Auftragsverarbeitungsvertrag nach Art. 28 III DS-GVO

Die Vertragsparteien

- **Im Folgenden: Auftraggeber –**

Unternehmen: _____

Straße: _____

PLZ Ort: _____

Land: _____

und

- **Im Folgenden: Auftragnehmer –**

SoftTec GmbH, Hindelanger Straße 35, 87527 Sonthofen

schließen folgenden Vertrag:

1. Gegenstand und Dauer

1.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers nach Art. 4 Nr. 2 und Art. 28 DSGVO. Der Inhalt des Auftrags, die Kategorien betroffener Personen und Datenarten sowie der Zweck der Verarbeitung sind in Anlage 1 des Vertrags geregelt.

1.2 Die Verarbeitung der Daten durch den Auftragnehmer findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der EU oder einem Vertragsstaat des EWR-Abkommens statt. Die Verarbeitung außerhalb der genannten Staaten erfolgt nur unter den Voraussetzungen von Art. 44 ff. DSGVO mit vorheriger Zustimmung des Auftraggebers.

1.3 Die Vergütung wird im jeweiligen Projekt festgelegt.

2. Vertragslaufzeit und Kündigung

Der Vertrag wird auf unbestimmte Zeit geschlossen. Die Kündigungsfrist beträgt halbjährlich zum Jahresende, der Vertrag ist von jeder Partei kündbar. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

3.1 Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er ist für die Beurteilung der Zulässigkeit von Datenverarbeitungsvorgängen nach Art. 6 I DSGVO und die Wahrung der Betroffenenrechte nach Art. 12 bis 22 DSGVO mit Unterstützung des Auftragnehmers zuständig. Die Unterstützungspflicht gilt insbesondere für die Erteilung von Auskünften und die Löschung, Berichtigung oder Einschränkung personenbezogener Daten.
Der Auftragnehmer ist verpflichtet, alle Anfragen unverzüglich an diesen weiterzuleiten, wenn sie erkennbar nur an den Auftraggeber gerichtet sind.

3.2 Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung gegenüber dem Auftragnehmer zu. In dieser Rolle kann er insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der vertragsgegenständlichen Daten verlangen. Der Auftragnehmer ist verpflichtet, den Weisungen des Auftraggebers Folge zu leisten, sofern keine berechtigen vertraglichen oder gesetzlichen Interessen entgegenstehen.
Der Auftraggeber benennt eine oder mehrere weisungsberechtigten Personen, Änderungen sind unverzüglich mitzuteilen.

3.3 Änderungen des Verarbeitungsgegenstands und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und –nehmer abzustimmen.

3.4 Der Auftragnehmer macht den Auftraggeber unverzüglich darauf aufmerksam, wenn eine erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt nach Art. 28 III 3 DSVGO. Wird eine Weisung erteilt, deren Rechtmäßigkeit der Auftragnehmer substantiiert anzweifelt, ist der Auftragsnehmer berechtigt, deren Ausführung vorübergehend auszusetzen, bis der Auftraggeber diese nochmals ausdrücklich bestätigt oder ändert.

3.5 Weisungen sind grundsätzlich schriftlich oder in einem elektronischen Format zu erteilen. Mündliche Weisungen sind auf Verlangen des Auftragnehmers schriftlich oder in einem elektronischen Format durch den Auftraggeber zu bestätigen. Der Auftragnehmer hat Person, Datum und Uhrzeit der mündlichen Weisung in angemessener Form zu protokollieren.

3.6 Der Auftragnehmer ist nicht berechtigt, die personenbezogenen Daten für eigene Zwecke zu nutzen.

4. Kontrollbefugnisse des Auftraggebers

4.1 Der Auftraggeber und –nehmer sind bezüglich der zu verarbeitenden Daten für die Einhaltung der einschlägigen Datenschutzgesetze verantwortlich. Der Auftraggeber ist berechtigt, die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz und zur Datensicherheit vor Beginn der Datenverarbeitung und während der Dauer des Vertrags regelmäßig im erforderlichen Umfang zu überprüfen oder durch Dritte kontrollieren zu lassen. Der Auftragnehmer hat die Kontrollen zu dulden und diese zu unterstützen, soweit dies erforderlich ist.
Der Auftragnehmer hat die erforderlichen Auskünfte zu erteilen, die Einsichtnahme in die gespeicherten Daten und Datenverarbeitungsprogramme und –systeme zu gestatten. Er hat weiterhin Vorort-Kontrollen zu ermöglichen.

4.2 Der Auftraggeber sorgt dafür, dass die Kontrollmaßnahmen verhältnismäßig sind und den Betrieb des Auftragnehmers nicht weiter als unbedingt erforderlich beeinträchtigen.

