

# Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO *Data Processing Agreement pursuant to Art. 28 GDPR*

zwischen | *between*

Name Rechtsform | *Name legal form*  
Adresse, Land | *Address, country*

- Verantwortlicher - nachstehend **Auftraggeber** genannt -  
*- Controller – hereinafter referred to as the Client -*

und | *and*

Name Rechtsform | *Name legal form*  
Adresse, Land | *Address, country*

- Auftragsverarbeiter - nachstehend **Auftragnehmer** genannt  
*- Processor – hereinafter referred to as the Contractor -*

## 1 Gegenstand und Dauer des Auftrags

### 1.1 Gegenstand

Der Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:



### 1.2 Dauer

♦  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.

oder

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

oder

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

oder

## 1 Subject and Duration of the Contract

### 1.1 Subject

The subject of the data processing contract is the performance of the following tasks by the Contractor:



### 1.2 Duration

♦  The contract is concluded for an indefinite period and can be terminated by either party with a notice period of ..... to ..... Termination without notice remains unaffected.

or

♦  The duration of this contract (term) is limited until .....

or

♦  The duration of this contract (term) corresponds to the term of the service agreement.

or

FB41749\_Auftragsverarbeitungsvertrag

- ◆  Der Auftrag wird zur einmaligen Ausführung erteilt.

- ◆  The contract is issued for one-time performance.

2 Konkretisierung des Auftragsinhalts

2 Specification of Contract Content

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

2.1 Nature and Purpose of the Intended Data Processing

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Detailed description of the subject matter of the contract regarding the nature and purpose of the Contractor's tasks:

- ◆
- ◆

- ◆
- ◆

2.2 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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind. Das angemessene Schutzniveau in .....

2.2 The provision of the contractually agreed data processing will take place exclusively in a Member State of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country requires prior approval from the Client and may only occur if the specific conditions of Art. 44 et seq. GDPR are met. The adequate level of protection in .....

- ◆  ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);
- ◆  wird hergestellt durch verbindliche interne Datenschutzvorschriften (Artt. 46 Abs. 2 lit. b i.V.m. 47 DS-GVO);
- ◆  wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 litt. c und d DS-GVO);
- ◆  wird hergestellt durch genehmigte Verhaltensregeln (Artt. 46 Abs. 2 lit. e i.V.m. 40 DS-GVO);
- ◆  wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Artt. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).
- ◆  wird hergestellt durch sonstige Maßnahmen: ..... (Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b DS-GVO)

- ◆  is determined by an adequacy decision of the Commission (Art. 45 (3) GDPR);
- ◆  is ensured by binding internal data protection rules (Art. 46 (2) (b) in conjunction with Art. 47 GDPR);
- ◆  is ensured by standard contractual clauses (Art. 46 (2) (c) and (d) GDPR);
- ◆  is ensured by approved codes of conduct (Art. 46 (2) (e) in conjunction with Art. 40 GDPR);
- ◆  is ensured by an approved certification mechanism (Art. 46 (2) (f) in conjunction with Art. 42 GDPR);
- ◆  is ensured by other measures: ..... (Art. 46 (2) (a), (3) (a) and (b) GDPR)

FB41749\_Auftragsverarbeitungsvertrag

2.3 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- ◆  Personenstammdaten (z.B. Name, Unterschrift, Herkunftsland)
- ◆  Position des MA im Unternehmen (z.B. Berufsbezeichnung, Betriebszugehörigkeit, Abteilung)
- ◆  Kommunikationsdaten (z.B. Telefon, E-Mail)
- ◆  Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ◆  Vertragsabrechnungs- und Zahlungsdaten
- ◆  Planungs- und Steuerungsdaten
- ◆  Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)
- ◆  Bild und Tonaufnahmen (darin z.T. ersichtlich Gesundheitsstand, Hautfarbe, Familienstand, politische Meinungen)
- ◆  .....

2.4 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ◆  Kunden
- ◆  Interessenten
- ◆  Abonnenten
- ◆  Beschäftigte
- ◆  Lieferanten und andere Dienstleister
- ◆  Handelsvertreter
- ◆  Ansprechpartner
- ◆  .....

