Vereinbarung zur Auftragsverarbeitung gem. Art. 28 EU-DSGVO zwischen

_____ _____ _____ (Nachstehend Auftraggeber genannt)	reitzner AG Johannes-Scheiffele-Straße 19 89407 Dillingen (Nachstehend Auftragnehmer genannt)

1. Allgemeines

Diese Vereinbarung wird als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Vorgaben der EU-Datenschutzgrundverordnung, insbesondere Artikel 28 EU-DSGVO („Auftragsverarbeitung") geschlossen. Den Parteien ist bekannt, dass ab dem 25.05.2018 die Datenschutz-Grundverordnung (DSGVO - EU-Verordnung 2016/679) gilt und sich die Vorgaben der Auftragsverarbeitung dann grundsätzlich nach Art. 28 DSGVO richten.
Der Auftragnehmer führt im Auftrag des Auftraggebers unten selektierte Arbeiten des Auftraggebers durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Pflege durchzuführen oder durchführen zu können.

2. Dauer und Beendigung des Auftrags

(1) Die Dauer dieser Auftragsverarbeitung entspricht der Laufzeit der Partnerschaft und den Leistungsvereinbarungen der Produkte und Dienste der reitzner AG.

Datenschutzbeauftragter Auftraggeber _____ _____ Tel _____ Email _____	Datenschutzbeauftragter Auftragnehmer Herr Thomas Hoch Tel 0152 53144668 Email datenschutzbeauftragter@reitzner.de

3. Gegenstand des Auftrags
Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind im Folgenden beschrieben:

Zweck:

- ☐ Installations-, Wartungs- und Fehlerbehebungsarbeiten an Telefonanlagen und anderer Hardware vor Ort und/oder per Fernwartung
- ☐ Installations-, Wartungs- und Fehlerberhebungsarbeiten an Servern, PCs, Notebooks, Infrastruktur und anderer Hardware vor Ort und/oder per Fernwartung
- ☐ Installations-, Wartungs- und Fehlerbehebungsarbeiten an Multifunktionsgeräten, Druckern, Infrastruktur und anderer Hardware vor Ort und/oder per Fernwartung
- ☐ Systempflege durch Installation, Update und Fehlerbeseitigung von eingesetzter Software vor Ort und/oder per Fernwartung
- ☐ Überwachung der Kundensysteme zur vorzeitigen Erkennung von Fehlern
- ☐ Dropdrive, Onlinespeicher
- ☐ Bereitstellung und Wartung eines ASP-Systems in einem Rechenzentrum der reitzner AG

Art der Daten:
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, etc.
Kreis der Betroffenen:
Kunden, Interessenten, Abonnenten, Beschäftigte i. S. d. Art. 28 EU-DSGVO, Lieferanten, Handelsvertreter, Ansprechpartner, etc.

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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 DS-GVO erfüllt sind.

4. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Wartung und Pflege gegenüber dem Auftragnehmer zu erteilen. Weisungen können schriftlich, per Fax, per E-Mail oder mündliche erfolgen

(2) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Wartung und Pflege durch den Auftragnehmer feststellt.

5. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, auf die er im Zusammenhang mit den Wartungs-/Pflegearbeiten Zugriff erhält, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(3) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(4) Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

- besondere Arten bzw. besondere Kategorien personenbezogener Daten i.S.d-Art. 9 DSGVO oder
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

(5) Der Auftragnehmer wird ab dem 25.5.2018 seinen Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verarbeitungsverzeichnisses nachkommen.

6. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber nach Art. 58 DSGVO i.V.m. § 40 BDSG (neu), insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

7. Fernwartung

(1) Sofern der Auftragnehmer die Wartung und/oder Pflege auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

(2) 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.

(3) 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.

8. Unterauftragsverhältnisse
(1) Die Beauftragung von Subunternehmen durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig.
(2) Der Auftragnehmer hat den Subunternehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. nach Art. 37 DSGVO i.V.m. § 38 BDSG (neu) bestellt hat, soweit dieser gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet ist.
(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Subunternehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.
(4) Die Verpflichtung des Subunternehmens muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.
(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 5 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

9. Datengeheimnis / Verschwiegenheit
(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des Art. 28 DSGVO zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.
(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes, auch explizit auf den § 203 StGB zu besonderen Verschwiegenheit betreffende Berufsgruppen vertraut macht, und diese auf das Datengeheimnis verpflichtet wurden. Ab dem 25.5.2018 wird der Auftragnehmer stattdessen die in Satz 2 genannten Personen in einer dem Art. 28 Abs. 3 lit. b) genügenden Weise zur Vertraulichkeit verpflichten, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

