

# **Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO (ENTWURF)**

## **Vereinbarung**

zwischen der

**Donau-Iller-Nahverkehrsverbund-GmbH**  
**Söflinger Straße 100,**  
**89077 Ulm**

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

**(FIRMA, ADRESSE)**

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

## **1. Gegenstand und Dauer des Vertrags**

### **(1) Gegenstand**

- Der Gegenstand des Vertrags ergibt sich aus der Leistungsvereinbarung/dem SLA/dem Auftrag ..... vom ....., auf die/den/das hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

- Gegenstand des Vertrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: ..... (Beschreibung der Aufgaben)

## **(2) Dauer**

- Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

- Der Vertrag beinhaltet eine einmalige Ausführung.

oder

- Die Dauer dieses Vertrags (Laufzeit) ist befristet bis zum .....

oder

- Der Vertrag wird für unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

## **2. Konkretisierung des Vertragsinhalts**

### **(1) Art und Zweck der vorgesehenen Verarbeitung von Daten**

- Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung vom ..... konkret beschrieben

oder

- Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:  
.....

## (2) Art der Daten

- Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter:  
.....

oder

- Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)
  - ☐ Personenstammdaten
  - ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
  - ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
  - ☐ Kundenhistorie
  - ☐ Vertragsabrechnungs- und Zahlungsdaten
  - ☐ Planungs- und Steuerungsdaten
  - ☐ Auskunftsangaben (von Dritten, z.B. Auskunftsteilen oder aus öffentlichen Verzeichnissen)

...

## (3) Kategorien betroffener Personen

- Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:  
.....

oder

- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
  - ☐ Kunden

- ☐ Interessenten
- ☐ Abonnenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ...

### **3. Technisch-organisatorische Maßnahmen**

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [Anlage 1]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzen.

### **4. Rechte von betroffenen Personen**

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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 die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

## **5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Die Wahrung der Vertraulichkeit gemäß Artt. 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 berechtigterweise 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 zur Verarbeitung verpflichtet sind.
- b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem

anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

- e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, 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.
- f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.
- g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.
- h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.
- i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

## 6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der

Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

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

- a) ☐ Eine Unterbeauftragung ist unzulässig.
- b) ☐ Der Auftraggeber stimmt der Beauftragung der in Anhang 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

- c) ☐ Die Auslagerung auf Unterauftragnehmer oder
  - ☐ der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmers sind zulässig, soweit:
    - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht überschreiten darf, vorab schriftlich oder in Textform anzeigt und
    - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
    - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.



(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

- ist nicht gestattet;
- bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
- bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

## 7. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

- Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen



Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

- Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland an die in Anlage 2 genannten Empfänger. In der Anlage werden die vom Auftraggeber genehmigten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

## **8. Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen 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 während der üblichen Geschäftszeiten 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 nachzuweisen.

(3) Der Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den 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 BSI-Grundschutz).

## 9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(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 wird.

## 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 aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen 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.

## 11. [OPTIONAL] Aufnahme weiterer Vertragsparteien

Verantwortliche oder Auftragsverarbeiter, die nicht Partei dieses Vertrags sind, können, mit Zustimmung der Vertragsparteien, diesem Vertrag jederzeit beitreten, indem sie die Anlagen dieses Vertrages ausfüllen und unterzeichnen.

ENTWURF

## **[OPTIONAL] Anlage X – Beitrittserklärung**

Hiermit erklärt die

<b>Firma/Geschäftsbezeichnung der Partei:</b>	
<b>Anschrift:</b>	
<b>Registerdaten:</b>	
<b>Ort und Datum:</b>	
<b>Name des/der Unterzeichner(s):</b>	
<b>Unterschrift(en):</b>	

ihren Beitritt als Partei gemäß Ziff. 11 dieses Vertrages. Zudem erklärt sie ihren Beitritt in der nachfolgenden Rolle:

Verantwortlicher	<input type="checkbox"/>
Auftragnehmer (Unterauftragnehmer)	<input type="checkbox"/>

### **Beschreibung der Verarbeitung:**

#### **(1) Gegenstand**

- Der Gegenstand der Verarbeitung ergibt sich aus der Leistungsvereinbarung/  
dem SLA/dem Auftrag ..... vom  
....., auf die/den/das hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

