Vereinbarung zur Auftragsverarbeitung

im Rahmen des Nutzungsverhältnisses „DachProfi24.online“

AUFTRAGNEHMER und AUFTRAGGEBER im Sinne dieser Vereinbarung sind die Parteien des Vertrags über die Nutzung der Plattform „DachProfi24.online“ und der darauf bereit gestellten Dienste (nachfolgend als „Plattform“ bezeichnet) auf Grundlage der Nutzungsbedingungen „DachProfi24.online“. Die dort als Kunde bezeichnete Partei ist der AUFTRAGGEBER.

Die Vertragsdurchführung geht bei bestimmten Diensten mit der Verarbeitung von personenbezogenen Daten einher, weshalb die Parteien den Vertrag bezüglich einzelner Dienste inhaltlich um die gem. Art. 28 Abs. 3 DS-GVO erforderlichen Inhalte ergänzen. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Ergänzungsvereinbarung zur Auftragsverarbeitung:

§ 1 Vertragsbestandteile

Folgende Anlagen sind Bestandteil dieser Vereinbarung:

Anlage			BESCHREIBUNG
AVV1			Übersicht Auftragsverarbeitung
AVV2			Genehmigte Subunternehmen
AVV3			Technische und organisatorische Maßnahmen

§ 2 Einzelheiten zu den Verarbeitungen

(1) Der AUFTRAGNEHMER erbringt für den AUFTRAGGEBER Leistungen im Bereich der Plattform auf Grundlage der Nutzungsbedingungen „DachProfi24.online“. Dabei erhält der AUFTRAGNEHMER Zugriff auf personenbezogene Daten und verarbeitet diese im Umfang der Anlage AVV1 im Auftrag und nach Weisung des AUFTRAGGEBERS. Die Dauer der Verarbeitungen entspricht der Dauer der Erbringung der vertragsgemäßen Leistungen.

(2) Umfang sowie Art und Zweck der Auftragsverarbeitung durch den AUFTRAGNEHMER ergeben sich aus dem Vertrag über die Nutzung der Plattform und den dazugehörigen Leistungsbeschreibungen in Verbindung mit Anlage AVV1.

(3) Die Regelungen der vorliegenden Vereinbarung gehen im Falle von Widersprüchen den Regelungen des Vertrags über die Nutzung der Plattform vor.

(4) Diese Vereinbarung ergänzt lediglich den Vertrag über die Nutzung der Plattform, so dass ihre Inhalte zum Bestandteil jenes Vertrags werden. Diese Vereinbarung kann über das Ende jenes

Vertrags hinaus Geltung erlangen, sofern sich dies aus den nachfolgenden Bestimmungen ergibt.

§ 3 Weisungsrecht

(1) Der AUFTRAGNEHMER darf Daten nur im Rahmen des Vertrags über die Nutzung der Plattform und gemäß den Weisungen des AUFTRAGGEBERS verarbeiten. Wird der AUFTRAGNEHMER durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen berechtigt, darf er diese ausführen (etwa zur Erfüllung von ihn treffenden gesetzlichen Verpflichtungen). Vor Ausführung derartiger Verarbeitungen, die auf gesetzlicher Grundlage, aber außerhalb des Auftrags des AUFTRAGGEBERS liegen, teilt der AUFTRAGNEHMER dem AUFTRAGGEBER die rechtlichen Anforderungen vor der Verarbeitung mit, sofern ihm eine solche Mitteilung nicht auf gesetzlicher Grundlage untersagt ist.

(2) Die Weisungen des AUFTRAGGEBERS werden anfänglich durch diesen Vertrag festgelegt und können vom AUFTRAGGEBER danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der AUFTRAGGEBER ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Durchführung von Verarbeitungen im Einzelfall, insbesondere ob eine Verarbeitung durchgeführt wird oder nicht. Dem Weisungsrecht unterliegen nicht die Auswahl der Mittel der Verarbeitung sowie technische oder organisatorische Schutzmaßnahmen. Derartige Änderungen sind einvernehmlich zu vereinbaren, wobei der AUFTRAGNEHMER Änderungswünsche des AUFTRAGGEBERS nicht unbillig ablehnen wird.

(3) Alle erteilten Weisungen sind vom AUFTRAGGEBER zu dokumentieren. Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der AUFTRAGNEHMER der Ansicht, dass eine Weisung des AUFTRAGGEBERS gegen datenschutzrechtliche Bestimmungen verstößt, hat er den AUFTRAGGEBER unverzüglich darauf hinzuweisen. Der AUFTRAGNEHMER ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den AUFTRAGGEBER bestätigt oder geändert wird. Der AUFTRAGNEHMER darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen. Die Bestätigung oder Änderung einer Weisung ist nur wirksam, wenn sie in schriftlicher Form oder in Textform erteilt werden.

