AUFTRAGSVERARBEITUNGSVEREINBARUNG

GEMÄß ART. 28 UND 29 DSGVO

VEREINBARUNG

zwischen dem / der

Hees GmbH
Leimbachstraße 266
57074 Siegen
GERMANY

- nachstehend Auftraggeber genannt –

und der

- nachstehend Auftragnehmer genannt –

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags

(Definition der Aufgaben)

Versionsdatum: 12.06.2024

Dauer des Auftrags

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder *(insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)*

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum ☐☐.☐☐.☐☐☐☐

oder

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von ☐☐ zum ☐☐.☐☐.☐☐☐☐ gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Auftragsinhalt

Der Auftragnehmer ist verpflichtet, die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich zur vertraglich vereinbarten Leistung zu verwenden.

Dem Auftragnehmer ist es gestattet, verfahrens- und sicherheitstechnisch erforderliche Zwischen-, Temporär- oder Duplikatsdateien zur leistungsgemäßen Verarbeitung oder Nutzung der personenbezogenen Daten zu erstellen, soweit dies nicht zu einer inhaltlichen Umgestaltung führt.

Dem Auftragnehmer ist nicht gestattet, unautorisiert Kopien der personenbezogenen Daten zu erstellen.

Daten aus Adressbüchern und Verzeichnissen dürfen nur zur Kommunikation im Rahmen der Auftragserfüllung mit dem Auftraggeber verwendet werden. Eine anderweitige Nutzung und Übermittlung für eigene oder fremde Zwecke, einschl. Marketingzwecke, ist nicht gestattet.

Weitere Einzelheiten zu Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder –nutzung sind unter Buchstabe A. der Anlage 1 zu dieser Vereinbarung aufgeführt.

Die Art der personenbezogenen Daten sind unter Buchstabe B. der Anlage 1 aufgeführt.

Der Kreis der Personen ist unter Buchstabe C. der Anlage 1 aufgeführt.

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer trifft alle erforderlichen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, soweit ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Die insoweit konkret getroffenen Maßnahmen ergeben sich aus Anlage 2 zu dieser Vereinbarung.

Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind die technischen und organisatorischen Maßnahmen durch den Auftragnehmer fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der hier und in der Anlage 2 festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber, auf Anfrage, die für die Führung der internen Verarbeitungsübersicht nach DSGVO erforderlichen Angaben zur Verfügung zu stellen.

4. Berichtigung, Sperrung und Löschung von Daten

Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags nach Art. 28, 29 u. EG81ff folgende Pflichten:

- Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 37 Abs. 1 DSGVO ausüben kann. Die Kontaktdaten des Datenschutzbeauftragten entnehmen Sie bitte der Anlage 3.

- Die Wahrung des Datengeheimnisses entsprechend Art. 29 DSGVO. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf das Datengeheimnis verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

- Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen entsprechend Art. 24, 25, 32, 35, 36 u. EG 78, 98ff DSGVO und Anlage.

- Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Dies gilt auch, soweit eine zuständige Behörde nach Art. 34 DSGVO beim Auftragnehmer ermittelt.

- Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftragnehmer im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags.

- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach ISO 27001 oder VdS 3473) vorlegen.

6. Unterauftragsverhältnisse

Soweit bei der Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers Unterauftragnehmer einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

- Die Einschaltung von Unterauftragnehmern ist grundsätzlich nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne schriftliche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung unter Wahrung seiner unter Punkt 5 erläuterten Pflicht zur Auftragskontrolle konzernangehörige Unternehmen sowie im Einzelfall andere Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung oder Nutzung mitteilt.

- Der Auftragnehmer hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer/n so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.

- Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

7. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu Art. 5, 25, 32, 35, 36 DSGVO vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

Im Hinblick auf mögliche Kontrollverpflichtungen des Auftraggebers vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO, und der Anlage 2 nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. ISO 27001 oder VdS 3473) erbracht werden.

8. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

Es ist bekannt, dass nach Art. 34 DSGVO Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach Art. 34 DSGVO treffen, hat der Auftragnehmer ihn hierbei zu unterstützen.

9. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate 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.
Der Auftragnehmer hat den Auftraggeber unverzüglich entsprechend zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte 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.

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 übergeben.