Insbesondere sollten Vorortkontrollen grundsätzlich zu den üblichen Geschäftszeiten und nach Terminvereinbarung mit angemessener Fristsetzung erfolgen, sofern der Kontrollzweck keiner vorherigen Ankündigung entgegensteht.

4.3 Das Ergebnis der Kontrolle ist von beiden Vertragsparteien zu protokollieren.

4.4 Die entstehenden Kosten sowohl auf Seiten des Auftraggebers als auch auf Seiten des Auftragnehmers für die Vorbereitung und Durchführung einer Überprüfung durch oder im Auftrag des Auftraggebers trägt der Auftraggeber

5. Pflichten des Auftragnehmers

5.1 Der Auftragsnehmer hält bei Auftragsdurchführung sämtliche gesetzliche Vorschriften ein, er hat insbesondere nach Art. 32 und 30 II DSGVO die notwendigen technischen und organisatorischen Maßnahmen einzuführen und das erforderliche Verzeichnis von Verarbeitungstätigkeiten zu führen, soweit es gesetzlich vorgesehen ist.

5.2 Die Verarbeitung der Daten durch den Auftragsnehmer erfolgt nur auf Grundlage der vertraglichen Vereinbarung mit den erteilten Weisungen des Auftraggebers. Eine abweichende Verarbeitung ist nur aufgrund zwingender europäischer oder mitgliedsstaatlicher Rechtsvorschriften zulässig. Ist eine Verarbeitung wegen zwingenden Rechts erforderlich, teilt der Auftragnehmer dies dem Auftraggeber vor der Verarbeitung mit, sofern das betreffende Recht einer solchen Mitteilung nicht entgegensteht.

5.3 Ist der Auftragnehmer zur Benennung eines Datenschutzbeauftragten verpflichtet, bestätigt er, dass er einen solchen ausgewählt hat und sichert zu, diesen unter Angabe der Kontaktdaten zu benennen. Änderungen sind unverzüglich mitzuteilen.

5.4 Die Datenverarbeitung außerhalb der Betriebsstätten des Auftragnehmers oder der Subunternehmer und/oder in Privatwohnungen ist nur mit ausdrücklicher Zustimmung des Auftraggebers gestattet.

5.5 Über die Herausgabe oder Löschung der Daten nach Vertragsende muss der Auftraggeber entscheiden. Entstehen nach Vertragsbeendigung zusätzliche Kosten durch Herausgabe oder Löschung von Daten so trägt diese der Auftragnehmer.

6. Technische und organisatorische Maßnahmen

6.1 Es wird ein angemessenes Schutzniveau für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen gewährleistet durch geeignete technische und organisatorische Maßnahmen nach Art. 25 DSGVO. Diese Maßnahmen wurden nach Art. 32 I DSGVO ausgewählt und mit dem Auftraggeber abgestimmt. Die Maßnahmen sind in Anlage 2 des Vertrages festgehalten.

6.2 Der Auftragnehmer kann diese bei gegebenem Anlass, mindestens aber einmal jährlich überprüfen, bewerten und evaluieren oder anpassen lassen, wesentliche Veränderungen sind mit dem Auftraggeber abzustimmen, insbesondere solche, welche das Schutzniveau verringern. Erforderliche Anpassungen werden vom Auftragnehmer dokumentiert und dem Auftraggeber auf Nachfrage zur Verfügung gestellt.

7. Einsatz von Unterauftragsverarbeitern (Subunternehmern)

7.1 Der Auftragnehmer ist nur mit Zustimmung des Auftragsgebers zum Einsatz von Subunternehmern berechtigt, Art. 28 II DSGVO. Die Subunternehmer müssen ausdrücklich benannt werden. Die bereits bestehenden Subunternehmerverhältnisse, welche in Anlage 3 des Vertrages beigefügt sind, gelten als bestätigt mit Unterzeichnung dieses Vertrages. Beabsichtigt der Auftragnehmer den Einsatz weiterer Subunternehmer, wird er dies dem Auftraggeber in schriftlicher oder elektronischer Form anzeigen, damit dieser deren Einsatz prüfen kann. Erfolgt keine Zustimmung durch den Auftraggeber, dürfen die betroffenen Subunternehmer nicht eingesetzt werden.

7.2 Die Auswahl eines Subunternehmers erfolgt durch den Auftragsnehmer unter Beachtung der gesetzlichen und vertraglichen Vorgaben. Nebenleistungen, die der Auftragnehmer zur Ausübung seiner geschäftlichen Tätigkeit in Anspruch nimmt, stellen keine Unterauftragsverhältnisse dar. Der Auftragnehmer wird jedoch auch bei diesen Drittleistungen die Einhaltung der gesetzlichen Datenschutzstandards gewährleisten.