§ 4 Art der verarbeiteten Daten, Kreis der Betroffenen

Im Rahmen der Durchführung des Vertrags über die Nutzung der Plattform erhält der AUFTRAGNEHMER Zugriff auf die dort spezifizierten personenbezogenen Daten. Der Kreis der betroffenen Personen ist ebenfalls im Vertrag über die Nutzung der Plattform dargestellt.

§ 5 Schutzmaßnahmen

(1) Der AUFTRAGNEHMER wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der AUFTRAGNEHMER trifft die erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des AUFTRAGGEBERS i.S.v. Art. 32 DS-GVO, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen (s. Anlage AVV3). Dem AUFTRAGGEBER sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

(2) Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem AUFTRAGNEHMER vorbehalten, wobei von diesem sicherzustellen ist, dass das bei Vertragsschluss gegebene Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den AUFTRAGNEHMER beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Der AUFTRAGNEHMER wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b) DS-GVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung kontrollieren.

§ 6 Informationspflichten

(1) Im Falle der Verletzung des Schutzes personenbezogener Daten wird der AUFTRAGNEHMER den AUFTRAGNEHMER unverzüglich informieren, sofern Daten betroffen sind, die im Auftrag des AUFTRAGGEBERS verarbeitet werden.

(2) Der AUFTRAGNEHMER trifft unverzüglich Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen.

(3) Sollten die Daten des AUFTRAGGEBERS bei dem AUFTRAGNEHMER durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der AUFTRAGNEHMER den AUFTRAGGEBER unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der AUFTRAGNEHMER wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim AUFTRAGGEBER als „Verantwortlichem“ im Sinne der DS-GVO liegt.

§ 7 Kontrollrechte des AUFTRAGGEBERS

(1) Der AUFTRAGGEBER hat das Recht, Kontrollen des AUFTRAGNEHMERS – einschließlich Inspektionen vor Ort – durchzuführen. Gegenstand des Kontrollrechts ist die Einhaltung der

Vorgaben dieses Vertrags sowie jener aus Art. 28 DS-GVO. Der AUFTRAGNEHMER wirkt an den Kontrollen mit, indem er z.B. Auskünfte erteilt, vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegt oder die technischen und organisatorischen Maßnahmen nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten zur Überprüfung stellt, welche der AUFTRAGEBER selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen kann, sofern dieser Dritte nicht in einem Wettbewerbsverhältnis zu dem AUFTRAGNEHMER steht. Der AUFTRAGGEBER wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des AUFTRAGNEHMERS dabei nicht unverhältnismäßig stören.

(2) Der AUFTRAGNEHMER verpflichtet sich, dem AUFTRAGGEBER auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen erforderlich sind.

(3) Der AUFTRAGGEBER dokumentiert das Kontrollergebnis und teilt es dem AUFTRAGNEHMER mit. Bei Fehlern oder Unregelmäßigkeiten, die der AUFTRAGGEBER insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den AUFTRAGNEHMER unverzüglich zu informieren.

§ 8 Einsatz von Subunternehmern

(1) Der AUFTRAGNEHMER ist im Allgemeinen berechtigt, zur Leistungserbringung Dritte als weitere Auftragsverarbeiter einzusetzen.

(2) Ausdrücklich genehmigt wird mit Vertragsschluss die Einschaltung der in Anlage AVV2 genannten Subunternehmer.

(3) Über beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines weiteren Auftragsverarbeiters informiert der AUFTRAGNEHMER den AUFTRAGGEBER. Der AUFTRAGGEBER ist berechtigt, binnen 5 Werktagen nach Zugang einer solchen Information Einspruch gegen den neuen Auftragsverarbeiter zu erheben. Im Falle des Einspruchs unterbleibt die beabsichtigte Einsetzung des neuen weiteren Auftragsverarbeiters.

(4) Die gesetzlichen Pflichten aus Art. 28 Abs. 2 und 4 DS-GVO sind dem AUFTRAGNEHMER bekannt und werden von diesem eingehalten.

§ 9 Unterstützungspflichten

(1) Der AUFTRAGNEHMER unterstützt den AUFTRAGGEBER im Rahmen der vereinbarten Leistungen mit darin enthaltenen technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten zur Erfüllung der Rechte betroffener Personen.