3 Technisch-organisatorische Maßnahmen

3.1 Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich

2.3 Type of Data

The processing of personal data involves the following types/categories of data:

- ◆  Personal identification data (e.g., name, signature, country of origin)
- ◆  Employee position in the company (e.g., job title, employment duration, department)
- ◆  Communication data (e.g., phone, email)
- ◆  Contractual data (contract relationship, product or contract interest)
- ◆  Contract billing and payment data
- ◆  Planning and control data
- ◆  Information from third parties (e.g., credit agencies, or public directories)
- ◆  Audio and visual recordings (possibly revealing health status, skin color, marital status, political opinions)
- ◆  .....

2.4 Categories of Data Subjects

The categories of data subjects affected by the processing include:

- ◆  Customers
- ◆  Prospects
- ◆  Subscribers
- ◆  Employees
- ◆  Suppliers and other service providers
- ◆  Sales representatives
- ◆  Contacts
- ◆  .....

3 Technical and Organizational Measures

3.1 The Contractor must document and submit for review the technical and organizational measures necessary and specified prior to the assignment, particularly regarding the specific execution of the contract. Upon

FB41749\_Auftragsverarbeitungsvertrag

der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

acceptance by the Client, the documented measures become the basis of the contract. If the Client's review/audit reveals a need for adjustments, these must be implemented by mutual agreement.

3.2 Der Auftragnehmer hat die Sicherheit gem. 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 **(Einzelheiten in Anlage 1)**.

3.2 The Contractor must ensure security in accordance with Art. 28 (3) (c), 32 GDPR, particularly in connection with Art. 5 (1), (2) GDPR. The measures to be implemented are related to data security and ensuring an appropriate level of protection concerning confidentiality, integrity, availability, and resilience of systems. The state of the art, implementation costs, the nature, scope, and purposes of processing, as well as the probability and severity of the risk to the rights and freedoms of natural persons in accordance with Art. 32 (1) GDPR must be considered **(details in Annex 1)**.

3.3 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. Wesentliche Änderungen sind zu dokumentieren.

3.3 The technical and organizational measures are subject to technological progress and development. Therefore, the Contractor is allowed to implement alternative adequate measures, provided that the security level of the established measures is not undercut. Significant changes must be documented.

4 Berichtigung, Einschränkung und Löschung von Daten

4 Correction, Restriction, and Deletion of Data

4.1 Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht

FB41749\_Auftragsverarbeitungsvertrag

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.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Daten Portabilität 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 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a)  Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
- b)  Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- c)  Als Datenschutzbeauftragter ist beim Auftragnehmer **(Bitte Kontakt hier eintragen)** bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- d)  Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- e)  Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird **Herr/Frau (Eintragen: Vorname, Name,**

4.1 The Contractor may not correct, delete, or restrict the processing of data processed on behalf of the Client independently, but only based on documented instructions from the Client. If a data subject contacts the Contractor directly in this regard, the Contractor will immediately forward the request to the Client.

4.2 If included in the scope of services, the deletion concept, right to be forgotten, correction, data portability, and information must be ensured by the Contractor in accordance with documented instructions from the Client.

5 Quality Assurance and Other Obligations of the Contractor

In addition to complying with the provisions of this contract, the Contractor must meet statutory obligations under Art. 28 to 33 GDPR; in particular, they must ensure compliance with the following requirements:

- a)  Written appointment of a Data Protection Officer who performs their duties in accordance with Art. 38 and 39 GDPR.
- b)  Their contact details will be provided to the Client for direct contact. Any change in the Data Protection Officer will be communicated to the Client immediately.
- c)  The Data Protection Officer at the Contractor is **(please enter contact here)**. Any change in the Data Protection Officer will be communicated to the Client immediately.
- d)  Their current contact details are made easily accessible on the Contractor's website.
- e)  The Contractor is not required to appoint a Data Protection Officer. The contact person at

FB41749\_Auftragsverarbeitungsvertrag

**Organisationseinheit, Telefon, E-Mail**  
benannt.

- f)  Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: **(Eintragen: Vorname, Name, Organisationseinheit, Telefon, E-Mail)**.
- g) 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 zur Verarbeitung verpflichtet sind.
- h) 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 **[Einzelheiten in Anlage 1]**.
- i) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- j) 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 Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- k) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen

the Contractor will be Mr./Ms. **(Enter: First name, Last name, Organization unit, Phone, Email)**.