- Gegenstand der Verarbeitung ist die Durchführung folgender Aufgaben durch den Auftragnehmer:  
..... (Beschreibung der Aufgaben)

## **(2) Dauer**

- Die Dauer dieser Verarbeitung (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

oder (insbesondere, falls keine Leistungsvereinbarung zur Dauer besteht)

- Die Verarbeitung beinhaltet eine einmalige Ausführung.

oder

- Die Dauer dieser Verarbeitung (Laufzeit) ist befristet bis zum .....

oder

- Die Verarbeitung erfolgt für unbestimmte Zeit und kann von beiden Parteien mit einer Frist von ..... zum ..... gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

## **(3) Art und Zweck der vorgesehenen Verarbeitung von Daten**

- Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind in der Leistungsvereinbarung vom ..... konkret beschrieben

oder

- Nähere Beschreibung des Vertragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: .....

## **(4) Art der Daten**

- Die Art der verwendeten personenbezogenen Daten ist in der Leistungsvereinbarung konkret beschrieben unter: .....

oder

- Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

☐ Personenstammdaten

- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Kundenhistorie
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben (von Dritten, z.B. Auskunftsteilen oder aus öffentlichen Verzeichnissen)
- ☐ ...

## **(5) Kategorien betroffener Personen**

- Die Kategorien der durch die Verarbeitung betroffenen Personen sind in der Leistungsvereinbarung konkret beschrieben unter:  
.....

oder

- Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
  - ☐ Kunden
  - ☐ Interessenten
  - ☐ Abonnenten
  - ☐ Beschäftigte
  - ☐ Lieferanten
  - ☐ Handelsvertreter
  - ☐ Ansprechpartner
  - ☐ ...

# Anlage 1 – Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

## 1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

### 1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Alarmanlage	<input type="checkbox"/> Schlüsselregelung / Liste
<input type="checkbox"/> Automatisches Zugangskontrollsystem	<input type="checkbox"/> Empfang / Rezeption / Pförtner
<input type="checkbox"/> Biometrische Zugangssperren	<input type="checkbox"/> Besucherbuch / Protokoll der Besucher
<input type="checkbox"/> Chipkarten / Transpondersysteme	<input type="checkbox"/> Mitarbeiter- / Besucherausweise
<input type="checkbox"/> Manuelles Schließsystem	<input type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input type="checkbox"/> Sicherheitsschlösser	<input type="checkbox"/> Sorgfalt bei Auswahl des Wachpersonals
<input type="checkbox"/> Schließsystem mit Codesperre	<input type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste
<input type="checkbox"/> Absicherung der Gebäudeschächte	<input type="checkbox"/>
<input type="checkbox"/> Türen mit Knauf Außenseite	<input type="checkbox"/>
<input type="checkbox"/> Klingelanlage mit Kamera	<input type="checkbox"/>
<input type="checkbox"/> Videoüberwachung der Eingänge	<input type="checkbox"/>



<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen bitte hier beschreiben:

## 1.2. Zugangskontrolle

*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.*

*Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).*

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Login mit Benutzername + Passwort	<input type="checkbox"/> Verwalten von Benutzerberechtigungen

