## Vertrag zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO

Vertrag über eine Auftragsverarbeitung zwischen:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Verantwortlicher im Sinne der DS-GVO; im Folgenden als Auftraggeber bezeichnet**

und

### \_\_\_\_\_\_\_\_\_\_\_\_

**Auftragsverarbeiter im Sinne der DS-GVO; im folgenden als Auftragsverarbeiter bezeichnet**

## 1. Gegenstand und Dauer des Auftrags

### 1.1 Gegenstand des Auftrags

Der Auftragsverarbeiter übernimmt folgende Verarbeitungen für den Auftraggeber:

*Herstellung von , die personenbezogene Daten im Inhalt enthalten.*

### 1.2 Dauer des Auftrags

Der Auftrag wird unbefristet erteilt und kann von beiden Parteien mit einer Frist von 4 Wochen gekündigt werden. [Bitte Frist des Auftrages oder Kündigungsfrist ergänzen]

## 2. Details der Verarbeitung

### 2.1 Art und Zweck der Verarbeitung

Beschreibung der Art der Verarbeitung personenbezogener Daten:  
*Herstellung, Personalisierung und Versand von Druckprodukten. [Bitte ergänzen bzw. Druckprodukte präzisieren]*

### 2.2 Art der personenbezogenen Daten

Gegenstand der personenbezogenen Daten sind folgende Datenkategorien:

*Bitte ankreuzen:*

* + *Personenstammdaten (z. B. Name und Adresse)*
  + *Kommunikationsdaten (z. B. E-Mail, Telefon)*
  + *Kundenidentifikationsdaten (Kundennummer)*
  + *Personenbezogene Daten im Druckprodukt*
  + *Sonstige:*

### 2.3 Kreis betroffener Personen

Die Kategorien der durch den Auftrag betroffenen Personen sind:

*Bitte ankreuzen:*

* + *Ansprechpartner bei Abonnenten*
  + *Ansprechpartner bei Kunden und Interessenten*
  + *Beschäftigte (z.B. Mitarbeiterzeitungen)*
  + *Im Druckprodukt genannte oder dargestellte Personen*
  + *Sonstige:*

*[ergänzen]*

### 2.4 Ort der Datenverarbeitung

Die gegenständliche Datenverarbeitung wird ausschließlich in der EU bzw. im EWR durchgeführt.

Die Übermittlung der Daten (auch teilweise) in ein Drittland darf nur erfolgen, wenn der Verantwortliche dieser Übermittlung ausdrücklich zustimmt hat und die besonderen Voraussetzungen der Art. 44 ff DS-GVO erfüllt sind.

## 3. Pflichten des Auftragsverarbeiters

### 3.1 Verarbeitung nach dokumentierter Weisung

Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich wie vertraglich vereinbart oder vom Auftraggeber ausdrücklich angewiesen zu verarbeiten. Erhält der Auftragsverarbeiter einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so wird er den Auftraggeber, sofern gesetzlich zulässig, unverzüglich darüber informieren und die Behörde an diesen verweisen.

Der Auftragsverarbeiter verarbeitet die zur Verarbeitung übergebenen Daten für keine anderen Zwecke, insbesondere nicht für eigene Zwecke.

### 3.2 Wahrung der Vertraulichkeit bzw. Verschwiegenheit

Der Auftragsverarbeiter verpflichtet sich zur Verschwiegenheit.

Der Auftragsverarbeiter erklärt, dass sich alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit schriftlich zur Verschwiegenheit verpflichtet haben.

Der Auftragsverarbeiter sichert zu, dass die zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung von den Bestimmungen des Datenschutzes und dieses Vertrags unterrichtet wurden.

### 3.3 Ergreifung geeigneter Maßnahmen für die Sicherheit der Verarbeitung

Der Auftragsverarbeiter erklärt, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DS-GVO ergriffen hat.

Die im Anhang 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich vereinbart, sie definieren das vom Auftragsverarbeiter geschuldete Mindestniveau des Datenschutzes.