7.3 Die vertraglichen Vereinbarungen mit Subunternehmern haben den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrags und der gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten zu entsprechen. Dies betrifft insbesondere die Implementierung geeigneter technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte nach Art. 28 III lit.h DSGVO einzuräumen.

7.4 Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 IV DSGVO bezüglich seiner Beschäftigten erfüllt hat.

7.5 Der Auftragnehmer hat die Einhaltung der Pflichten der Subunternehmer zu überprüfen und das Ergebnis zu dokumentieren. Dieses ist dem Auftraggeber zugänglich zu machen.

7.6 Der Auftragnehmer hat sich von seinen Unterauftragsverarbeitern bestätigen zu lassen, dass diese – soweit gesetzlich vorgeschrieben – einen Datenschutzbeauftragten benannt haben.

8. Geheimhaltungspflicht

8.1 Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangte Geschäftsgeheimnisse und Datensicherheitsmaßnahmen des Auftragnehmers sowie die personenbezogenen Daten vertraulich zu behandeln. Die Verpflichtung bleibt nach Beendigung des Vertrags bestehen. Der Auftraggeber hat diesen bei Auftragserteilung auf bestehende besondere Geheimschutzregeln hinzuweisen.

8.2 Der Auftragsnehmer gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen, Art. 28 III lit.b DSGVO). Vor der Unterwerfung unter die Verschwiegenheitspflicht dürfen die betreffenden Personen keinen Zugang zu den vom Auftraggeber überlassenen personenbezogenen Daten erhalten.

9. Schlussbestimmungen

9.1 Änderungen und Ergänzungen sowie Nebenabreden dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung.

9.2 Verstöße gegen diesen Vertrag, gegen Weisungen oder gegen sonstige datenschutzrechtliche Bestimmungen sind dem Auftraggeber unverzüglich mitzuteilen. Das gleiche gilt bei Vorliegen eines Verdachts.

9.3 Bei Änderungen der DSGVO während der Vertragslaufzeit, gelten die hiesigen Verweise auch für die jeweiligen Nachfolgeregelungen

9.4 Bei Unwirksamkeit einzelner Teile dieser Vereinbarung, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

9.5 Sämtliche Anlagen zu diesem Vertrag sind Vertragsbestandteil.

Auftraggeber	**Auftragnehmer**
_____	Sonthofen, 13.08.2020
Ort, Datum	Ort, Datum
	
_____	
Stempel, Unterschrift	Stempel, Unterschrift

Anlage 1

Auftragsdetails

Der vorliegende Vertrag umfasst folgende Leistungen (ggf. in Zusammenhang mit dem Hauptvertrag):

- *Durchführung von Wartungsarbeiten zur Anpassung,*
- *Hilfestellung oder Korrektur der vom Auftragnehmer gelieferten Software.*

Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

- *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)*
- *Daten, die in der Software des Auftragsgebers vom Auftraggeber erfasst wurden*

Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

- *Kunden*
- *Mitarbeiter*
- *Gäste*

Der Zugriff auf die betroffenen Daten geschieht in folgender Weise:

Im Rahmen der Wartung wird definiert, welche Systeme und Anwendungen durch den Auftragnehmer installiert und betreut werden.

Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies erfolgt durch den Einsatz der Fernwartungssoftware Teamviewer, Anydesk, OpenVPN,

Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

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. DSGVO er-füllt sind.

Der Auftraggeber unterliegt folgenden besonderen Geheimschutzregeln, die auch vom Auftragnehmer zu beachten sind:

Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

Anlage 2

Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragnehmers nach Art. 32 DSGVO

Der Auftragnehmer setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen werden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

ERFASSUNGSBOGEN ZUR SICHERHEIT DER VERARBEITUNG PERSONENBEZOGENER DATEN GEMÄß ART. 32 ABS. 1 EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DS-GVO)
Der Verantwortliche und der Auftragsverarbeiter treffen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten.