Datum, Ort

_____

(Auftraggeber)

Datum, Ort

_____

(Auftragnehmer)

Anlage 1: A. Ergänzungen zu Punkt 2 Umfang, Art und Zweck der Datenverarbeitung
B. Aufführung der Art der Daten gemäß § 2
C. Kreis der Personen gemäß § 2

Anlage 2: Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Anlage 3: Datenschutzbeauftragter gemäß Art. 37 Abs. 1 DSGVO

ANLAGE 1

A. Zu § 2 Ergänzungen zu Umfang, Art und Zweck der Datenverarbeitung

B. Zu § 2 Art der personenbezogenen Daten

(maßgebliche Datenarten sind angekreuzt)

☐ Adressdaten, ☐ Kontaktdaten, ☐ Vertragsdaten, ☐ Bankverbindungsdaten, ☐ Kontodaten,
☐ Abrechnungsdaten inkl. Bonuszahlungen, ☐ Leistungsdaten, ☐ Finanzdaten, ☐ Angebotsdaten,
☐ Mitarbeiter-/Personaldaten, ☐ Pensionsdaten, ☐ Bewerberdaten, ☐ Qualifikationsdaten,
☐ Videoaufzeichnungen, ☐ Gesundheitsdaten, ☐ Angaben zur Konfessionszugehörigkeit,
☐ Angaben zu Schwerbehinderungen, ☐ Krankheitsdaten, ☐ Zeitdaten,
☐ Informationen zu Abfindungszahlungen, ☐ Reisebuchungs- und kostendaten,
☐ Kreditkartenabrechnungen

Andere Kategorien personenbezogener Daten:

C. Zu § 2 Kreis der Personen

☐ Mitarbeiter
☐ Kunden
☐ Praktikanten
☐ Bewerber
☐ Lieferanten/Dienstleister
☐ sonstige

ANLAGE 2

Bei der HEES Gruppe werden folgende technische und organisatorische Maßnahmen getroffen, um den Schutz von Daten zu gewährleisten, dies schließt personenbezogene Daten jeder Kategorie ein.

- Passwörter müssen in allen Systemen ein angemessenes Sicherheitsniveau aufweisen, dies wird technisch erzwungen
- Zutritt zu internen Bereichen wird Gästen nur nach Registrierung oder unter Aufsicht gestattet
- Datenlöschung und die Vernichtung von Datenträgern erfolgen immer nach festgelegtem Schema und entsprechen dem Stand der Technik
- Mobile Datenverarbeitung unterliegt immer den gleichen Sicherheitsregularien wie die Datenverarbeitung im Hause
- Zugriffsrechte von Nutzern sind immer auf das notwendige Maß beschränkt
- Werden Notebooks oder Tablets verwendet, so sind die Datenträger immer verschlüsselt. Wechseldatenträger sind ebenfalls verschlüsselt, zusätzlich unterliegt der Einsatz dieser strengen Regularien
- Ausstattung darf von Mitarbeiter/innen nicht verändert werden, somit wird sichergestellt, dass nur zugelassene Hardware verwendet wird
- E-Mails werden sicher archiviert und nach vorgegebener Zeit automatisiert gelöscht
- Der Computerbildschirm wird beim Verlassen des Arbeitsplatzes gesperrt und es liegen keine Dokumente mit personenbezogenen Daten auf dem Schreibtisch, wenn dieser verlassen wird
- Auf mehreren Ebenen wird Antiviren- und Malwareschutz eingesetzt, um Daten vor Offenlegung oder Verlust zu schützen
- Externe Arbeit unterliegt den gleichen Regularien und ist ausschließlich auf Firmengeräten mit eingeschalteter VPN-Verbindung erlaubt
- Mobile Endgeräte unterliegen einem Mobile Device Management, somit ist eine sichere Löschung jederzeit möglich
- Es finden regelmäßig Datenschutz und Information Security Awareness Schulungen statt, um Mitarbeiter für diese Bereiche zu sensibilisieren und aktuellstes Wissen zu vermitteln

Jeder der aufgeführten Punkte gilt für alle Mitarbeiter/innen des Auftragnehmers und sollen den Mitarbeitern Handlungssicherheit im Umgang mit personenbezogenen Daten geben.

Für Rückfragen und Auskünfte benennt der Auftragnehmer folgende/n Mitarbeiter/in:

Name, Anschrift, Tel., E-Mail:

ANLAGE 3

Zur/m Datenschutzbeauftragte/n für das Unternehmen des Auftragnehmers wurde bestellt:

Name, Anschrift, Tel., E-Mail:

Anlage: Vereinbarung zur Verarbeitung von Daten im Auftrag

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

des Auftragnehmers:

Als nicht-öffentliche Stelle, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen wir technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Insbesondere sind Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammen- hang mit der Datenverarbeitung sicherzustellen. Die folgenden technischen und organisatorischen Maßnahmen sind dazu in unserem Unternehmen umgesetzt (zutreffendes ist angekreuzt):