### 3.5 Unterstützung des Auftraggebers bei der Beantwortung von Anträgen betroffener Personen

Der Auftragsverarbeiter ergreift die geeigneten technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach der DS-GVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen.

Wird ein solcher Antrag von einem Betroffenen an den Auftragsverarbeiter gerichtet, leitet dieser den Antrag an den Auftraggeber weiter und verweist die betroffene Person an diesen.

### 3.6 Unterstützung des Auftraggebers bei der Einhaltung dessen Pflichten aus Art. 32 bis 36 DS-GVO

Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DS-GVO genannten Pflichten.

Die angeführten Pflichten umfassen:

* (Maßnahmen zur Sicherheit der Datenverarbeitung nach (Art. 28 Abs, 2 lit. f DS-GVO iVm. Art. 32 DS-GVO),
* Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Art. 28 Abs. 2 lit. f DS-GVO iVm Art. 33 DS-GVO)
* Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Art. 28 Abs. 2 lit. f DS-GVO iVm Art. 34 DS-GVO)
* Datenschutz-Folgenabschätzung (Art. 28 Abs. 2 lit. f DS-GVO i.m Art. 35 DS-GVO),
* vorherige Konsultation der Aufsichtsbehörde bei Verarbeitung mit hohen Risiken (Art. 28 Abs. 2 lit. f DS-GVO iVm Art. 36 DS-GVO).

Der Auftragsverarbeiter verpflichtet sich für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DS-GVO zu errichten.

Im Zusammenhang mit der beauftragten Verarbeitung unterstützt der Auftragsverarbeiter den Auftraggeber bei Erstellung und Wartung des Verarbeitungsverzeichnisses und bei der Durchführung der Datenschutzfolgeabschätzung.

### 3.7 Löschung oder Rückgabe nach Beendigung des Auftrags

Der Auftragsverarbeiter ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die personenbezogene Daten enthalten, zu löschen. Des Weiteren ist der Auftragsverarbeiter verpflichtet, jederzeit aus eigenem Anlass Daten, welche zur weiteren Verarbeitung nicht mehr benötigt werden, zu löschen.

### 3.8 Mitteilungspflicht bei Data Breach

Der Auftragsverarbeiter teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Die Meldung hat spätestens 48 Stunden ab Kenntnis des Auftragsverarbeiters zu erfolgen.

## 5. Sub-Auftragsverarbeiter

Der Auftragnehmer kann Sub-Auftragsverarbeiter [*Tätigkeiten*] hinzuziehen.

Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

## 4. Rechte und Pflichten des Auftraggebers

### 4.1 Verarbeitung auf dokumentierter Weisung

Der Verantwortliche erteilt alle Aufträge und Weisungen dokumentiert.

### 4.2 Überprüfungen/Audits

Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften des Vertrags beim Auftragsverarbeiter selbst oder durch Dritte durch Überprüfungen bzw. Audits zu kontrollieren. Diese Kontrolle kann durch die Einholung von Auskünften, die Einsichtnahme in gespeicherte Daten oder sonstige Kontrollen vor Ort erfolgen. Eine Überprüfung vor Ort ist nur nach vorheriger terminlicher Vereinbarung möglich.

Der Auftragsverarbeiter ist verpflichtet, entsprechende Auskünfte zu erteilen und Nachweise zu führen, die für die Kontrollen notwendig sind. Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

Kontrollen beim Auftragsverarbeiter haben ohne vermeidbare Störungen im Geschäftsbetrieb zu erfolgen.

### 4.3 Haftung des Auftraggebers

Der Auftraggeber sichert dem Auftragsverarbeiter zu, die von ihm bereit gestellten personenbezogenen Daten im Einklang mit den jeweils gültigen datenschutzrechtlichen Bestimmungen zu verarbeiten und zur Datenverarbeitung, insbesonders der Weitergabe an die Druckerei [ergänzen]sowie die Reproduktion, berechtigt zu sein.