Bearbeitet durch:	Entwickler der Abteilung			
Verantwortliche Abteilung:	Entwicklung			
Kontaktdaten:	Tel:	08321 6749 0	E-Mail:	info@softtec.de
Datum:	13.08.2020			

Name, Adresse und Kontaktdaten des Verantwortlichen (Kunde)				
Firmenname/Bezeichnung:				
(Besuchs-)Adresse:				
Leitung des Verantwortlichen:				
Kontaktdaten:	Tel:		E-Mail:	

Name, Adresse und Kontaktdaten des Auftragsverarbeiters				
Firmenname/Bezeichnung:	SoftTec GmbH			
(Besuchs-)Adresse:	Hindelanger Str. 35			
Leitung des Verantwortlichen:	Oliver Anschütz			
Kontaktdaten:	Tel:	08321 6749 0	E-Mail:	info@softtec.de

Bemerkung:	Unternehmen haben gemäß Artikel 32 Abs. 1 Europäische Datenschutzgrundverordnung (DS-GVO) die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, die Anforderungen aktueller Datenschutznormen (insbesondere der DS-GVO) zu erfüllen. Hierbei sind die in Art. 32 Abs. 1 lit. a) - d) DS-GVO genannten Anforderungen zu berücksichtigen. Um diesen Anforderungen gerecht zu werden bzw. gegebenenfalls ein Vor-Ort-Audit zur Überprüfung der getroffenen Maßnahmen zu vermeiden, wurde der folgende Fragebogen entwickelt. Bitte beantworten Sie die Fragen, soweit wie für Sie möglich.

Hinweis:	Allgemeines Gleichbehandlungsgesetz (AGG) Aus Gründen der leichteren Lesbarkeit wird in diesem Dokument auf eine geschlechterspezifische Differenzierung verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für beide Geschlechter.

Technisch-organisatorische Maßnahmen							
Wahrung der Vertraulichkeit personenbezogener Daten (Art. 32 Abs. 1 lit. b) DS-GVO)							
1.	**Zutrittskontrolle** – Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z. B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.						
1.1.	Liegt eine Beschreibung/Dokumentation der gesamten am Standort eingesetzten Zutrittskontrollmaßnahmen vor?	☒	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.2.	Gibt es am Standort maschinelle Zutrittskontrollsysteme zur Überwachung des Betretens und evtl. auch Verlassens eines Gebäudes/eines Gebäudeteils?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.3.	Werden eventuell biometrische Kontrollsysteme (Handflächen, Iris-Scanner, Fingerabdruck-Leser) eingesetzt?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.4.	Ist die Verwaltung und Wartung der maschinellen Zutrittskontrollsysteme geregelt und dokumentiert?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.5.	Werden in den Zutrittskontrollanlagen personenbezogene Daten gespeichert, so dass nachvollziehbar ist, wer wann einen bestimmten räumlichen Bereich betreten und ggf. auch wieder verlassen hat?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.6.	Werden die protokollierten Daten regelmäßig oder aufgrund besonderer Anlässe wie nach (versuchten) Sicherheitsverletzungen ausgewertet?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.7.	Gibt es ein ausreichendes Gebäude-Sicherungskonzept, welches auf die Zutrittsmöglichkeiten eingeht?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.8.	Um welche Bebauungsart handelt es sich?	☐	Freistehender Gebäudekomplex				
	☒ Geschlossene Bebauung	☐	Mit Werksgelände				
	☐ Umzäuntes Grundstück	☐	Offen zugängliches Grundstück				
Bemerkung:							
1.9.	Sind Sicherheitszonen unterschiedlicher Klassifizierung und Sensibilität vorgesehen?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.10.	Sind diese im Gebäude-Sicherungskonzept ausreichend genau beschrieben?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.11.	Sind die Verteilerräume oder -bereiche (Gebäudetechnik) gegen unbefugten Zutritt gesichert?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							

1.12. Ist eine durchgängige Außenhautsicherung (Einbruchshemmende Maßnahmen) vorhanden?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
1.13. Sind Sicherungsmaßnahmen gegen Überfälle im Einsatz? (bspw. Gegensprechanlagen, elektrische Türöffner, Lichtschranken, Überfallmelder, Videoüberwachung)	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
1.14. Existieren angemessene, nicht maschinelle Zutrittskontrollen (z. B. einfache Schlösser) zu dem Gebäude?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
1.15. Ist sichergestellt, dass die Zutrittsprotokolle nur solange aufbewahrt werden, wie dies für den vorgesehenen zulässigen Zweck erforderlich ist?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung: Firma führt keine Zutrittsprotokolle						
1.16. Ist sichergestellt, dass die Form der Auswertung der Zutrittsprotokolle datenschutzkonform geschieht?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
1.17. Liegt für alle Schlüssel (oder andere Identifikationsmittel) des Gebäudes (von Etagen, Fluren und Räumen) ein Schließplan vor?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
1.18. Ist die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln (oder anderer Identifikationsmittel) zentral geregelt und dokumentiert?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
1.19. Sind Reserveschlüssel (oder andere Identifikationsmittel) vorhanden und gesichert aufbewahrt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
1.20. Besteht eine Pflicht zum Tragen von Dienst- oder Firmenausweisen?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
1.21. Tragen alle Mitarbeiter ihre Dienst- oder Firmenausweise sichtbar?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
1.22. Besteht eine Kennzeichnungspflicht für fremde Personen durch sichtbar zu tragende Ausweise?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
1.23. Ist die Vergabe von Besucher- und Firmenausweisen revisionsfähig?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
1.24. Werden persönliche Daten von Firmenbesuchern in ein Besucherbuch aufgenommen?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
1.25. Werden die Unternehmensserver in einem abgeschlossenen und zutrittsgesicherten Raum betrieben?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						