- f)  As the Contractor is located outside the Union, they appoint the following representative in the Union in accordance with Art. 27 (1) GDPR: **(Enter: First name, Last name, Organization unit, Phone, Email)**.
- g) Ensure confidentiality in accordance with Art. 28 (3) Sentence 2 (b), 29, 32 (4) GDPR. The Contractor uses only employees who are bound to confidentiality and have been made aware of the relevant data protection provisions. The Contractor and any person under their authority with access to personal data may only process such data according to the Client's instructions, including the powers granted in this contract, unless legally obligated to process the data.
- h) Implementation and compliance with all necessary technical and organizational measures for this contract in accordance with Art. 28 (3) Sentence 2 (c), 32 GDPR **(details in Annex 1)**.
- i) The Client and the Contractor cooperate with the supervisory authority upon request in fulfilling their tasks.
- j) Immediate notification to the Client of control actions and measures by the supervisory authority, as far as they relate to this contract. This also applies if a competent authority is investigating the processing of personal data in connection with the Contractor's data processing.
- k) If the Client is subject to a supervisory authority's control, an administrative or criminal procedure, a liability claim by a data

FB41749\_Auftragsverarbeitungsvertrag

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.

- l) 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.
- m) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

subject or a third party, or any other claim related to the Contractor's data processing, the Contractor must support the Client to the best of their ability.

- l) The Contractor regularly monitors internal processes and technical and organizational measures to ensure that processing within their area of responsibility complies with applicable data protection laws and protects the rights of data subjects.
- m) Documentation of the technical and organizational measures taken to the Client within the scope of their control rights under Section 7 of this contract.

6 Unterauftragsverhältnisse

6.1 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 z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. 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 sowie Kontrollmaßnahmen zu ergreifen.

6.2 Der Auftragnehmer darf Unterauftragnehmer (**weitere Auftragsverarbeiter**) nur nach vorheriger ausdrücklicher schriftlicher

6 Subcontracting

6.1 Subcontracting under this regulation refers to services that are directly related to the provision of the main service. This does not include ancillary services, such as telecommunications services, postal/transport services, and other measures to ensure the confidentiality, availability, integrity, and resilience of data processing systems used by the Contractor. However, the Contractor is required to ensure adequate and lawful contractual agreements and control measures to protect the Client's data, even in outsourced ancillary services.

6.2 The Contractor may only engage subcontractors (**additional processors**)

FB41749\_Auftragsverarbeitungsvertrag

bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

with the prior express written or documented consent of the Client.

- a)  Eine Unterbeauftragung ist unzulässig.
- b)  Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer **(Aufzählung der Unterauftragnehmer in Anlage 2)** zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:
- c)  Die Auslagerung auf Unterauftragnehmer **oder**
- d)  der Wechsel des bestehenden Unterauftragnehmers ist zulässig, **soweit:**
  - ♦ der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit 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 DS-GVO zugrunde gelegt wird.

- a)  Subcontracting is not permitted.
- b)  The Client approves the engagement of subcontractors (list of subcontractors in Annex 2) under the condition of a contractual agreement in accordance with Art. 28 (2-4) GDPR.
- c)  Outsourcing to subcontractors **or**
- d)  Changing the existing subcontractor is permitted, **provided that:**
  - ♦ The Contractor notifies the Client of such outsourcing to subcontractors in writing or in text form in advance and
  - ♦ The Client does not object in writing or in text form to the planned outsourcing before the data transfer to the Contractor, and
  - ♦ A contractual agreement in accordance with Art. 28 (2-4) GDPR is established.

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

6.3 The transfer of personal data from the Client to the subcontractor and the subcontractor's initial activities are only permitted once all requirements for subcontracting are met.

6.4 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.

6.4 If the subcontractor provides the agreed service outside the EU/EEA, the Contractor ensures data protection compliance through appropriate measures. The same applies if service providers as described in Section 1 Sentence 2 are to be used.

6.5 Eine weitere Auslagerung durch den Unterauftragnehmer

- a)  ist nicht gestattet;

6.5 Further outsourcing by the subcontractor

**FB41749\_Auftragsverarbeitungsvertrag**

- b)  bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
- c)  bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform);

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

**7 Kontrollrechte des Auftraggebers**

7.1 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 zu überzeugen.

7.2 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.

7.3 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-

a)  is not permitted;

b)  requires the express consent of the main Contractor (at least in text form);

c)  requires the express consent of the main Contractor (at least in text form);

all contractual provisions in the contractual chain must also be imposed on the further subcontractor.

**7 Control Rights of the Client**

7.1 The Client has the right to conduct reviews or have reviews conducted by specifically named auditors in coordination with the Contractor. The Client has the right to perform spot checks, which should generally be announced in advance, to verify compliance with this agreement by the Contractor in their business operations.