Der Auftraggeber verpflichtet sich, den Auftragsverarbeiter von jeglichen Ansprüchen Dritter mit oder im Zusammenhang einer vom Auftraggeber verschuldeten Verletzung von datenschutzrechtlichen Vorschriften schad- und klaglos zu halten.

## 5. Anwendbares Recht und Gerichtsstand

Dieser Vertrag und alle seine Anlagen unterliegen österreichischem Recht unter Ausschluss der Verweisungsnormen des österreichischen IPRG und der Bestimmungen des UN-Kaufrechtsabkommens.

Für alle Streitigkeiten aufgrund oder im Zusammenhang mit diesem Vertrag wird die ausschließliche Zuständigkeit des für den Auftragsverarbeiter sachlich zuständigen Gerichts vereinbart (ergänzen).

## 6. Schlussbestimmungen

### 6.1 Vertraulichkeit

Beide Parteien verpflichten sich, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über Geschäftsgeheimnisse oder Datensicherheitsmaßnahmen der anderen Partei auch für die Zeit nach der Beendigung des Vertrages vertraulich zu behandeln und über diese Verschwiegenheit zu bewahren.

### 6.2 Schriftform

Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform, sofern nicht gesetzlich eine strengere Form vorgeschrieben ist. Das Erfordernis der Schriftform kann nur durch schriftliche Vereinbarung aufgehoben werden.

### 6.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam sein, so bleiben die übrigen Bestimmungen wirksam. Die Vertragsparteien verpflichten sich, im Falle der Unwirksamkeit einzelner Bestimmungen, die unwirksamen Bestimmungen durch Bestimmungen, die dem Zweck der unwirksamen Bestimmungen möglichst entsprechen, zu ersetzen.

### 6.4 Anlagen

Die in diesem Vertrag genannten Anlagen sind integrierender Bestandteil dieses Vertrages. Dieser Vertrag und die darin erwähnten Anlagen enthalten alle Vereinbarungen zwischen den Vertragsparteien bezüglich des Gegenstandes dieses Vertrages. Nebenabreden bestehen nicht.

## Anhang 1: Technisch-organisatorische Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit der überlassenen Daten

Der Auftragsverarbeiter verpflichtet sich, die folgenden, auf Art 32 DS-GVO basierenden, technisch-organisatorischen Maßnahmen zu ergreifen, um den Datenschutz und die Datensicherheit der überlassenen Daten zu gewährleisten.

### 1. Vertraulichkeit und Verschlüsselung

#### Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu den Datenverarbeitungsanlagen:

Während der Geschäftszeiten: Zutritt der Mitarbeiter mit elektronischem Zutrittsausweis (Chipkarten), zusätzliche Kontrolle durch Personal am Empfang, der Zutritt für Kunden ist nur im Empfangsbereich gestattet, falls ein Kunde aus produktionstechnischen Gründen andere Räumlichkeiten des Unternehmens betreten muss, wird dieser ausnahmslos von einem Mitarbeiter begleitet.

Außerhalb der Geschäftszeiten: Gebäude ist versperrt und nur einem eingeschränkten Personenkreis mit Chipkarten zugänglich. Es ist weiters gesichert durch Bewegungsmelder und einer Alarmanlage, mit direkter Verbindung zur Polizei. Der Bürotrakt ist nochmals mit einer eigenen Zugangskontrolle für einen eingeschränkten Personenkreis gesichert.

Für jede Person mit Zutrittsausweis ist dokumentiert in welchem Umfang, in welchem Zeitraum und zu welchen Bereichen Zutritt gewährt wird. Die Zeiten des Zutritts und des Verlassens des Gebäudes durch die Mitarbeiter, sowie die Rückgabe des Zutrittsausweises werden dokumentiert.

#### Zugangskontrolle, Zugriffskontrolle

Schutz vor unbefugter Systembenutzung durch Kennwörter und automatische Sperrmechanismen bei jedem Computer. Nach dreimaliger falscher Eingabe eines Passwortes wird der Zugang gesperrt und kann nur von einem Administrator nach Identifizierung des Users wieder frei gegeben werden.