1.26.	Haben nur Befugte Zutritt zum Serverraum/Rechenzentrum?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
1.27.	Werden Maßnahmen zur Raumüberwachung des Serverraums/Rechenzentrums getroffen (Videokameras/Bewegungsmelder)?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.28.	Befinden sich die Netzwerkkomponenten in dafür vorgesehenen zutrittskontrollierten Räumen (zutrittsgesichert z. B. durch den Einsatz von Ausweislesern)?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
1.29.	Existiert eine Regelung bzw. ein Prozess für den Fall, dass externe Kräfte Zutritt zum Serverraum/Rechenzentrum benötigen? (z. B. Wartungsdienste, Reinigungsdienst, Besucher)	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
1.30.	Werden die eingerichteten Schutzmaßnahmen regelmäßig einem eingehenden Test unterzogen, um festzustellen, ob sie noch den gewünschten Schutzzweck erfüllen?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
2.	**Zugangskontrolle** – Keine unbefugte Systembenutzung, z. B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.						
2.1.	Werden die eingerichteten Schutzmaßnahmen regelmäßig einem eingehenden Test unterzogen, um festzustellen, ob sie noch den gewünschten Schutzzweck erfüllen?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
2.2.	Gibt es für alle Informationssysteme und Dienste eine formale Benutzer-Registrierung und Deregistrierung zur Vergabe und Rücknahme von Zugangsberechtigungen?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
2.3.	Ist sichergestellt, dass Benutzer nur Zugang zu den Netzdiensten bekommen, zu deren Nutzung sie ausdrücklich befugt sind?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
2.4.	Ist sichergestellt, dass nur berechtigte Personen logischen Zugang zu den Netzwerkkomponenten haben?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
2.5.	Gibt es ein formales Freigabeverfahren, welche Systeme und Applikationen mit personenbezogenen Daten zu durchlaufen haben, bevor diese Netzwerkzugang bekommen dürfen?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
2.6.	Ist sichergestellt, dass nur autorisierte Geräte von privaten Personen oder Besuchern logischen Zugang zum Netzwerk der Organisation bekommen?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
2.7.	Ist sichergestellt, dass das WLAN ausreichend vor unbefugtem Zugang gesichert ist?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							

2.8.	Ist der eingesetzte Autorisierungs- und Verschlüsselungsmechanismus des WLANs genügend sicher?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
2.9.	Wird in regelmäßigen Abständen von unabhängigen Testern ein Angriff auf das Netzwerk simuliert, um Schwachstellen zu identifizieren?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
2.10.	Existieren ausreichende Maßnahmen zur Identifikation und Authentisierung von externem Wartungspersonal (z. B. sicherer Passwortschutz)?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
2.11.	Wird das Benutzerpasswort für das Wartungspersonal unmittelbar nach dem Abschluss von Wartungsaktivitäten geändert?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
2.12.	Wird bei der Fernwartung die Verbindung von einer Person aufgebaut, welche Mitglied der eigenen Organisation ist?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
2.13.	Geschieht der Verbindungsaufbau von innerhalb des Netzwerks aus?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
2.14.	Ist durch die Organisation sichergestellt, dass Softwareänderungen bei Wartungseinsätzen kontrolliert werden?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
2.15.	Ist bei der lokalen Wartung durch Externe sichergestellt, dass keine Ausrüstungsgegenstände (Geräte, Datenträger) den DV-Bereich unkontrolliert verlassen können?	☒	Ja	☐	Nein	☐	Teilweise
3.	**Zugriffskontrolle** – Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.						
3.1.	Stellen die Benutzer sicher, dass ihre DV-Ausstattung (PC, Laptop, Smartphone etc.), falls unbeaufsichtigt, ausreichend (z. B. durch Abmelden vom System usw.) geschützt ist?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
3.2.	Wird der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms gelebt (Clean Desk)?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
3.3.	Wird dem Benutzer der Zeitpunkt der letztmaligen Verfahrensnutzung angezeigt?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
3.4.	Wird für die Gewährleistung der Datensicherheit und der Zugriffssicherung eine spezielle Sicherheitssoftware (z. B. Intrusion Detection) eines Fremdherstellers eingesetzt?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
3.5.	Wird von der Verschlüsselung der Daten auf Dateiebene/Verzeichnisebene Gebrauch gemacht?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							