10. Wartung von Betroffenenrechten
Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

11. Technische und organisatorische Maßnahmen zur Datensicherheit
(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind.
(2) Für den Fall, dass der Auftragnehmer die Wartung und Pflege für den Auftraggeber auch außerhalb der Geschäftsräume des Auftraggebers durchführt (z.B. auch im Falle der Fernwartung), sind vom Auftragnehmer zwingend die von ihm getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO als **ANLAGE** zu diesem Vertrag zu dokumentieren. Dies beinhaltet auf Aufforderung des Auftraggebers auch Nachweise über das nach Art. 32 Abs. 1 lit. d) einzurichtende Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

12. Beendigung
(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.
(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

13. Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland, wobei die Geltung des UN-Kaufrechts ausgeschlossen wird.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

_____ , den _____		_____ , den _____	
Ort	Datum	Ort	Datum
_____		_____	
Stempel, Unterschrift (Kunde)		Stempel, Unterschrift (reitzner AG)	

Anlagen:
I. Beschreibung der Technischen und Organisatorischen Maßnahmen
II. Auszug EU-DSGVO Art. 28, 30 (Stand: 2018)
III. Muster Mitarbeiter-Verpflichtungserklärung zum Datenschutz der reitzner AG (optional)

Anlage I. - Beschreibung der Technischen und Organisatorischen Maßnahmen

1. Allgemeine Maßnahmen	**Ja**	**Nein**	
Ist ein Datenschutzbeauftragter bestellt?	☒	☐	Name: MMC, Thomas Hoch Kontaktdaten: info@thomashoch.de Ist bestellt seit: 01.06.2012
Sind die Mitarbeiter auf das Datengeheimnis verpflichtet?	☒	☐	Vorlage eines Verpflichtungsmusters (Siehe Anlage)
Werden die Mitarbeiter laufend in die Anforderungen des Datenschutzes eingewiesen?	☒	☐	☐ Schulungsnachweise vorhanden ☒ andere Nachweise: Anwesenheitsliste der Datenschutzunterweisung, Verschwiegenheitsverpflichtung
Gibt es ein Datenschutzkonzept bzw. ein Datenschutzhandbuch zur Regelung und Umsetzung des Datenschutzes im Unternehmen?	☒	☐	☒ Konzept vorhanden / in Überarbeitung ☐ Datenschutzhandbuch vorhanden ☐ Zertifikat vorhanden ☐ Verfahrensanweisung vorhanden über:
Wird die Datenverarbeitung auf dem Gebiet der Bundesrepublik Deutschland bzw. innerhalb der Europäischen Union oder der Staaten des Europäischen Wirtschaftsraums durchgeführt?	☒	☐	Ggf. in welchem Staat außerhalb dieses Gebietes?
2. Technische und organisatorische Maßnahmen			
2.1 Zutrittskontrolle			
Besteht eine Regelung/Verfahren zur Besucherführung?	☒	☐	☒ Empfang ☐ Besucherbuch ☐ Besucherausweis ☒ Persönliche Besucherführung ☐ Sonstiges:
Sind Zutrittssicherungen eingerichtet?	☒	☐	☒ Zutrittskontrollsystem ☐ mit ☐ ohne Sicherheitszonen ☒ Zentrales Schließsystem ☒ Sicherheitsschlösser ☒ Schlüsselregelung inkl. Dokumentationen ☐ Sonstiges:
Sind sonstige Schutzmaßnahmen eingerichtet?	☒	☐	☐ Pförtner ☐ Wachdienst ☒ Alarmanlage ☐ Sonstiges:

2.2 Zugangskontrolle			
Sind Maßnahmen zur Zugangskontrolle zum Desktop und zu den vernetzten Systemen eingerichtet?	☒	☐	☒ Userkennung ☒ Sicheres Passwort ☒ Passwortwiederholungssperre nach Fehlversuchen ☐ Andere Verfahren:
Ist eine zeitgesteuerte passwortgeschützte Pausenschaltung (Bildschirmschoner) eingerichtet?	☐	☒	
Sind die vernetzten Systeme gegen unbefugtes Eindringen geschützt?	☒	☐	☒ Firewall ☒ Virenscanner ☐ Schnittstellenschutz (Netzwerkschaltschränke, Schutz nicht benötigter Netzwerksteckdosen etc.) In Form von:
Bestehen sonstige Maßnahmen der Zugriffskontrolle, z.B.?	☒	☐	☒ Programmprüfungs- und Freigabeverfahren ☒ Protokollierung und Auswertung von sicherheitskritischen Vorfällen ☒ WLAN gegen unbefugten Zugang abgesichert ☐ Sonstige Maßnahmen:
2.3 Zugriffskontrolle			
Besteht ein Berechtigungsprofil, das sicherstellt, dass jeder Mitarbeiter nur über die Zugriffsbefugnisse verfügt, die er zur Aufgabenerledigung benötigt?	☒	☐	differenziert nach ☐ Leseberechtigung ☐ Schreibberechtigung ☐ Sonstigen Berechtigungen: Rolle und Organisationseinheit
Sind die festgelegten Berechtigungen nachvollziehbar dokumentiert?	☒	☐	In welcher Form?
2.4 Trennungskontrolle			
Sind die Daten der verschiedenen Kunden in geeigneter Weise voneinander getrennt, um eine getrennte Verarbeitung zu gewährleisten?	☒	☐	Art der Trennung Logische Trennung auf ☐ Betriebssystemebene ☒ Anwendungsebene (V-LAN) ☐ Mandantentrennung ☐ Physikalische Trennung
2.5 Pseudonymisierung			
Die Verarbeitung personenbezogener Daten erfolgt 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 entsprechende technischen und organisatorischen Maßnahmen unterliegen.	☒	☐	