7.2 The Contractor ensures that the Client can verify compliance with the Contractor's obligations under Art. 28 GDPR. The Contractor commits to providing the Client with the necessary information upon request and, in particular, to proving the implementation of the technical and organizational measures.

7.3 Proof of measures that do not only concern the specific contract may be provided by

- ◆  adherence to approved codes of conduct under Art. 40 GDPR;
- ◆  certification under an approved certification procedure under Art. 42 GDPR;
- ◆  current attestations, reports, or report excerpts from independent bodies (e.g., auditors, internal audits, data protection

**FB41749\_Auftragsverarbeitungsvertrag**

<p>Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);</p> <p>♦ <input type="checkbox"/> eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).</p> <p>7.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.</p> <p><b>8 Mitteilung bei Verstößen des Auftragnehmers</b></p> <p>8.1 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.</p> <p>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</p> <p>b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden</p> <p>c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen</p> <p>d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung</p>	<p>officers, IT security departments, data protection auditors, quality auditors);</p> <p>♦ <input type="checkbox"/> suitable certification by IT security or data protection audit (e.g., according to BSI Basic Protection).</p> <p>7.4 The Contractor may claim compensation for enabling controls by the Client.</p> <p><b>8 Notification of Contractor Violations</b></p> <p>8.1 The Contractor supports the Client in complying with the obligations under Articles 32 to 36 GDPR regarding the security of personal data, notification of data breaches, data protection impact assessments, and prior consultations. This includes:</p> <p>a) Ensuring an adequate level of protection through technical and organizational measures that consider the circumstances and purposes of processing as well as the likely probability and severity of a possible legal breach due to security gaps and enabling the immediate detection of relevant breach events</p> <p>b) The obligation to report personal data breaches immediately to the Client</p> <p>c) The obligation to support the Client in fulfilling their information obligations towards the data subject and to provide all relevant information immediately in this context</p> <p>d) Supporting the Client with their data protection impact assessment</p>
---	--

**FB41749\_Auftragsverarbeitungsvertrag**

<p>e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.</p>	<p>e) Supporting the Client in prior consultations with the supervisory authority.</p>
<p>8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.</p>	<p>8.2 For support services not included in the service description or not attributable to the Contractor's fault, the Contractor may claim compensation.</p>
<p>9 Weisungsbefugnis des Auftraggebers</p>	<p>9 Instructions Authority of the Client</p>
<p>9.1 Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).</p>	<p>9.1 Oral instructions must be confirmed by the Client immediately (at least in text form).</p>
<p>9.2 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 so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.</p>	<p>9.2 The Contractor must inform the Client immediately if they believe that an instruction violates data protection regulations. The Contractor is entitled to suspend the implementation of the relevant instruction until it is confirmed or modified by the Client.</p>
<p>10 Löschung und Rückgabe von personenbezogenen Daten</p>	<p>10 Deletion and Return of Personal Data</p>
<p>10.1 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.</p>	<p>10.1 Copies or duplicates of data are not created without the knowledge of the Client, except for backup copies necessary to ensure proper data processing and data required to comply with legal retention obligations.</p>
<p>10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse</p>	<p>10.2 Upon completion of the contractually agreed tasks or earlier upon request by the Client – at the latest upon termination of the service agreement – the Contractor must return all documents, processing results, and data obtained in connection with the</p>



FB41749\_Auftragsverarbeitungsvertrag

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.

contractual relationship to the Client or, with prior consent, securely delete them. The same applies to test and scrap material. The deletion protocol must be provided upon request.

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

10.3 Documentation serving as proof of proper data processing must be retained by the Contractor according to the applicable retention periods beyond the end of the contract. The Contractor may hand it over to the Client for their relief at the end of the contract.

Ort, den XX.XX.XXXX; Location, on the XX.XX.XXX

Text eingeben. *Enter text.*

.....

**Unterschrift Auftraggeber**  
**Client Signature**

Text eingeben. *Enter text.*

.....

