒ Unterbrechungsfreie Stromversorgung	☒ Firewall ☒ DMZ ☒ Netzwerkzugänge von außen (VPN; SSL) ☒ Vertretungspersonal ☒ Möglichkeit der Aufgabenerledigung durch Dritte (Outsourcing) ☐ Arbeitsanweisungen für Administratoren ☒ E-Mail-Benachrichtigungen von Verfügbarkeitsprozessen ☒ Kontrolle und Prüfung der Schutzmaßnahmen im Bereich Verfügbarkeit ☒ Reparaturstrategien

Belastbarkeit
☒ Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) durch Tests sicherstellen
☐ Penetrationstests

4. Verarbeitung nur auf Weisung (Art. 29 DSGVO)

☒ Verschwiegenheitserklärungen
☒ Arbeitsanweisung oder Verhaltensrichtlinien zu datenschutzrelevanten Themen
☒ Stellenbeschreibungen
☐ regelmäßige Datenschutzschulungen und Sensibilisierung

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

☒ Datenschutz-Management
☒ Incident-Response-Management (IT-Störungsmanagement)
☒ Backup-Kontrollen
☒ Virenschutz-Prüfungen
☒ Firewall-Prüfungen
☒ Kontrolle von weiteren Sicherheitseinrichtungen (z. B. Notstrom, USV)
☐ Policies-Prüfungen
☒ Löschfristen-Kontrollen
☒ Protokollauswertung Zugriff (bei Bedarf)
☒ Protokollauswertung Eingabe (bei Bedarf)
☐ Kontrolle von Richtlinien und Arbeitsanweisungen (Einhaltung)
☐ Kontrolle der ordnungsgemäßen Vernichtung
☒ Kontrolle der Auftragsverarbeiter

Sonstiges:
☒ Kontrollverfahren sind nachvollziehbar dokumentiert
☒ Kontrollen werden protokolliert (z. B. durch Belege)