Auftragsverarbeitungsvertrag nach EU-DSGVO

Zwischen _____

_____

_____

- nachfolgend „Auftraggeber“ genannt -

und **Kaysser Heimtiernahrung GmbH**
In der Schorbach 14
67714 Waldfischbach-Burgalben

- nachfolgend „Auftragnehmer“ genannt -

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Die Parteien sind durch eine Direktversand-Vereinbarung miteinander verbunden. Der Auftraggeber verkauft Waren des Auftragnehmers im eigenen Namen und auf eigene Rechnung. Zur Abwicklung der jeweiligen Vertragsverhältnisse zwischen dem Auftraggeber und den Endkunden überträgt der Auftraggeber an den Auftragnehmer Daten der Endkunden, damit dieser im Auftrag des Auftraggebers die Ware an den Endkunden versendet. Inhalt des Vertrages ist die Regelung der datenschutzrechtlichen Fragen zwischen Auftraggeber und Auftragnehmer.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrages durch den Auftraggeber oder den Auftragnehmer.

(3) Datenschutzbeauftragter

Abel und Kollegen Rechtsanwälte PartGmbB
Kaiserstraße 77
66386 St. Ingbert
Deutschland

Tel.: 06894 / 3272
Fax: 06894 / 382185
E-Mail: kanzlei@abel-kollegen.de

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Zweck Verarbeitung	Rechtsgrundlage	Kategorien von Daten	Dauer und Ort der Speicherung
Auftragsbearbeitung, Buchhaltung	Vertrag, gesetzliche Bestimmungen, unser berechtigtes Interesse	Fremd- und selbsterhobene Daten	Vertragsdauer, Dauer der Aufbewahrungs- und Schadensersatzpflicht lt. Gesetz, bei Einwilligung bis auf Widerruf. Bei Websites können Cookies deaktiviert werden, damit keine Verarbeitung erfolgt. Die Daten werden auf Servern bei unserem Provider in Hamburg gespeichert.
Webseiten, Kontaktformulare	Konkludente Einwilligung, (vor)vertragliche Maßnahmen, unser berechtigtes Interesse	Daten lt. Formulare, Cookies, IP-/MAC Adressen	

Die Erbringung der 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 Auftragsgebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien

Personenstammdaten
(Name, Vorname, Lieferanschrift, ggf. E-Mail Adresse und Telefonnummer)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen

Kunden

3. Technisch-organisatorische Maßnahmen

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

(2) Der Auftragnehmer hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c. 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten

und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

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

4. Berichtigung, Einschränkung und Löschung der Daten

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

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzepte, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 und 22 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Soweit der Auftragnehmer gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet ist wird er dessen Kontaktdaten dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitteilen. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

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

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

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

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

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

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

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

6. Unterauftragsverhältnisse

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

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

(3) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

(4) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

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

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

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- Die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- Die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO

- Aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- Eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSIGrundschutz)

8. Mitteilung bei Verstößen des Auftragnehmers

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

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

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

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

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgeeinschätzung

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

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. in schriftlicher Form)

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

10. Löschung und Rückgabe von personenbezogenen Daten

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

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinem Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber

auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

Waldfischbach-Burgalben, 07.12.2023 _____

Kaysser Heimtiernahrung GmbH – Auftragnehmer –

_____, _____ _____

- Auftraggeber –

Anlage: Maßnahmen zur Gewährleistung der Schutzziele

Die Gewährleistungsziele finden ihren ganz wesentlichen Anker in den Grundsätzen der Verarbeitung personenbezogener Daten in Art. 5 DS-GVO, die wiederum den Schutzauftrag aus Art. 8 der Charta der Grundrechte der Europäischen Union aufnehmen.

Die DS-GVO verpflichtet die verantwortlichen Stellen und verarbeitenden Organisationen dazu, zur Gewährleistung des grundrechtlichen Schutzes der Rechte der Betroffenen sowie gegen unbefugte Zugriffe durch Dritte die dafür angemessenen technischen und organisatorischen Maßnahmen (insbesondere Art. 32 DS-GVO) auszuwählen und im Rahmen der Technikgestaltung und datenschutzfreundlicher Voreinstellungen gemäß Art. 25 DS-GVO einzusetzen und zu prüfen (Art. 32 I d). Der Verantwortliche ist für die Einhaltung der Grundsätze der Verarbeitung nach Art. 5 Abs. 1, 24 DS-GVO verantwortlich und muss dessen Einhaltung nachweisen können. Weitere Erläuterungen finden sich in ErwGr 39 „Grundsätze der Datenverarbeitung“.