3.6.	Werden die Informationen auf mobilen Datenträgern ausreichend davor geschützt, im Verlustfall ausgelesen werden zu können?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
3.7.	Wird die Software eines anerkannten Herstellers eingesetzt, so dass von hinreichend sicheren Verschlüsselungsalgorithmen und Schlüssellängen ausgegangen werden kann?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
3.8.	Gibt es eine Anweisung darüber, wie mit nicht mehr benötigten Datenträgern umzugehen ist (dazu gehört auch beschriebenes oder bedrucktes Papier)?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
3.9.	Gibt es eine Anweisung darüber, wie bei der Entsorgung oder Weiterverwendung von Geräten vorzugehen ist, die mit Speichermedien ausgerüstet sind?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
3.10.	Ist sichergestellt, dass Dokumente und Datenträger, deren Aufbewahrungsfrist abläuft, nachhaltig vernichtet bzw. gelöscht werden?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
4.	**Trennungskontrolle** – Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. Mandantenfähigkeit, Sand Boxing.						
4.1.	Werden personenbezogene Daten auf den Systemen physisch voneinander getrennt (Verarbeitung unterschiedlicher Datensätze auf getrennten Systemen)?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
4.2.	Werden personenbezogene Daten auf den Systemen logisch voneinander getrennt (unterschiedliche Datensätze in einer einheitlichen Datenbank werden je nach Zweck markiert (softwareseitige Unterscheidbarkeit))?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
4.3.	Sind die im Unternehmen eingesetzten Systeme mandantenfähig?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
4.4.	Ist die Mandantenfähigkeit für die davon betroffenen Verfahren durchgängig realisiert?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
4.5.	Ist die Mandantenfähigkeit der Verfahren in der Verfahrensdokumentation nachvollziehbar dokumentiert?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
4.6.	Befinden sich Office-, Entwicklungs-, Test- und Wirksysteme in klar voneinander getrennten Netzsegmenten, vielleicht sogar physikalisch voneinander getrennt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
4.7.	Ist sichergestellt, dass im Entwicklungs- und Testsystem nur Testdaten verarbeitet werden?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							

4.8.	Ist sichergestellt, dass Testdaten, die aus Echtdaten abgeleitet werden, anonymisiert sind?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
5.	**Pseudonymisierung** – Die Verarbeitung personenbezogener Daten in einer Weise, 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.						
4.9.	Werden im Unternehmen Pseudonymisierungsverfahren mit getrennter Aufbewahrung der Zuordnungsdatei eingesetzt?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
Wahrung der Integrität personenbezogener Daten (Art. 32 Abs. 1 lit. b) DS-GVO)							
6.	**Weitergabekontrolle** – Weitergabekontrolle – Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.						
6.1.	Wurden alle Personen, die mit der Verarbeitung/Nutzung personenbezogener Daten beschäftigt sind, zur Einhaltung der Vertraulichkeit verpflichtet?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
6.2.	Werden allen neuen Mitarbeitern bei der Verpflichtung zur Vertraulichkeit Informationen zum Datenschutz ausgehändigt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
6.3.	Sind die Mitarbeiter, die personenbezogene Daten verarbeiten/nutzen, durch Datenschutzschulungen auf datenschutzgerechtes Verhalten am Arbeitsplatz geschult worden?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
6.4.	Gibt es Regelungen für die Behandlung ausscheidender, insbesondere gekündigter Mitarbeiter?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
6.5.	Gibt es ein unternehmensweit gültiges Schema für die Klassifizierung von Daten?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
6.6.	Sind angemessene Sicherheitsmaßnahmen für den physischen Transport von Datenträgern (inkl. Papier) umgesetzt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
6.7.	Sind angemessene Sicherheitsmaßnahmen für die Weitergabe von Datenträgern zu Wartungszwecken oder zur Fehleranalyse umgesetzt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
6.8.	Erfolgt die Datenübergabe gegen Nachweis (Quittung)?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
6.9.	Ist sichergestellt, dass Daten nur an die vom Auftraggeber festgelegten oder der Zweckbestimmung nach richtigen Adressaten übermittelt werden?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							