(2) Ferner unterstützt der AUFTRAGNEHMER unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den AUFTRAGGEBER bei der Erfüllung von dessen Pflichten aus den Art. 32 bis 36 DS-GVO, sofern und soweit solche

Unterstützungsleistungen dem AUFTRAGNEHMER zumutbar und zur Erfüllung der Pflichten des AUFTRAGGEBERS unverzichtbar sind. Der AUFTRAGGEBER und AUFTRAGNEHMER arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem AUFTRAGNEHMER geltend, so verweist er den Betroffenen unverzüglich an den AUFTRAGGEBER.

§ 10 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zu dem AUFTRAGNEHMER alleine der AUFTRAGGEBER gegenüber dem Betroffenen verantwortlich. Dies gilt nicht, sofern der AUFTRAGNEHMER seinen datenschutzrechtlichen Pflichten als Auftragsverarbeiter nach Maßgabe der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des AUFTRAGGEBERS oder gegen dessen Anweisungen gehandelt hat.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie nach Maßgabe des Abs. 1 im Innenverhältnis nicht verantwortlich ist. Entsprechendes gilt im Falle eines etwaigen Mitverschuldensanteils.

§ 11 Beendigung des Vertrags über die Nutzung der Plattform

(1) Der AUFTRAGNEHMER wird dem AUFTRAGGEBER nach Beendigung des Vertrags über die Nutzung der Plattform oder jederzeit auf dessen Anforderung alle personenbezogenen Daten zurückgeben und etwaig verbliebene Kopien löschen oder – auf Wunsch des AUFTRAGGEBERS – löschen. Eine Verpflichtung zur Löschung besteht nicht, sofern nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten für den AUFTRAGNEHMER besteht

(2) Der AUFTRAGNEHMER ist verpflichtet, auch über das Ende des Vertrags über die Nutzung der Plattform hinaus die ihm im Zusammenhang mit dem Vertrag über die Nutzung der Plattform bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Vertrags über die Nutzung der Plattform hinaus so lange gültig, wie der AUFTRAGNEHMER die zuvor im Auftrag verarbeiteten personenbezogene Daten noch nicht zurückgegeben bzw. auf Wunsch des AUFTRAGGEBERS gelöscht hat.

Anlage AVV1.

„Übersicht Auftragsverarbeitungen“

zur Vereinbarung zur Auftragsverarbeitung „DachProfi24.online“

HAUPTVERTRAG	ART DER DATEN	BETROFFENE[1]	SUBUNTERNEHMER[2]
MARKETING			
Websitebaukasten	Inhaltsdaten; Verbindungsdaten/Logdaten	2 (Besucher); 4	1, 3
Sanierungsrechner	Daten über das Sanierungsvorhaben	2	1
Dachfensterkonfigurator	Kommunikationsdaten; Kundendaten; Projektdaten	2	1
MEIN BÜRO			
MEINE DATEIABLAGE	Diverse Daten des Verantwortlichen	1; 2; 3;	1, 2
OFFICE ANWENDUNGEN	Inhaltsdaten	1; 2; 3; 4	1, 2
CRM	Kundendaten; Projektdaten	2	1
MASCHINENVERWALTUNG	Maschinendaten	1; 2	1
BAUTAGEBUCH /BAUSTELLENVERWALTUNG	Projektdaten	1; 2; 3	1
ERP			1, 2
Buchhaltung	Forderungen und Verbindlichkeiten; Belege; Debitoren-/Kreditorendaten; Berichte	1; 2; 3	
Vermögenswerte	Inventardaten; Anlagenbuchführungsdaten		
Einkauf	Lieferantendaten; Angebots-/Vertragsdaten	1; 3; 4	
Kalkulation	Kundendaten; Angebotsdaten	1; 2	
CRM	Kundendaten; Projektdaten	2; 3	
Projekte	Kundendaten;	1; 2; 3	
HR	Personaldaten	1	
Lohn- und Gehalt	Mitarbeiterstammdaten; Lohn- und Gehaltsdaten; Bankdaten; sonstige Lohn- und Gehaltsdaten	1; 4	
Beschaffung	Angebots-/Vertragsdaten	3;	
Zeiterfassung	Mitarbeiterstammdaten; Arbeitszeiten; Urlaub; Krankheit	1	