**Unterschrift Auftragnehmer**  
**Contractor Signature**

# Anlage 1 | Annex 1

## Technische und organisatorische Maßnahmen

### *Technical and organizational measures*

nach Art. 32 DSGVO | *in accordance with Art. 32 of the GDPR*

der | of

**HÖRMANN Intralogistics Solutions GmbH**  
Gneisenaustraße 15  
80992 München | *Munich*

#### 11 Transparenz | Transparency

- ◆ Dokumentation der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung. ***Documentation of the nature, scope, circumstances, and purposes of the processing.***
- ◆ Dokumentation der Mandanten und zugehörigen Datenbereiche. ***Documentation of clients and associated data areas.***
- ◆ Dokumentation von Auftrags- und Unterauftragsverhältnissen. ***Documentation of contract and subcontract relationships.***
- ◆ Bereitstellung der erforderlichen Dokumentationen auf Antrag der betroffenen Person. ***Providing the necessary documentation upon request of the data subject.***
- ◆ Dokumentation der Löschrufen. ***Documentation of deletion periods.***
- ◆ Veröffentlichung der Informationen zur Verarbeitung von personenbezogenen Daten (z. B. online oder als Aushang) als Datenschutzerklärung. ***Publication of information regarding the processing of personal data (e.g., online or as a notice) as a privacy statement.***

#### 12 Zweckbindung | Purpose limitation

- ◆ Darstellung der Zwecke im Verzeichnis von Verarbeitungstätigkeiten. ***Representation of purposes in the record of processing activities.***
- ◆ Erlass einer schriftlichen Dienstanweisung zur Verarbeitung personenbezogener Daten. ***Issuance of a written service instruction for the processing of personal data.***
- ◆ Verpflichtung der Mitarbeiter auf die Beachtung der Anforderungen der DSGVO. ***Obligation of employees to comply with the requirements of the GDPR.***
- ◆ Entgegennehmen ausschließlich schriftlicher Weisungen (jedenfalls in Textform, z.B. E-Mail) nur von befugten Mitarbeitern des Verantwortlichen bzw. Auftraggebers. ***Receipt of instructions exclusively in writing only (at least in written form, e.g., email) from authorized employees of the controller or client.***

#### 13 Datenminimierung | Data minimization

- ◆ Festlegung verbindlicher Löschrufen. ***Establishment of binding deletion deadlines.***
- ◆ Festlegung automatisierter Löschrufen. ***Establishment of automated deletion cycles.***

## FB41749\_Auftragsverarbeitungsvertrag

## 14 Richtigkeit | Accuracy

- ◆ Zertifikatsbasierte Authentifizierung der Datenquelle Entra-ID (AAD). **Certificate-based authentication of the data source Entra-ID (AAD).**
- ◆ Beantragung einer Berichtigung durch elektronische Antragstellung. **Application for correction through electronic application submission.**
- ◆ Einrichtung eines Verfahrens zur Berichtigung von Daten auf Antrag per E-Mail. **Establishment of a procedure for data correction upon request via email.**

## 15 Vertraulichkeit | Confidentiality

- ◆ **Clean Desk policy.**
- ◆ Zugang nur mit Parkkarte. **Access only with parking card.**
- ◆ Parkplatzschranke. **Parking barrier.**
- ◆ Technikkeller mit Schlüsselausgabeliste. **Technical room with key issuance list.**
- ◆ Archivkeller mit Zugriffsbeschränkung. **Archive cellar with access restriction.**
- ◆ Sichere Behältnisse bei physischem Transport. **Secure containers for physical transport.**
- ◆ Alarmanlage im Gebäude. **Alarm system in the building.**
- ◆ Sicherheitsschlösser. **Security locks.**
- ◆ Personenkontrolle anhand des Besucherformulars. **Personnel control based on the visitor form.**
- ◆ Auf Datenschutz verpflichtetes Reinigungspersonal. **Privacy-committed cleaning staff.**
- ◆ Unterteilung in Sicherheitszonen. **Division into security zones.**
- ◆ Schlüsselregelung. **Key control arrangement.**
- ◆ Schließsystem mit Transponder. **Locking system with transponder.**
- ◆ Zugangskontrollsystem. **Access control system.**
- ◆ Einbruchhemmende Türen. **Burglar-resistant doors.**
- ◆ Festgelegte Reinigungszeiten. **Established cleaning schedules.**
- ◆ Manuelles Schließsystem. **Manual locking system.**
- ◆ Zugangsbeschränkung nach Endgerät. **Access restriction by device.**
- ◆ Benutzerkonto für jeden Mitarbeiter. **User account for each employee.**
- ◆ Arbeiten mit individuellen Benutzerkennungen. **Use of individual user IDs.**
- ◆ Regelmäßige Passwortwechsel. **Regular password changes.**
- ◆ Authentifikation mit Passwort. **Authentication with password.**
- ◆ Automatische Sperrung. **Automatic locking.**
- ◆ Aufteilung der Administratorrechte unter verschiedenen Personen. **Division of administrator rights among different individuals.**
- ◆ Zertifiziertes Löschen von Datenträgern. **Certified erasure of data carriers.**
- ◆ Sperren der Bootkonfiguration (BIOS, UEFI). **Locking of boot configuration (BIOS, UEFI).**
- ◆ Kontensperrung nach mehrmaliger Falscheingabe des Passworts. **Account lockout after multiple incorrect password entries.**
- ◆ Keine Adminrechte außerhalb der internen IT. **No admin rights outside internal IT.**
- ◆ Differenzierung administrativer Aufgaben. **Differentiation of administrative tasks.**
- ◆ Physikalisch getrennte Speicherung und Verarbeitung. **Physically separated storage and processing.**