2.6 Eingabekontrolle

Werden die Benutzung von Datenverarbeitungssystemen und die Eingabe von Daten protokolliert?	☒	☐	Protokollierung der Dateibenutzung: ☐ Ja ☒ Nein Protokollierung von Eingaben und Veränderungen: ☐ Datenfeldbezogen ☒ Datensatzbezogen ☐ Dateibezogen ☐ Keine Protokollierung

2.7 Weitergabekontrolle

Werden die Daten bei ihrer Übertragung vor unbefugter Kenntnisnahme geschützt?	☒	☐	☒ Verschlüsselung ☒ Sichere Verbindungen, z.B. VPN ☒ Sonstige Maßnahmen: Virenscanner ☐ Es findet keine Datenübertragung statt
Werden Datenübermittlungen nachvollziehbar protokolliert und kontrolliert?	☐	☒	Wie und in welcher Form? ☒ Es findet keine Datenübertragung statt
Werden Schnittstellen von PCs und externe Laufwerke (mobile Festplatten, USB-Sticks etc.) gegen Missbrauch geschützt?	☐	☒	☐ Sperrung unbefugter Geräte ☐ Protokollierung der Nutzung ☐ Verschlüsselung der mobilen Datenträger ☐ Sicherheitsrichtlinien ☐ Sonstiges:
Ist die sichere Nutzung mobiler Datenträger geregelt?	☐	☒	Wie und in welcher Form?
Ist eine sichere Löschung/Entsorgung von Datenträgern gewährleistet?	☒	☐	Wie ist die Löschung/Entsorgung geregelt? Fa. Reisswolf (Dillingen/Augsburg) (siehe Beiblatt) Fa. Büchl (Ingolstadt/Neuburg) (siehe Beiblatt)
Erfolgt bei Fernwartung der Zugriff auf die Kundendaten und Kundensysteme nur über sichere Leitungen?	☒	☐	Wie sind die Leitungen gesichert? ☒ VPN ☒ Verschlüsselung ☐ Sonstiges: Ist dies auch bei einem Zugriff von anderen Stellen aus der Fall, z.B. im Home-Office Betrieb? ☒ Ja ☐ Nein

2.8 Auftragskontrolle

Wird die Durchführung des Kundenauftrags/der Serviceaktion nachvollziehbar überwacht, um eine auftragskonforme Erledigung zu gewährleisten?	☒	☐	In welcher Form? Manuelle Protokollierung bzgl. Fakturierung

2.9 Verfügbarkeitskontrolle			
Sind die Kundendaten durch geeignete Sicherungsverfahren vor Zerstörung und Verlust geschützt?	☒	☐	z.B. ☒ Gespiegelter Datenbestand ☒ Regelmäßige Sicherungskopien/ Backup-Lösung ☐ Sonstiges: Gibt es ein Sicherungskonzept, in dem die Art und Weise einer regelmäßigen Sicherung und die Rekonstruktion der Daten festgelegt ist? ☒ Ja ☐ Nein
Werden die Sicherungsbestände sicher verwahrt?	☒	☐	In welcher Weise? Zutrittsgesicherter Serverraum
2.10 Prüfung / Bewertung / Evaluierung			
Datenschutz-Management	☐	☐	
Incident-Response-Management	☐	☐	
Datenschutzfreundliche Voreinstellung	☐	☐	

Anlage II. - Auszug aus dem EU-DSGVO (Datenschutzgrundverordnung) Art. 28, Art. 30**, Art. 32**

Art. 28 DSGVO – Auftragsdatenverarbeiter

1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.
2) [1]Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. [2]Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.
3) [1]Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. [2]Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter
   a. die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;
   b. gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
   c. alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
   d. die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
   e. angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;
   f. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;
   g. nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,
   h. dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

   Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.
4) [1]Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. [2]Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.
5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.
6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.
7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 93 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.
8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.
9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.
10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Art. 30 DSGVO – Verzeichnis von Verarbeitungstätigkeiten

1) [1]Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. [2]Dieses Verzeichnis enthält sämtliche folgenden Angaben:
   a. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
   b. die Zwecke der Verarbeitung;
   c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
   d. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
   e. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
   f. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
   g. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.
2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:
   a. den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
   b. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
   c. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
   d. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.
3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.
4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.
5) Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

Art. 32 DSGVO – Sicherheit der Verarbeitung

1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
   a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
   b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
   c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
   d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.