<input type="checkbox"/> Login mit biometrischen Daten	<input type="checkbox"/> Erstellen von Benutzerprofilen
<input type="checkbox"/> Anti-Viren-Software Server	<input type="checkbox"/> Zentrale Passwortvergabe
<input type="checkbox"/> Anti-Virus-Software Clients	<input type="checkbox"/> Richtlinie „Sicheres Passwort“
<input type="checkbox"/> Anti-Virus-Software mobile Geräte	<input type="checkbox"/> Richtlinie „Löschen / Vernichten“
<input type="checkbox"/> Firewall	<input type="checkbox"/> Richtlinie „Clean desk“
<input type="checkbox"/> Intrusion Detection Systeme	<input type="checkbox"/> Allg. Richtlinie Datenschutz und / oder Sicherheit
<input type="checkbox"/> Mobile Device Management	<input type="checkbox"/> Mobile Device Policy
<input type="checkbox"/> Einsatz VPN bei Remote-Zugriffen	<input type="checkbox"/> Anleitung „Manuelle Desktopsperre“
<input type="checkbox"/> Verschlüsselung von Datenträgern	<input type="checkbox"/>
<input type="checkbox"/> Verschlüsselung Smartphones	<input type="checkbox"/>
<input type="checkbox"/> Gehäuseverriegelung	<input type="checkbox"/>
<input type="checkbox"/> BIOS Schutz (separates Passwort)	<input type="checkbox"/>
<input type="checkbox"/> Sperre externer Schnittstellen (USB)	<input type="checkbox"/>
<input type="checkbox"/> Automatische Desktopsperre	<input type="checkbox"/>
<input type="checkbox"/> Verschlüsselung von Notebooks / Tablet	<input type="checkbox"/>

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen:

### 1.3. Zugriffskontrolle

*Maßnahmen, die gewährleisten, 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. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.*

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Aktenschredder (mind. Stufe 3, cross cut)	<input type="checkbox"/> Einsatz Berechtigungskonzepte
<input type="checkbox"/> Externer Aktenvernichter (DIN 32757)	<input type="checkbox"/> Minimale Anzahl an Administratoren
<input type="checkbox"/> Physische Löschung von Datenträgern	<input type="checkbox"/> Datenschutztresor
<input type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	<input type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen:

#### 1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Trennung von Produktiv- und Test- umgebung	<input type="checkbox"/> Steuerung über Berechtigungs- konzept
<input type="checkbox"/> Physikalische Trennung (Sys- teme / Datenbanken / Datenträger)	<input type="checkbox"/> Festlegung von Datenbankrech- ten
<input type="checkbox"/> Mandantenfähigkeit relevanter Anwendungen	<input type="checkbox"/> Datensätze sind mit Zweckattri- buten ver- sehen
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen:

### 1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

*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;*

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	<input type="checkbox"/> Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen:

## 2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

### 2.1. Weitergabekontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger 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. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z.B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.*

<b>Technische Maßnahmen</b>	<b>Organisatorische Maßnahmen</b>
<input type="checkbox"/> Email-Verschlüsselung	<input type="checkbox"/> Dokumentation der Datenempfänger sowie der Dauer der geplanten Über- lassung bzw. der Löschfristen
<input type="checkbox"/> Einsatz von VPN	<input type="checkbox"/> Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
<input type="checkbox"/> Protokollierung der Zugriffe und Abrufe	<input type="checkbox"/> Weitergabe in anonymisierter oder pseudonymisierter Form
<input type="checkbox"/> Sichere Transportbehälter	<input type="checkbox"/> Sorgfalt bei Auswahl von Transport- Personal und Fahrzeugen
<input type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https	<input type="checkbox"/> Persönliche Übergabe mit Protokoll
<input type="checkbox"/> Nutzung von Signaturverfahren	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen:

## 2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input type="checkbox"/> Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
<input type="checkbox"/> Manuelle oder automatisierte Kontrolle der Protokolle	<input type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)
<input type="checkbox"/>	<input type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
<input type="checkbox"/>	<input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verar- beitungen übernommen wurden
<input type="checkbox"/>	<input type="checkbox"/> Klare Zuständigkeiten für Löschungen

Weitere Maßnahmen:



### 3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

#### 3.1. Verfügbarkeitskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.*

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Feuer- und Rauchmeldeanlagen	<input type="checkbox"/> Backup & Recovery-Konzept (ausformuliert)
<input type="checkbox"/> Feuerlöscher Serverraum	<input type="checkbox"/> Kontrolle des Sicherungsvorgangs
<input type="checkbox"/> Serverraumüberwachung Temperatur und Feuchtigkeit	<input type="checkbox"/> Regelmäßige Tests zur Datenwiederher- Herstellung und Protokollierung der Ergebnisse
<input type="checkbox"/> Serverraum klimatisiert	<input type="checkbox"/> Aufbewahrung der Sicherungs- medien an einem sicheren Ort außerhalb des Serverraums
<input type="checkbox"/> USV	<input type="checkbox"/> Keine sanitären Anschlüsse im oder oberhalb des Serverraums
<input type="checkbox"/> Schutzsteckdosenleisten Serverraum	<input type="checkbox"/> Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)