[1] Mitarbeiter = 1
Interessenten/Kunden = 2
Lieferanten = 3
Sonstige = 4

[2] Zu den Subunternehmern vgl. Anlage 2

Anlage AVV2

„Genehmigte Subunternehmer“

zur Vereinbarung zur Auftragsverarbeitung „DachProfi24.online“

NR.	SUBUNTERNEHMEN	ANSCHRIFT / ORT DER DV	GEGENSTAND DER DV
1.	**Zedach eG**	Humpertshof 2 59069 Hamm Deutschland	Hosting, Administration und Wartung der Plattform
2.	**ALYF GmbH**	Demmeringstr. 57, 04177 Leipzig Deutschland	Entwicklung DACHERP
3.	**Jannis Gebauer**	Vorstadt 21 55411 Bingen am Rhein	Entwicklung und automatische Konfiguration der digitalen Plattform
4.	**Tomislav Pree**	Oggersheimerstr. 3 67112 Mutterstadt	Entwicklung und Frontendentwicklung

Anlage AVV3

„Technische und organisatorische Maßnahmen“

zur Vereinbarung zur Auftragsverarbeitung „DachProfi24.online“

1 Grundsatz

Art. 32 DS-GVO bestimmt, dass der Verantwortliche und der Auftragsverarbeiter geeignete technische- und organisatorische Maßnahmen treffen müssen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Maßnahmen müssen unter Berücksichtigung des Standes 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 getroffen werden.

2 Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter als auch die von ihm eingesetzten Subunternehmen haben insbesondere die folgenden Maßnahmen getroffen:

2.1 Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten

Die Pseudonymisierung und Verschlüsselung von im Auftrag verarbeiteter personenbezogener Daten obliegt grundsätzlich dem Verantwortlichen.

2.2 Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

2.2.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

☒	Alarmanlage
☒	Sicherheitsschlösser
☒	Chip-/Transponder-Schließsystem
☒	Allgemeines Schlüsselvergabekonzept
☒	Schlüsselkonzept RZ/Serverraum
☒	verschlossener Serverschrank in RZ

☒	sorgfältige Auswahl Wachpersonal
☒	Besucherkonzept
☒	sorgfältige Auswahl Reinigungspersonal

2.2.2 Zugangskontrolle

Durch die Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Auf die Serverumgebung selbst können nur die IT zugreifen.

2.2.2.1 Allgemein

	Maßnahmen
☒	Rollen- und Berechtigungskonzept
☒	Zuordnung von Benutzerrechten
☒	Passwortvergabe
☒	Erstellen von Benutzerprofilen
☒	Anmeldung mit Benutzername/Passwort
☒	Antivirensoftware
☒	Einsatz einer Hardwarefirewall
☒	Einsatz einer Softwarefirewall
☒	Intrusion Detection und Intrusion Prevention System

2.2.2.2 Interne Systeme des Auftragsverarbeiters

	Zusätzliche Maßnahmen
☒	Sperren von USB-Ports
☒	Sperren bestimmter Ports
☒	Einsatz von VPN-Verbindungen
☒	Verschlüsselung von Datenträgern / mobilen Endgeräten
☒	Verschlüsselung von Smartphone-Inhalten
☒	Mobile Device Management

2.2.3 Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

2.2.3.1 Allgemein

	Maßnahmen
☒	Rollen- und Berechtigungskonzept
☒	Rechteverwaltung durch Admin
☒	Anzahl Adminrollen so gering wie möglich

2.2.3.2 Interne Systeme des Auftragsverarbeiters

	Zusätzliche Maßnahmen
☒	Passwortrichtlinie (inkl. Passwortlänge, Passwortwechsel)
☒	Protokollierung von Zugriffen auf Anwendungen (insbesondere bei Eingabe, Änderung, Löschung von Daten)
☒	Sichere Aufbewahrung von Datenträgern
☒	physische Löschung von Datenträgern vor Wiederverwendung
☒	ordnungsgemäße Vernichtung von Datenträgern
☒	Einsatz von Aktenvernichtern/Dienstleister
☒	Protokollierung der Vernichtung (z.B. Vernichtszertifikat durch Dienstleister)
☒	Verschlüsselung von Datenträgern
☒	Automatisches Ausloggen bei Inaktivität (z.B. Bildschirmsperre bei Abwesenheit)

2.2.4 Verfügbarkeitskontrolle

Durch die Verfügbarkeitskontrolle wird gewährleistet, dass personenbezogene Daten gegen den zufälligen Verlust geschützt sind.