FB41749\_Auftragsverarbeitungsvertrag

- ◆ Datenträgervernichtung nach DIN 66399. **Data carrier destruction according to DIN 66399.**
- ◆ Trennung von Produktiv- und Testsystem. **Separation of productive and test systems.**
- ◆ Dem Zweck angemessene Passworrichtlinien. **Password policies appropriate to the purpose.**
- ◆ Authentifikation über Verzeichnisdienste. **Authentication via directory services.**
- ◆ Regelungen beim Ausscheiden von Mitarbeitern. **Provisions for employees leaving the company.**
- ◆ Sicheres Löschen einzelner Dateien. **Secure deletion of individual files.**
- ◆ Beaufsichtigung von Wartungstätigkeiten. **Supervision of maintenance activities.**
- ◆ Nach Verarbeitungszweck differenziertes Berechtigungskonzept. **Authorization concept differentiated by processing purpose.**

16 Pseudonymisierung | Pseudonymization

- ◆ Datenschutz durch Technikgestaltung. **Data protection by design.**
- ◆ Vornahme datenschutzfreundlicher Voreinstellungen. **Data protection by default.**
- ◆ Datenträgerverschlüsselung. **Data carrier encryption.**
- ◆ Transportverschlüsselte Datenübertragung. **Transport encrypted data transmission.**
- ◆ Durchgängige Transportverschlüsselung bei der E-Mail-Übertragung. **Consistent transport encryption in email transmission.**
- ◆ Datenkommunikation über VPN-Tunnel. **Data communication via VPN tunnel.**
- ◆ Dateiverschlüsselung. **File encryption.**
- ◆ Verschlüsselung der Internetpräsenz. **Encryption of the internet presence.**
- ◆ Inhaltsverschlüsselte Datenübertragung. **Content-encrypted data transmission.**
- ◆ Verschlüsselung von mobilen Datenträgern. **Encryption of mobile storage devices.**

17 Integrität | Integrity

- ◆ Einsatz von Virenschutzlösungen. **Use of antivirus solutions.**
- ◆ **Intrusion Detection System.**
- ◆ **Packet Filter Firewall.**
- ◆ Automatisierte Updateprozesse für Betriebssysteme, Anwendungen und Dienste. **Automated update processes for operating systems, applications, and services.**
- ◆ Plausibilitätskontrollen bei der Datenverarbeitung. **Plausibility checks in data processing.**
- ◆ Regelung zum Umgang mit mobilen Datenträgern. **Guidelines for handling mobile storage devices.**
- ◆ Anti Spam Filter für geschäftliche E-Mails. **Anti-Spam filter for business emails.**
- ◆ Differenzierte Berechtigungen für Datenobjekte. **Differentiated permissions for data objects.**