6.10.	Wird eine Übersicht/Liste über diejenigen Stellen geführt, an die Datenübermittlungen programmgesteuert stattfinden können?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
6.11.	Erfolgt eine revisionssichere Protokollierung der programmgesteuerten Übermittlungen durch Aufzeichnung des aufrufenden Verfahrens, Empfänger, Daten, Datum, Uhrzeit?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
6.12.	Erfolgt die Übermittlung der weitergegebenen Daten verschlüsselt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
6.13.	Wird bei der Weitergabe von Daten von den Möglichkeiten der Anonymisierung/Pseudonymisierung Gebrauch gemacht, soweit möglich?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
6.14.	Ist durch entsprechende Maßnahmen sichergestellt, dass eine Aufdeckung des Pseudonyms nicht oder nur sehr schwer möglich ist?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
7.	**Eingabekontrolle** – Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung, Dokumentenmanagement.						
7.1.	Ist dokumentiert, welche benutzer- oder verfahrensbezogene Auswertemöglichkeiten im Unternehmen eingesetzt werden?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
7.2.	Ist bekannt (und dokumentiert), welche Hilfsmittel (Audit-Programme) zur maschinellen Auswertung von Log-Dateien eingesetzt werden und welche Filterkriterien angewandt werden?	☐	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
7.3.	Ist geregelt, wie lange diese protokollierten Daten aufbewahrt werden dürfen?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
7.4.	Unterliegen diese Daten einer strengen Zweckbestimmung?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
7.5.	Finden stichprobenartig Kontrollen durch den DSB oder durch eine andere benannte Person statt (auch hinsichtlich der Einhaltung der Löschungsfristen)?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
7.6.	Sind die protokollierten Daten gegen unbefugte Einsicht oder Manipulation geschützt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
7.7.	Werden digitale Signaturverfahren zur Manipulationserkennung eingesetzt?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
Wahrung der Verfügbarkeit personenbezogener Daten (Art. 32 Abs. 1 lit. b) DS-GVO)							
8.	**Verfügbarkeitskontrolle** – Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV),						

	Virenschutz, Firewall, Meldewege und Notfallpläne; rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c) DS-GVO).						
8.1.	Wurde eine Risiko- und Schwachstellenanalyse durchgeführt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
8.2.	Wurden die Risikofaktoren gegen die Aufrechterhaltung des DV-Betriebes untersucht?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
8.3.	Ist das oder sind die Gebäude vor Überschwemmungen geschützt?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
8.4.	Wird in regelmäßigen Abständen überprüft, ob die Versorgung mit Fernmelde- und Datenleitungen, Strom, Wärme und Wasser noch ausreichend ist?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
8.5.	Ist die Art der Versorgungsleitungen unterirdisch?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
8.6.	Wurden die Netzwerk-Komponenten zum Zweck der Risikoverteilung und Ausfallminimierung auf mehrere geschützte Bereiche verteilt?	☐	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
8.7.	Befinden sich wasserführenden Leitungen (Heizung, Frisch- und Abwasser) in den Rechnerräumen?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
8.8.	Ist eine vollständige Dokumentation der eingesetzten Klimatechnik vorhanden?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
8.9.	Werden ausreichend dimensionierte USVs eingesetzt?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
8.10.	Ist dokumentiert, welche Geräte bei einem Ausfall der Stromversorgung wie lange versorgt werden?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
8.11.	Findet eine ständige Überwachung der Ausgangsspannung(en) statt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
8.12.	Verfügt die USV-Anlage über Überspannungsschutzeinrichtungen?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
8.13.	Gibt es Blitzschutzeinrichtungen?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:							
8.14.	Befinden sich im Serverbereich brennbaren Gegenstände wie Reinigungsmittel, Papiervorräte oder Papierabfälle (außer Tagesbedarf/Tagesanfall) oder Vorhänge?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:							
8.15.	Ist ein Frühwarnsystem mit automatischen Brandmeldern (Ionisations- oder Rauchmelder) installiert?	☒	Ja	☐	Nein	☐	Teilweise