	Maßnahmen
☒	Backup- und Recoverykonzept
☒	USV
☒	Klimaanlage in RZ

	Maßnahmen
☒	Temperaturüberwachung / Feuchtigkeitsüberwachung in RZ
☒	Schutzsteckdosenleisten in RZ
☒	Feuer- und Rauchmeldeanlagen in RZ
☒	Alarmmeldung bei unberechtigten Zutritten zu den Serverräumen
☒	Serverräume nicht unter sanitären Anlagen
☒	Erstellen eines Notfallplans
☒	Spiegelung der Systeme
☒	Regelmäßige Erstellung von Sicherheitskopien
☒	Aufbewahrung von Datensicherungen in anderen Brandabschnitten
☒	Testen von Datenwiederherstellung

2.2.5 Trennungsgebot

Durch das Trennungsgebot wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

	Maßnahmen
☒	physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
☒	logische Mandantentrennung
☒	Festlegung von Datenbankrechten
☒	Trennung Produktiv- und Testsystem

2.2.6 Eingabekontrolle

Durch die Eingabekontrolle wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind.

	Maßnahmen des Auftragsverarbeiters (intern)
☒	Vergabe von Änderungs- Lösch- und Bearbeitungsrechten aufgrund eines Rollen & Berechtigungskonzeptes
☒	Logfilekontrolle
☒	Protokollierung von Stammdatenänderungen
☒	Nachvollziehbarkeit von Eingabe, Änderung, Löschung von Daten durch individuelle Nutzer

	Maßnahmen des Auftragsverarbeiters (intern)
☒	Protokollierung von Zugriffen auf Anwendungen (insbesondere bei Eingabe, Änderung, Löschung von Daten)
☒	Protokollierung der Serveraktivitäten
☒	Protokollierung gescheiterter Zugriffsversuche

2.2.7 Transportkontrolle

Bei der Transportkontrolle wird gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports, ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

	Maßnahmen des Auftragsverarbeiters (intern)
☒	VPN-Tunnel bei externen Geräten
☒	E-Mail-Verschlüsselung
☒	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung
☒	sichere Transportbehälter
☒	Sorgfältige Auswahl Transportpersonal

2.2.8 Auftragskontrolle

Durch die Auftragskontrolle wird gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

	Maßnahmen
☒	Vereinbarung über die Auftragsverarbeitung
☒	Auswahl des Unterauftragnehmers unter Sorgfaltsgesichtspunkten
☒	schriftliche Weisungen an den Auftragnehmer
☒	Verpflichtung Mitarbeiter des Auftragnehmers auf den Datenschutz / Verschwiegenheitspflichten
☒	Auftragnehmer hat Datenschutzbeauftragten bestellt (wenn gesetzlich vorgeschrieben)
☒	Sicherstellung der Vernichtung von Daten nach Vertragsende
☒	Kontrollrechte gegenüber dem Auftragnehmer

2.3 Maßnahmen zur Sicherstellung der Wiederherstellbarkeit und Verfügbarkeit und dem Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall

	Maßnahmen
☒	Incident-Management
☒	Backup- und Recoverykonzept
☒	Erstellen eines Notfallplans
☒	Verfügbarkeitskontrolle (s.o.)

2.4 Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Die getroffenen Maßnahmen müssen einer regelmäßigen Kontrolle unterzogen werden. Auch sind sie dem jeweils entsprechenden Stand der Technik anzupassen und aktuell zu halten. Im Unternehmen wird ein solches regelmäßiges Kontroll- und Evaluierungskonzept wie folgt umgesetzt:

	Maßnahmen
☒	Etablierung einer Datenschutz- und Informationssicherheitsorganisation
☒	Benennung eines Datenschutzbeauftragten (DSB)
☒	Benennung eines Informationssicherheitsbeauftragten (ISB)
☒	Regelmäßige Mitarbeiterschulungen- und Prüfungen
☒	Verpflichtung sämtlicher Mitarbeiter auf Vertraulichkeit im Umgang mit personenbezogenen Daten und zur Verschwiegenheit
☒	Dokumentation (Verzeichnis) von Verarbeitungstätigkeiten und Datenschutzfolgenabschätzungen (bei Bedarf)
☒	Regelmäßige Prüfung der technischen Komponenten und des Backup- und Recoverykonzepts
☒	Etablierung von Leitlinien und Richtlinien zum Datenschutz- und Informationssicherheitsmanagement
☒	Etablierung von Prozessen zur Wahrnehmung von Betroffenenrechten und sonstigen Verhaltensregelungen zum Schutze von personenbezogenen Daten und zur Informationssicherheit
☒	Wartungsprotokolle technischer Komponenten
☒	Regelmäßiges Einspielen von Patches und Softwareupdates