Folgende Maßnahmen werden durch Kaysser Heimtiernahrung GmbH, Waldfischbach-Burgalben getroffen:

1. Transparenz

Der Grundsatz der Transparenz ist in Art. 5 Abs. 1 lit. a DS-GVO festgeschrieben. Er findet sich als tragender Grundsatz des Datenschutzrechts in zahlreichen Regelungen der DS-GVO. Insbesondere die Informations- und Auskunftspflichten tragen ihm Rechnung.

Maßnahmen zur Gewährleistung der Transparenz sind:

X	Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren
	Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren
X	Dokumentation der Verträge mit den internen Mitarbeitern, Verträgen mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen
X	Dokumentation von Einwilligungen und Widersprüchen
	Protokollierung von Zugriffen und Änderungen (Teilweise)
X	Nachweis der Quellen von Daten (Authentizität)
	Versionierung (Teilweise)
	Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts
	Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept

2. Datenminimierung

Das Gewährleistungsziel Datenminimierung findet sich unmittelbar begrifflich im Verordnungstext wieder: In Art. 5 Abs. 1 lit. c und lit. e DS-GVO steht, dass personenbezogene Daten dem Zweck angemessen und erheblich, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen.

Das Gewährleistungsziel Datenminimierung wird erreicht durch:

X	Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
X	Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
X	Bevorzugung von automatisierten Verarbeitungsprozessen, die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerter Prozesse
	Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren
X	Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren

Datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung (Art. 25 Abs. 2 DS-GVO)

	Technische Maßnahmen		Organisatorische Maßnahmen
X	Beschränkung der Angaben und weiteren Verwendung auf das notwendige Maß	X	Transparente Datenverarbeitung
	Automatisierte Löschfunktionen für nicht mehr benötigte Daten / Lifecycle-Management	X	Regelungen zur Datenminimierung, Datensparsamkeit, Erforderlichkeit
	Durch den Betroffenen auswählbare Sicherheitseinstellungen	X	Einhaltung der Branchenstandards
	Automatisierte Erinnerungsfunktion zur Überprüfung erteilter Einwilligungen	X	Minimierung von Pflichtfeldern
	Verwendung von Opt-In-Lösungen		Deutliche Kennzeichnung von freiwilligen Angaben

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

Die Verpflichtung zur Wahrung der Vertraulichkeit ergibt sich insbesondere aus Art. 5 Abs. 1 lit. f DS-GVO, aus Art. 32 Abs. 1 lit. b DS-GVO sowie Art. 38 Abs. 5 DS—GVO (Geheimhaltungspflicht des Datenschutzbeauftragten) bzw. Art. 28 Abs. 3 lit. b DS-GVO (Geheimhaltungspflicht des Auftragsverarbeiters). Es gewährleistet den Schutz vor unbefugter und unrechtmäßiger Verarbeitung. Eine Verletzung der Vertraulichkeit stellt in der Regel eine Datenverarbeitung ohne Rechtsgrundlage dar.

Maßnahmen zur Gewährleistung der Vertraulichkeit sind:

X	Festlegung eine Rechte- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle
	Implementierung eines sicheren Authentifizierungsverfahrens
	Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen
	Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle, spezifizierte, für das Verfahren ausgestattete Umgebungen (Gebäude, Räume)
X	Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarung etc.)
	Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept)
X	Schutz vor äußeren Einflüssen (Spionage, Hacking)

a) Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

	Technische Maßnahmen		Organisatorische Maßnahmen
	Alarmanlage		Personenkontrolle beim Pförtner

	Absicherung von Gebäudeschächten		Protokollierung der Besucher
	Automatisches Zutrittskontrollsystem	X	Schlüsselregelung / Schlüsselbuch
	Biometrische Zutrittssperren		Sorgfältige Auswahl von Sicherheitspersonal
	Chipkarten-/Transponder-Schließsystem		Tragepflicht von Mitarbeiter- / Gästeausweisen
	Lichtschranken / Bewegungsmelder		Sicherheitszonen mit verschiedenen Zutrittsberechtigungen
X	Manuelles Schließsystem		Werkschutz
	Schließsystem mit Codesperre		Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
X	Sicherheitsschlösser		
	Videoüberwachung der Zugänge Eingang und Notausgang		

b) Zugangskontrolle: Keine unbefugte Systemnutzung

	Technische Maßnahmen		**Organisatorische Maßnahmen**
X	Authentifikation mit Benutzer + Passwort	X	Benutzerberechtigungen verwalten
	Authentifikation mit biometrischen Daten	X	Regelmäßige Überprüfung der Berechtigungen
	Zwei-Faktor-Authentifizierung		Definierte Passwortregeln
X	Einsatz von Firewalls		Passwortfreigabeverfahren
	Einsatz von Mobile Device Management		Passwortrücksetzungsverfahren
	Einsatz von VPN-Technologie		
	Gehäuseverriegelungen		
X	Sperren von externen Schnittstellen (z.B. USB Ports)		
X	Einsatz von Anti-Viren-Software		
X	Einsatz automatischer Bildschirmschoner		

c) Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

	Technische Maßnahmen		**Organisatorische Maßnahmen**
X	Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)	X	Anzahl der Administratoren auf das „Notwendigste“ reduzieren
X	Physische Löschung von Datenträgern vor deren Wiederverwendung	X	Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifizierung)
	Protokollierung der Vernichtung von Daten		Erstellen eine Berechtigungskonzepts
X	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten		Passwortrichtlinie, inkl. Länge und Wechsel
	Verschlüsselung von Datenträgern		Sichere Aufbewahrung von Datenträgern
	Verschlüsselung von Smartphones	X	Verwaltung der Benutzerrechte durch Systemadministratoren
			Mehraugen-Prinzip
		X	Einsatz von Aktenvernichtern
			Vergabe von Berechtigungen nach dem Need-to-Know-Prinzip

d) Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

	Technische Maßnahmen		**Organisatorische Maßnahmen**

	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten System		Erstellung eines Berechtigungskonzepts
	Anonymisierung von Datensätzen		Versehen der Datensätze mit Zweckattributen / Datenfeldern
	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	**X**	ID wird nur einmalig mit dem personengebundenen Datensatz verbunden. Anschließend erfolgt die Verarbeitung anonymisiert
X	Trennung von Produktiv- und Testsystem		
	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden		
X	Logische Mandantentrennung (softwareseitig)		

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifisch betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

	Technische Maßnahmen		**Organisatorische Maßnahmen**
X	Kürzung der Datensätze um identifizierende Merkmale (z.B. IP-Adresse)	**X**	Anweisungen / Regelungen zur möglichst frühzeitigen Verfremdung von Datensätzen
	Verfremdung von identifizierenden Merkmalen durch Eigen- oder Fremdsoftware		Erstellung von Verfremdungskonzepten
	Löschung von identifizierenden Merkmalen vor Übermittlung		Festlegung von Verfremdungsregeln
	Ausschluss der (Re-)Identifizierung von Merkmalen durch Berichtigungen		Dokumentation von Einsatzbereichen der Verfremdungsregeln / -konzepte

f) Auftragskontrolle: Auftragsverarbeitung im Sinne von Art. 28 DS-GVO

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	…	**X**	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
			Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechende Dokumentation der Nachweise
			Regelmäßige Überprüfung des Auftragnehmers hinsichtlich Datenschutz / Datensicherheit
		X	Abschluss von Verträgen zur Auftragsverarbeitung unter Berücksichtigung aller gesetzlichen Anforderungen gemäß Art. 28 DS-GVO
			Überprüfung aller vertraglich zugesicherten technischen Maßnahmen (ggf. vor Ort)

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

Das Gewährleistungsziel der Integrität ist in Art. 5 Abs. 1 lit. f DS-GVO als Grundsatz für die Verarbeitung von Daten und in Art. 32 Abs. 1 lit. b DS-GVO als Voraussetzung für die Sicherheit einer Datenverarbeitung genannt. Es soll unbefugte Veränderungen und Entfernungen ausschließen.

Maßnahmen zur Gewährleistung der Integrität bzw. zur Feststellung von Integritätsverletzungen sind:

	Einschränkung von Schreib- und Änderungsrechten
	Einsatz von Prüfsummen, elektronische Siegel und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts
X	Dokumentierte Zuweisung von Berechtigungen und Rollen
	Prozesse zur Aufrechterhaltung der Aktualität von Daten
	Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen
	Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Einrichtung von VPN-Tunneln		Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
X	E-Mail-Verschlüsselung		Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
	Verschlüsselung von Anhängen		Sorgfältige Auswahl von Transportpersonal und –fahrzeugen
	Sichere Transportbehälter/-verpackungen		Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
	Elektronische Signatur		

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B. Protokollierung, Dokumentenmanagement

	Technische Maßnahmen		**Organisatorische Maßnahmen**
X	Protokollierung der Eingabe, Änderung und Löschung der Daten	**X**	Aufbewahren von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
			Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
		X	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
		X	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

5. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. d DS-GVO)

Der Grundsatz der Verfügbarkeit ist in Art. 32 Abs. 1 lit. b und lit. c DS-GVO explizit im Kontext der Sicherheit von Datenverarbeitungen aufgenommen. Es ist zudem in Art. 5 Abs. 1 lit. e DS-GVO als Voraussetzung für die Identifizierung der betroffenen Person verankert. Es gewährleistet die Verfügbarkeit der Daten zu dem jeweiligen Zweck, solange dieser noch besteht. Der Grundsatz kommt zum Tragen bei den Informations- und Auskunftspflichten (Art. 13 und 15 DS-GVO)

gegenüber den Betroffenen. Für das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) ist das Gewährleistungsziel der Verfügbarkeit ebenso Grundvoraussetzung.