Bemerkung:						
8.16. Wird das Brandmeldesystem regelmäßig gewartet?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.17. Sind Druckknopfmelder zur manuellen Alarmauslösung vorhanden und deutlich gekennzeichnet?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.18. Werden Alarmmeldungen des Frühwarnsystems weitergegeben (Leitstelle, Werkschutz (Brandmeldestelle), Polizei, Feuerwehr, externer Wachdienst, ...)?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.19. Sind ausreichend geeignete Feuerlöscher/Flutungsanlagen sowie das richtige Löschmittel im Einsatz und wird dabei auf Einheitlichkeit geachtet (z. B. ausschließlich CO^2-Löscher)?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.20. Findet eine regelmäßige Wartung und Überprüfung der Rauchmelder und Handfeuerlöscher statt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.21. Wurden alle in Frage kommenden Katastrophenmöglichkeiten untersucht (Streik, Personalausfall, Sachbeschädigung, Feuer, Explosion, Erdbeben, Wassereinbruch, längere Störungen oder Ausfälle der Infrastruktur)?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.22. Gibt es ein Backup-Rechenzentrum (Ausweichrechner, Ausweichräume)?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.23. Existiert ein Notfallhandbuch und wird dieses laufend aktualisiert?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
8.24. Wurde ein IT-Sicherheitsbeauftragter bestellt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.25. Ist die Verantwortlichkeit und Weisungsbefugnis im Katastrophenfall eindeutig geregelt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.26. Gibt es für den DV-Wiederanlauf eine schriftliche Unterlage (Zusammensetzung und Aufgaben des Katastrophenstabes)?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
8.27. Existiert ein Notfallkonzept für das Netzwerk?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.28. Finden regelmäßige Notfallübungen statt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.29. Sind die Anforderungen an das Backup in einem Backup-Konzept dokumentiert?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						

8.30. Sind die Backups ausreichend vor Diebstahl und Zerstörung geschützt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.31. Wurden Prozesse für die Sicherung erstellt und diese in Handlungsanweisungen dokumentiert?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
8.32. Wurden die für die Sicherung verantwortlichen Personen namentlich benannt und wurde dieses dokumentiert?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.33. Wird regelmäßig getestet, ob das Backup brauchbar ist?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.34. Existiert ein eigener Archivraum?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.35. Existiert ein Sicherheitsarchiv in einem anderen Gebäude oder Brandabschnitt?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
8.36. Ist der Zutritt zum Archiv auf einen genau festgelegten Personenkreis eingeschränkt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
8.37. Befinden sich wasserführenden Leitungen (Heizung, Frisch- und Abwasser) in den Räumlichkeiten des Archivs bzw. in den angrenzenden Wänden?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
9. Auftragskontrolle – Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Art. 32 DS-GVO).						
9.1. Sind alle Auftragsverarbeiter (z. B. der Steuerberater oder ggf. der Betreiber eines externen Archivs) vollständig vertraglich verpflichtet?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
9.2. Erfüllt der schriftliche Auftrag die Anforderungen des Regelungskatalogs des Art. 28 Abs. 3 a) bis h) DS-GVO?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
9.3. Hat sich der Auftraggeber vor Beginn der Verarbeitung von der Einhaltung des Datenschutzes bei dem Auftragnehmer überzeugt und kontrolliert er sodann regelmäßig die Einhaltung des Datenschutzes bei dem Auftragnehmer?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
9.4. Dokumentiert der Auftraggeber die Kontrollen bei dem Auftragnehmer?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
9.5. Ist klar festgelegt, welche Mitarbeiter des Auftraggebers gegenüber dem Auftragnehmer weisungsbefugt sind? Sind dem Auftragnehmer diese Personen bekannt?	☒	Ja	☐	Nein	☐	Teilweise

9.6. Erfolgen Weisungen schriftlich?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
10. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d), Art. 25 Abs. 1 DS-GVO).						
10.1. Ist ein Datenschutz-Managementsystem (DSMS) eingeführt?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
10.2. Ist ein Incident-Response-Management eingerichtet?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
10.3. Wurden alle Systeme gemäß Art. 42 DS-GVO datenschutzfreundlich eingestellt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
10.4. Werden regelmäßige IT-Sicherheitsaudits durchgeführt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
10.5. Wenn ja, in welchem Zyklus werden diese durchgeführt?	☒	Ja	☐	Nein	☐	Teilweise
Bemerkung:						
10.6. Ist das Unternehmen durch ein spezielles Verfahren gemäß Art. 42 DS-GVO durch die Aufsichtsbehörden zertifiziert?	☐	Ja	☒	Nein	☐	Teilweise
Bemerkung:						
10.7. Wenn ja, wie lautet der Name bzw. die Bezeichnung des Verfahrens?	Klicken oder tippen Sie hier, um Text einzugeben.					
Bemerkung:						

Anlage 3

Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

(Unternehmens-) Name und Anschrift	**Beschreibung der Leistung**	**Ort der Leistungserbringung**
ID.KOM Networks GmbH Dieselstr. 1 87437 Kempten	Hosting	Rechenzentrum Kempten
CHT GmbH & Co. KG Werner-von-Siemens Straße 6 86159 Augsburg	Externe Datensicherung Online-Backup	Rechenzentrum Augsburg