<input type="checkbox"/> Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quell- dichtung etc.)	<input type="checkbox"/> Getrennte Partitionen für Betriebssysteme und Daten
<input type="checkbox"/> RAID System / Festplattenspiegelung	<input type="checkbox"/>
<input type="checkbox"/> Videoüberwachung Serverraum	<input type="checkbox"/>
<input type="checkbox"/> Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen:

## 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

### 4.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Software-Lösungen für Datenschutz-Management im Einsatz	<input type="checkbox"/> Interner / externer Datenschutzbeauftragter  Name / Firma / Kontaktdaten
<input type="checkbox"/> Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	<input type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
<input type="checkbox"/> Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	<input type="checkbox"/> Regelmäßige Sensibilisierung der Mitarbeiter  Mindestens jährlich
<input type="checkbox"/> Anderweitiges dokumentiertes Sicherheitskonzept	<input type="checkbox"/> Interner / externer Informationssicherheitsbeauftragter Name / Firma/Kontakt
<input type="checkbox"/> Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	<input type="checkbox"/> Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
<input type="checkbox"/>	<input type="checkbox"/> Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

<input type="checkbox"/>	<input type="checkbox"/> Formalisierter Prozeß zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen:

#### 4.2. Incident-Response-Management

*Unterstützung bei der Reaktion auf Sicherheitsverletzungen*

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung	<input type="checkbox"/> Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten- Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
<input type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung	<input type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
<input type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung	<input type="checkbox"/> Einbindung von <input type="checkbox"/> DSB und <input type="checkbox"/> ISB in Sicherheitsvorfälle und Datenpannen

<input type="checkbox"/> Intrusion Detection System (IDS)	<input type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
<input type="checkbox"/> Intrusion Prevention System (IPS)	<input type="checkbox"/> Formaler Prozeß und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen:

#### 4.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

*Privacy by design / Privacy by default*

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	<input type="checkbox"/>
<input type="checkbox"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	<input type="checkbox"/>

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Weitere Maßnahmen:

#### 4.4. Auftragskontrolle (Outsourcing an Dritte)

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.*

Technische Maßnahmen	Organisatorische Maßnahmen
<input type="checkbox"/>	<input type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
<input type="checkbox"/>	<input type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
<input type="checkbox"/>	<input type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln

<input type="checkbox"/>	<input type="checkbox"/> Schriftliche Weisungen an den Auftrag- nehmer
<input type="checkbox"/>	<input type="checkbox"/> Verpflichtung der Mitarbeiter des Auftrag- nehmers auf Datengeheimnis
<input type="checkbox"/>	<input type="checkbox"/> Verpflichtung zur Bestellung ei- nes Daten- schutzbeauftragten durch den Auftrag- nehmer bei Vorliegen Bestell- pflicht
<input type="checkbox"/>	<input type="checkbox"/> Vereinbarung wirksamer Kon- trollrechte gegenüber dem Auftragneh- mer
<input type="checkbox"/>	<input type="checkbox"/> Regelung zum Einsatz weiterer Sub- unternehmer
<input type="checkbox"/>	<input type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
<input type="checkbox"/>	<input type="checkbox"/> Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragneh- mers und seines Schutzniveaus

Weitere Maßnahmen:

alternativ:



☐ Hiermit versichern wir, keine Subunternehmer im Sinne einer Auftragsverarbeitung für die Dienstleistung für Sie einzusetzen.

## Anlage 2 - Genehmigte Unterauftragsverhältnisse

<b>Firma Unterauftragnehmer</b>	<b>Anschrift/Land</b>	<b>Leistung</b>	<b>Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland*</b>

---

\* An dieser Stelle kommen insbesondere die Standarddatenschutzklauseln der Kommission gem. Art. 46 Abs. 2 lit. c DS-GVO in der Variante „Übermittlung von Auftragsverarbeiter an Auftragsverarbeiter“ (Modul 3) in Betracht.