1. VERTRAULICHKEIT (ART. 32 ABS. 1 LIT. B EU-DSGVO)

a) Zutrittskontrolle/Gebäudeabsicherung

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

- ☑ Alarmanlage
- ☐ Absicherung von Gebäudeschächten
- ☐ Automatisches Zutrittskontrollsystem
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ Schließsystem mit Codesperre
- ☐ Manuelles Schließsystem
- ☐ Biometrische Zugangssperren
- ☐ Videoüberwachung der Zugänge
- ☐ Lichtschranken / Bewegungsmelder
- ☐ Sicherheitsschlösser
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☐ Protokollierung der Besucher
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Einsatz von sorgfältig ausgewähltem Wachpersonal
- ☐ Tragepflicht von Berechtigungsausweisen
- ☐
- ☐

b) Zugangskontrolle/Absicherung Systemzugang

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

- ☐ Zuordnung von Benutzerrechten
- ☐ Einsatz von individuellen Benutzernamen
- ☐ Vorgaben für sichere Passwörter
- ☐ Authentifikation mit biometrischen Verfahren
- ☐ Authentifikation mit Benutzername/ Passwort
- ☐ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☐ Gehäuseverriegelungen am Server/ Rechnern
- ☐ Einsatz von VPN-Technologie (Fernzugriff)
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Einsatz von Intrusion-Detection-Systemen
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum Fern-Löschen)
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Sichere Passwörter für Smartphones
- ☐ Verschlüsselung von Datenträgern in Laptops
- ☐ Einsatz von individuellen Benutzernamen
- ☐
- ☐

c) Zugriffskontrolle/Sicherstellung von Zugriffsberechtigungen

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

- ☐ Erstellen eines Berechtigungskonzepts
- ☐ Verwaltung der Rechte durch Systemadministrator
- ☐ Anzahl der Administratoren auf das „Notwendigste“reduziert
- ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☐ Protokollierung der Vernichtung
- ☐ Verschlüsselung von Datenträgern
- ☐ Einsatz von Anti-Viren-Software
- ☐ Einsatz einer Hardware-Firewall
- ☐ Einsatz einer Software-Firewall
- ☐
- ☐

d) **Trennungskontrolle/Maßnahmen zur Zwecktrennung von Daten**

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Erstellung eines Berechtigungskonzepts
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Festlegung von Datenbank-Rechten
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Keine Produktivdaten in Testsystemen
- ☐
- ☐

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 spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- ☐ Verarbeitung von Daten in pseudonymisierter Form
- ☐

2. INTEGRITÄT (ART. 32 ABS. 1 LIT. B EU-DSGVO)

a) **Weitergabekontrolle/Sicherheit beim Datentransfer**

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

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- ☐
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☐ Verschlüsselung externer Datenträger bei Weitergabe (CDs, USB-Sticks etc.)
- ☐

b) **Eingabekontrolle**

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

- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐

3. VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B EU-DSGVO)

a) **Verfügbarkeitskontrolle/Schutz von Daten vor zufälliger Zerstörung und Verlust**

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Erstellen eines Backup- und Recoverykonzepts
- ☐ Serverräume über der Wasser grenze (nur in Hochwasser-gebieten relevant)
- ☐
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Erstellen eines Notfallplans
- ☐ Serverräume nicht unter sanitären Anlagen
- ☐

b) **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)**

- ☐ Wiederherstellung nach Backup- und Recoverykonzept
- ☐ Kontrolle eines Notfallplans
- ☐ Testen von Datenwiederherstellung
- ☐

4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D DS- GVO; ART. 25 ABS. 1 EU-DSGVO)

a) **Datenschutz-Management**

- ☐ Die Grundsätze zum Datenschutz (Erhebung, Verarbeitung oder Nutzung personenbezogener Daten) sind einer unternehmensinternen Richtlinie festgelegt.
- ☐ Der DSB ist bei der Datenschutzfolgeabschätzung eingebunden
- ☐ Es ist ein Datenschutzbeauftragter schriftlich benannt
- ☐ Der DSB ist im Organigramm eingebunden
- ☐ Verpflichtung der Mitarbeiter auf das Daten- und Fernmeldegeheimnis
- ☐ Schulung von Mitarbeitern
- ☐ Die interne Verarbeitungsübersicht der Verarbeitungsprozesse ist vorhanden
- ☐ Kontrollsystems, das den unberechtigten Zugriff auf personenbezogene Daten aufdeckt
- ☐
- ☐

b) **Incident-Response-Management**

- ☐ Einrichtung eines Incident Management-Plans
- ☐ Sicherheitsteam ist benannt und geschult
- ☐ Team mit realitätsnahen Übungen getestet
- ☐

c) **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**

- ☐ Beachtung privacy by design
- ☐ Beachtung privacy by
- ☐
- ☐

d) **Auftragskontrolle/Einbindung von Unter-Auftragsverarbeiter**

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

- ☐ Auswahl der (Unter-)Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☐ Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z. B. durch Auftragsdatenverarbeitungsvertrag)
- ☐ Auftragsverarbeiter hat Datenschutz-beauftragten bestellt (wenn erforderlich)
- ☐ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- ☐
- ☐ Vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- ☐ Verpflichtung der Mitarbeiter des Auftragsverarbeiter auf das Datengeheimnis/ Vertraulichkeit
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Laufende Überprüfung des Auftragsverarbeiter und seiner Tätigkeiten
- ☐

_____
Ort, Datum

_____
Befugte Person (in Druckbuchstaben)

_____
Unterschrift der befugten Person