FB41749\_Auftragsverarbeitungsvertrag

18 Verfügbarkeit | Availability

- ◆ Sicherungs- und Wiederherstellungs- konzept. **Backup and Recovery Concept.**
- ◆ Aufbewahrung von Datenträgern in gegen Elementarschäden gesicherten Behältnissen. **Storage of data carriers in containers secured against elemental damage.**
- ◆ Festgelegte Zuständigkeiten für die Datensicherung. **Designated responsibilities for data backup.**
- ◆ Notfallplan zur Wiederinbetriebnahme von Servern und Diensten. **Emergency plan for the restoration of servers and services.**
- ◆ Notfallplan bei Kompromittierung. **Emergency plan in case of compromise.**
- ◆ Redundante IT-Systeme. **Redundant IT systems.**
- ◆ Automatisches Benachrichtigungssystem bei Ausfall. **Automated notification system in case of failure.**
- ◆ Automatisiertes Anfertigen von Datensicherungen (Backup). **Automated data backup (Backup).**
- ◆ Aufbewahrung der Datensicherung in einem anderen Brandabschnitt. **Storage of backups in a different fire compartment.**
- ◆ Regelmäßiger Test der Datenwiederherstellung. **Regular testing of data recovery.**
- ◆ Datenträgerspiegelung (RAID). **Data mirroring (RAID).**
- ◆ Notfallplan bei Datenverlust. **Emergency plan for data loss.**
- ◆ Virtualisierte Infrastruktur. **Virtualized infrastructure.**

19 Belastbarkeit | Resilience

- ◆ Unterbrechungsfreie Stromversorgung. **Uninterruptible Power Supply (UPS).**
- ◆ Klimaanlage in Serverräumen. **Air conditioning in server rooms.**
- ◆ Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen. **Climate monitoring (room temperature, humidity) in server rooms.**
- ◆ Feuchtigkeitssensoren im Archiv. **Humidity sensors in the archive.**
- ◆ Überspannungsschutz. **Surge protection.**
- ◆ Feuer- und Rauchmeldeanlagen. **Fire and smoke detection systems.**
- ◆ Feuerlöscher. **Fire extinguishers.**
- ◆ IT-Komponenten verfügen über erforderliche Leistungsfähigkeit. **IT components have the necessary performance capabilities.**
- ◆ Eignung der Räumlichkeiten / des Baus. **Suitability of premises/building.**

FB41749\_Auftragsverarbeitungsvertrag

20 Rechenschaftspflicht | Accountability

- ◆ Führen eines Verzeichnisses von Verarbeitungstätigkeiten. ***Maintaining a record of processing activities.***
- ◆ Dokumentation über vorhandene IT- Infrastruktur. ***Documentation of the existing IT infrastructure.***
- ◆ Dokumentation der getroffenen Sicherheitsmaßnahmen. ***Documentation of the implemented security measures.***
- ◆ Protokollierung der Anmeldevorgänge. ***Logging of login processes.***
- ◆ Protokollierung gescheiterter Zugriffsversuche. ***Logging of failed access attempts.***
- ◆ Automatisierte Auswertung der Protokolldaten. ***Automated analysis of log data.***
- ◆ Protokollierung von Löschvorgängen. ***Logging of deletion processes.***
- ◆ Protokollierung von Administratorenaktivitäten. ***Logging of administrator activities.***
- ◆ Stichprobenartige Überprüfung der Wirksamkeit bestimmter Maßnahmen. ***Random checks on the effectiveness of certain measures.***
- ◆ Bestellung eine(r/s) Datenschutzbeauftragten. ***Appointment of a Data Protection Officer (DPO).***
- ◆ Dokumentation über eingesetzte Programme und Anwendungen. ***Documentation of deployed programs and applications.***
- ◆ Protokollierung der Datenzugriffe in der Cloud. ***Logging of data accesses in the cloud.***
- ◆ Sicherung der Protokolldaten gegen Veränderung und Verlust. ***Securing log data against alteration and loss."***
- ◆ Protokollierung der Datenträgervernichtung. ***Logging of data destruction processes.***
- ◆ Benutzerkennungsbezogene Protokollierung bei Anmeldung. ***User-specific logging during login.***
- ◆ Arbeitssicherheitsunterweisungen Büro und Baustelle. ***Occupational safety training for office and construction site.***
- ◆ Brandschutzschulungen für betriebliche Ersthelfer. ***Fire protection training for company first aiders.***
- ◆ externe Ersthelferkurse. ***External first aid courses.***
- ◆ Protokollierung der sicheren Löschungen von Datenträgern. ***Logging of secure deletions of data carriers.***



FB41749\_Auftragsverarbeitungsvertrag

# Anlage 2 | Annex 2 Unterauftragnehmer | Subcontractor

der | of

**HÖRMANN Intralogistics Solutions GmbH**  
Gneisenaustraße 15  
80992 München | *Munich*

<b>Firma Unterauftragnehmer</b> <i>Company Subcontractor</i>	<b>Anschrift/ Land</b> <i>Address/Country</i>	<b>Leistung</b> <i>Service</i>