

**Vertrag zur Auftragsverarbeitung
gemäß Art. 28 DS-GVO**

Vereinbarung

zwischen dem/der

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

**SKIT GmbH und SKIT Systems GmbH
Dresdner Straße 6
74613 Öhringen**

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Vertrags

1.1 Gegenstand

- Der Gegenstand des Vertrags ergibt sich aus der Dienstleistungsvereinbarung

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

oder

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

1.2 Dauer

- Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

- Der Vertrag wird zur einmaligen Ausführung erteilt.

oder

- Die Dauer dieses Vertrags (Laufzeit) ist befristet bis zum _____

oder

- Der Vertrag wird auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von einem Monat zum Folgemonat gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

1.3 Der Vertrag gilt unbeschadet des vorstehenden Absatzes solange, wie der Auftragnehmer personenbezogenen Daten des Auftraggebers verarbeitet (einschließlich Backups).

1.4 Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

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 Vertragsgegenstandes 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

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:

- | | |
|---|--|
| <input type="checkbox"/> Kunden | <input type="checkbox"/> Steuerberater |
| <input type="checkbox"/> Interessenten | <input type="checkbox"/> Rechtsanwälte |
| <input type="checkbox"/> Abonnenten | <input type="checkbox"/> IT Berater |
| <input type="checkbox"/> Beschäftigte | <input type="checkbox"/> Bankangestellte |
| <input type="checkbox"/> Lieferanten | <input type="checkbox"/> Gesellschafter |
| <input type="checkbox"/> Handelsvertreter | <input type="checkbox"/> _____ |
| <input type="checkbox"/> Ansprechpartner | <input type="checkbox"/> _____ |

3. Technisch-organisatorische Maßnahme

- 3.1** Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [siehe Anlage]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.
- 3.2** Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- 3.3** Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzen.

4. Rechte von betroffenen Personen

- 4.1** Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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 die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

5.1 Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Vertrags gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art.38 und 39 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) 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 berechtigterweise 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.
- c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- d) 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.
- e) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- f) 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.
 - g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
 - h) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
 - i) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zu Verfügung.
 - j) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.
- 5.2** Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DSGVO.

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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 Dynamics GmbH	Am Frauwald 12, 65510 Idstein	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

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

- 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, die 14 Tage nicht unterschreiten darf, 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. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

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)
- bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform)

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

7. Internationale Datentransfers

7.1 Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

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.

Es findet eine Verlagerung in folgende Drittländer statt: _____

Das angemessene Schutzniveau

- 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)

7.2 Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8. Kontrollrecht des Auftraggebers

- 8.1** 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 Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.
- 8.2** Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- 8.3** Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den 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).
- 8.4** Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen, wenn der Dienstleistungsaufwand für die Kontrolle einen Tag übersteigt.

9. Weisungsbefugnis des Auftraggebers

- 9.1** Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

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 aber 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.

Auftraggeber		Auftragnehmer	
Ort		Ort	Öhringen
Datum		Datum	
Name		Name	Hans-Peter Köhler
Unterschrift und Firmenstempel		Unterschrift und Firmenstempel	

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
<input type="checkbox"/> Sicherheitsschlösser <input type="checkbox"/> Magnet- oder Chipkarten <input checked="" type="checkbox"/> Transponder <input type="checkbox"/> Schließsystem mit PIN <input checked="" type="checkbox"/> Manuelles Schließsystem <input checked="" type="checkbox"/> Elektrischer Türöffner <input type="checkbox"/> Biometrische Zugangssperren <input type="checkbox"/> Elektronisches Zutrittskontrollsystem <input type="checkbox"/> Lichtschranken/Bewegungsmelder <input type="checkbox"/> Alarmanlage <input type="checkbox"/> Videoüberwachung <input checked="" type="checkbox"/> Extra Zugangskontrolle zu Rechnerräumen <input type="checkbox"/> Absicherungen am Gebäude	<input checked="" type="checkbox"/> Personenkontrolle beim Pfortner <input type="checkbox"/> Wachpersonal <input checked="" type="checkbox"/> Besucherregelungen (z. B. Klingel, Ausweise, Begleitung durch Mitarbeiter) <input checked="" type="checkbox"/> Schlüsselregelung <input type="checkbox"/> Hausausweise <input type="checkbox"/> Sicherheitspersonal <input checked="" type="checkbox"/> seriöses Reinigungspersonal <input type="checkbox"/> Videoüberwachung Dokumentation <input type="checkbox"/> Protokollierung von Zutritt

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

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

Trennungskontrolle	
Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Mandantenfähige Software <input checked="" type="checkbox"/> Trennung der verarbeitenden Systeme <input checked="" type="checkbox"/> Trennung der Nutzerkonten <input checked="" type="checkbox"/> Verarbeitung auf unterschiedlichen Servern, Systemen, Datenbanken oder Tabellen <input checked="" type="checkbox"/> Produktiv- und Testsystem	<input checked="" type="checkbox"/> Logische Mandantentrennung <input type="checkbox"/> Zweckbindung <input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Verschlüsselung von Daten bei Übertragung <input checked="" type="checkbox"/> Sichere Verbindungen (VPN, SSL) <input type="checkbox"/> Sicherer Transportbehälter <input checked="" type="checkbox"/> Verschlüsselung von E-Mail-Anhängen <input type="checkbox"/> Verschlüsselung von E-Mails <input type="checkbox"/> Elektronische Signatur <input type="checkbox"/> Content-Filter, SSL-Scanner	<input checked="" type="checkbox"/> Protokollierung von Empfängern und hierzu relevante Daten <input checked="" type="checkbox"/> Dokumentation regelmäßiger Abruf- und Übermittlungsvorgänge (Datenflussplan) <input type="checkbox"/> Einsatz von verlässlichem Transportpersonal und Transportmitteln

Eingabekontrolle	
Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Protokollierung von Änderungen an Daten, Anwendungen und Systemen <input checked="" type="checkbox"/> Erfassung gescheiterter Zugriffsversuche <input checked="" type="checkbox"/> Dokumentenmanagement	<input checked="" type="checkbox"/> Protokollierung von Administration <input checked="" type="checkbox"/> Auswertung von Protokolldaten <input type="checkbox"/> Plausibilitätskontrollen <input checked="" type="checkbox"/> Dokumentation, mit welchen Anwendungen welche Daten eingegeben, geändert, gelöscht werden können <input type="checkbox"/> Festlegung, wer Daten bearbeiten darf

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

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