Scheidet ein Mitarbeiter aus dem Unternehmen aus, muss der elektronische Zutrittsausweis beim Geschäftsführer abgeben werden. Der für den Mitarbeiter bei den Computern angelegte Zugang, wird gelöscht.

Unbefugte Zugriffe auf das System werden verhindert (z. B.: Standard-Berechtigungen und -prozesse zur Berechtigungsvergabe, Protokollierung der Zugriffe, laufende Überprüfung der vergebenen Berechtigungen, insbesondere der von Administratoren). Es existiert das Verbot der ungenehmigten Installation von Soft- und Hardware. Schutzprogramme werden regelmäßig aktualisiert.

#### Pseudonymisierung

Für die Datenverarbeitung in unserem Haus ist eine Pseudonymisierung nicht erforderlich. Auf unserer Homepage erfolgt die Übertragung der IP-Adressen nur pseudonymisiert.

### 2. Integrität

Vom Auftraggeber übermittelte personenbezogene Daten werden am einem für die Mitarbeiter genau definierten Ordner am Server gespeichert. Zugriff darauf gibt es nur für einen bestimmten Mitarbeiterkreis im Unternehmen. Die Löschung der Daten wird mit Löschprotokollen dokumentiert.

Das Netzwerk in [Standort] ist durch eine Firewall vor Zugriffen vom Internet gesichert.

Filiale :

Das Netzwerk in [ergänzen]ist durch eine Firewall vor Zugriffen vom Internet gesichert.

Der Zugriff auf den Server in [ergänzen]wird über ein VPN (Router zu Router) realisiert.

Somit ist auch kein unberechtigter direkter Zugriff von unbefugten Benutzern über Internet möglich.

Zugriffe über Home PC`s der Geschäftsführer vom Internet werden über VPN gesichert.

Der **Mailserver** befindet sich bei der Firma [ergänzen].  
Die Mails werden nach technischer Möglichkeit der PC´s über Imap S(ecure) oder POP S(ecure)abgeholt und über SMTP S(ecure) versendet.

Die Firewalls werden bei Bedarf (z.b. Security Problemen etc..) durch die Firmware von [ergänzen] upgedatet.

Wir haben mit allen Sub-Verarbeitern entsprechende Verarbeiter-Vereinbarungen getroffen und diese der Verschwiegenheit verpflichtet.

### 3. Verfügbarkeit und Belastbarkeit

Schutz gegen zufällige oder mutwillige Zerstörung und Verlust:

Der Server ist durch eine USV vor Stromausfällen gesichert.  
Dies ermöglicht es, bei einem längeren Stromausfall den Server kontrolliert herunter zu fahren, kurze Stromausfälle (bis [ergänzen] min) werden damit überbrückt.  
  
Eine Sicherung der Server wird [ergänzen] auf [ergänzen] erstellt.  
die USB Festplatten werden unterschiedlich gewechselt. Am Wochenende wird eine Festplatte gesondert außerhalb der Geschäftsräumlichkeiten aufbewahrt.

[ergänzen]

Zusätzlich gibt es auch eine Sicherung auf eine NAS.

Ein Virenschutz ist [ergänzen]

installiert.

### 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management:

Regelmäßige Mitarbeiter-Schulungen, dokumentiertes Datenschutzkonzept, Verpflichtung der Mitarbeiter zur Wahrung der Betriebs- und Datengeheimnisse, Löschungsregelungen für personenbezogene Daten

Festplatten von Alt-PC´s oder sonstige Maschinen mit Speichermedien werden von [ergänzen] ordnungsgemäß gelöscht.

Die Überprüfung des Servers erfolgt [ergänzen].

Die Rücksicherungen erfolgen durch Beauftragung der Firma [ergänzen]. Im Falle eines Problems mit der Sicherheit bzw. Datenschutzproblem wird sofort die Firma [ergänzen] kontaktiert.

#### Auftragskontrolle

Es findet keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers – ohne entsprechenden Auftragsverarbeitungsvertrag - statt.