Maßnahmen zur Gewährung der Verfügbarkeit sind:

X	Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts
X	Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
	Dokumentation der Syntax von Daten
X	Redundanz von Hard- und Software, sowie Infrastruktur
	Umsetzung von Reparaturstrategien und Ausweichprozessen
	Vertretungsregelungen für abwesende Mitarbeiter

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Schutz gegen zufällige oder mutwillige Zerstörung sowie Verlust und Vorkehrungen, um möglichst schnell die Daten wieder herzustellen

	Technische Maßnahmen		**Organisatorische Maßnahmen**
X	Feuerlöschgeräte in Serverräumen		Regelmäßige Durchführung von Krisen- / Notfallübungen
	Feuer- und Rauchmeldeanlagen	**X**	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen		Erstellen eines Backup- und Recoverykonzepts
	Klimaanlage in Serverräumen	**X**	Erstellen eines Notfallplans
	Schutzsteckdosenleisten in Serverräumen		Festlegung von Meldewegen
X	Unterbrechungsfreie Stromversorgung (USV)		Testen von Datenwiederherstellung
	Doppelte IT-Infrastruktur (Redundanz)	**X**	Serverräume nicht unter sanitären Anlagen
	Regelmäßige Belastungstests		

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

Datenschutz-Management

	Technische Maßnahmen		**Organisatorische Maßnahmen**
	Regelmäßige Penetrationstests	**X**	Bestellung eines Datenschutzbeauftragten
	Regelmäßige Prüfung der Hardware (Lifecycle, Performance)		Bestellung eines IT-Sicherheitsbeauftragten
	Incident-Response-Management	**X**	Regelmäßiges Berichtswesen an die Geschäftsführung
		X	IT-Sicherheitskonzept
		X	Datenschutzkonzept
			Eskalationsverfahren für Notfälle
			Regelmäßige Auditierung / Zertifizierung durch Externe
			Regelmäßige interne Überprüfung / Aktualisierung der getroffenen Maßnahmen gemäß dem Stand der Technik (durch DSB, IT, Revision etc.)

7. Nichtverkettung

Die Verpflichtung, Daten nur für den Zweck zu verarbeiten, zu dem sie erhoben wurden, ist insbesondere den einzelnen Verarbeitungsbefugnissen zu entnehmen, die die Geschäftszwecke, die Forschungszwecke etc. zum Maßstab machen und findet über den Zweckbindungsgrundsatz aus Art. 5 Abs. 1 lit. c DS-GVO Eingang in die Grundverordnung. Bei der Datenverarbeitung auf der Grundlage der Einwilligung ergibt sich aus Art. 7 Abs. 4 DS-GVO, das eine Einwilligung unwirksam sein kann, wenn die Daten zur Zweckerfüllung nicht erforderlich sind.

Eine typische Maßnahme der Nichtverkettung ist etwa die Pseudonymisierung und wird beispielsweise in Art. 40 Abs. 2 lit. d DS-GVO genannt.

Maßnahmen zur Gewährleistung der Nichtverkettung sind:

	Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
	Programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten
	Regelnde Maßgabe zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
	Trennung nach Organisations- / Abteilungsgrenzen
X	Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentifizierungsverfahrens
	Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle
	Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten
	Geregelte Zweckänderungsverfahren

8. Intervenierbarkeit

Die Interventionsrechte der Betroffenen ergeben sich explizit aus den Vorschriften zu Berichtigung, Sperrung, Löschung und zum Widerspruch (Art. 16, 17 DS-GVO). Sie können sich außerdem als Ergebnis einer Interessenabwägung im Rahmen eines gesetzlichen Erlaubnistatbestandes ergeben. Wiederum müssen die verantwortlichen Stellen gemäß Art. 5 Abs. 1 lit. d DS-GVO die Voraussetzung für die Gewährung dieser Rechte, sowohl auf organisatorischer als auch, soweit erforderlich, auf technischer Ebene schaffen.

Maßnahmen zur Gewährung der Intervenierbarkeit sind:

	Differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
X	Schaffung notwendiger Datenfelder z.B. für Sperrkennzeichen, Benachrichtigung, Einwilligungen, Widersprüche, Gegendarstellungen
X	Dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes
X	Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
	Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und / oder Durchsetzung von Ansprüchen
	Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte
X	Einrichtung eines Single Point of Contact (SPoC) für Betroffene
	Operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten