



## VEREINBARUNG ÜBER EINE AUFTRAGSVERARBEITUNG NACH ART 28 DSGVO

### 1. Gegenstand der Vereinbarung

Die Österreichische Post AG (Post) stellt für die Versandvorbereitung durch die Kunden (Verantwortlicher) / dessen Erfüllungsgehilfen den Post-Labelcenter (PLC) zur Verfügung. Bei Verwendung dieses Versandsystems durch die Kunden / dessen Erfüllungsgehilfen tritt die Post als datenschutzrechtlicher Auftragsverarbeiter auf.

Verarbeitet werden Kategorien personenbezogener Daten und Kategorien betroffener Personen gemäß Anlage 1.

### 2. Dauer der Vereinbarung

Die Laufzeit der Vereinbarung richtet sich nach der Nutzung des Versandsystems lt. Punkt 1). Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von drei Monaten zum Monatsende schriftlich gekündigt werden. Die Möglichkeit zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

### 3. Pflichten des Auftragsverarbeiters

#### 3.1. Weisungsgebundenheit des Auftragsverarbeiters

Der Auftragsverarbeiter ist verpflichtet personenbezogene Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Weisung des Verantwortlichen zu verarbeiten. Alle Datenverarbeitungstätigkeiten finden ausschließlich in einem Mitgliedsstaat der Europäischen Union statt.

Die Übermittlung oder Offenlegung von personenbezogenen Daten an Dritte, zu der keine gesetzliche Verpflichtung des Auftragsverarbeiters besteht, setzt eine schriftliche Zustimmung des Verantwortlichen voraus. Soweit der Auftragsverarbeiter dazu aufgrund gesetzlicher Bestimmungen verpflichtet ist, hat er den Verantwortlichen im Vorhinein zu informieren.

Eine Verarbeitung der personenbezogenen Daten für eigene Zwecke des Auftragsverarbeiters darf nur nach vorherigem schriftlichem Einverständnis des Verantwortlichen erfolgen.

#### 3.2. Vertraulichkeit der beauftragten Personen des Auftragsverarbeiters

Der Auftragsverarbeiter verpflichtet sich zur Wahrung des Datengeheimnisses und erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen.

Er hat alle mit der Datenverarbeitung betrauten Personen verpflichtet, personenbezogene Daten, die diesen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut oder zugänglich werden, unbeschadet sonstiger gesetzlicher Verschwiegenheitsverpflichtungen, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung/Bekanntgabe der Daten besteht. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragsverarbeiter aufrecht.



### **3.3. Technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit**

Der Auftragsverarbeiter verpflichtet sich alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO zu ergreifen.

Der Auftragsverarbeiter sichert zu, die in Anlage 2 beschriebenen und ausgewählten, dem Risiko angemessenen, technischen und organisatorischen Maßnahmen ergriffen zu haben und auch in Zukunft zu ergreifen, um die personenbezogenen Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust zu schützen, um ihre ordnungsgemäße Verarbeitung und die Nichtzugänglichkeit für unbefugte Dritte sicherzustellen. Der Auftragsverarbeiter verpflichtet sich dazu, die technischen und organisatorischen Maßnahmen in obigem Sinne auf dem Stand der Technik zu halten und nach technischem Fortschritt bzw. geänderter Bedrohungslage zu aktualisieren bzw. anzupassen.

Der Auftragsverarbeiter stellt sicher, dass der Verantwortliche die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) und unter Berücksichtigung des österreichischen Bundesgesetzes zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (DSG idgF) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann, überlässt dem Verantwortlichen alle dafür notwendigen Informationen und unterstützt diesen bei der Erfüllung diesbezüglicher Pflichten nach besten Kräften.

Wird ein entsprechender Antrag, mit dem Betroffenenrechte geltend gemacht werden, an den Auftragsverarbeiter gerichtet und ist aus dem Inhalt des Antrages ersichtlich, dass der Antragsteller den Auftragsverarbeiter irrtümlich für den Verantwortlichen der von ihm für den Verantwortlichen durchgeführten Verarbeitungstätigkeit hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller unter Bekanntgabe des Datums des Einlangens des Antrages mitzuteilen.

Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation) nach besten Kräften.

Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

Über Ersuchen des Verantwortlichen wird diesem im Einzelfall auch die Erklärung über die Wahrung des Datengeheimnisses hinsichtlich jener Personen vorgelegt, die mit der Durchführung des Auftrags betraut sind.

Dem Verantwortlichen wird hinsichtlich der Verarbeitung der von ihm überlassenen personenbezogenen Daten das Recht eingeräumt, selbst durch qualifizierte und zur Geheimhaltung verpflichtete Mitarbeiter oder durch eine zur Berufsverschwiegenheit verpflichtete Person (gerichtlich zertifizierter Sachverständiger etc.) beim Auftragsverarbeiter die Ordnungsgemäßheit der Datenverarbeitung nach vorheriger Ankündigung von mindestens 30 Werktagen (ausgenommen Samstag) auf eigene Kosten zu überprüfen. Dies während der büroüblichen Zeiten und in



Abstimmung mit dem Datenschutzbeauftragten des Auftragsverarbeiters oder einer sonst für den Datenschutz verantwortlichen Person.

### **3.4. Besondere technische und organisatorische Maßnahmen für sensible Daten**

Sofern die Übermittlung personenbezogener Daten umfasst, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen oder Straftaten enthalten (im Folgenden „**sensible Daten**“), verarbeitet der Auftragsverarbeiter die sensiblen Daten nur bei Vorliegen eines Ausnahmetatbestandes des Art 9 DSGVO und wendet spezielle Beschränkungen und/oder zusätzliche Garantien an, die an die spezifische Art der Daten und die damit verbundenen Risiken angepasst sind.

Dies kann die Beschränkung des Personals, das Zugriff auf die personenbezogenen Daten hat, zusätzliche Sicherheitsmaßnahmen (wie Pseudonymisierung) und/oder zusätzliche Beschränkungen in Bezug auf die weitere Offenlegung umfassen.

### **3.5. Übermittlung von Daten an Drittländer oder internationale Organisationen**

Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage vorheriger schriftlicher Zustimmung durch den Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss die Voraussetzungen der Art 44 ff DSGVO erfüllen. Soweit nach Art 46 DSGVO die Standardvertragsklauseln (Standarddatenschutzklauseln) als Rechtsgrundlage verwendet werden, gelten die jeweils zuletzt von der Kommission gemäß dem Prüfverfahren gemäß Artikel 93 Abs 2 DSGVO erlassenen Standardvertragsklauseln.

## **4. Einsatz von Sub-Auftragsverarbeiter**

Sub-Auftragsverarbeiter (Unterauftragsverarbeiter) sind all jene Unternehmen, welche von Auftragsverarbeiter wiederum als dessen Auftragsverarbeiter herangezogen werden. Der Auftragsverarbeiter kann Sub-Auftragsverarbeiter heranziehen. Er hat den Verantwortlichen von der beabsichtigten Heranziehung so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann.

Nicht hierzu gehören Nebendienstleistungen, die der Auftragsverarbeiter z.B. als Post-/Transport-/Telekommunikationsdienstleistungen oder zur Wartung/ Servicierung von Datenträgern und Datenverarbeitungsanlagen in Anspruch nimmt.

Der Auftragsverarbeiter 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 eingetht, die dem Auftragsverarbeiter auf Grund dieser Vereinbarung obliegen. Die Überbindung der Verpflichtungen ist dem Verantwortlichen über Aufforderung nachzuweisen.



Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

Der Verantwortliche erteilt seine Zustimmung zur Heranziehung der in Anlage 3 genannten Sub-Auftragsverarbeiter.

## **5. Mitteilungen an Kontaktpersonen**

Mitteilungen im Rahmen dieses Vertrages, werden zwischen Kontaktpersonen, welche von den Vertragsparteien bestimmt wurden, schriftlich ausgetauscht. Sofern keine gesonderte E-Mail-Adresse bekanntgegeben wird, wird die E-Mail-Adresse des jeweiligen Online-Service Benutzers, bzw. die E-Mail-Adresse des Ansprechpartners laut Angebot oder Vertrag für datenschutzrechtliche Mitteilungen herangezogen. Ein Wechsel der Kontaktpersonen wird unverzüglich mitgeteilt, längstens jedoch innerhalb von zwei Wochen.

Sollte der Verantwortliche Daten vom FTP-Server des Auftragsverarbeiters downloaden, so ist der Verantwortliche in der Verpflichtung, diese Daten sofort nach dem Download vom FTP-Server zu löschen.

## **6. Löschung und Rückgabe von personenbezogenen Daten nach Beendigung des Auftrages**

Der Auftragsverarbeiter ist nach Beendigung des Auftrags verpflichtet, dem Verantwortlichen alle Verarbeitungsergebnisse und Unterlagen, die vertragsgegenständliche personenbezogene Daten enthalten, zu übergeben; davon unberührt bleibt die Speicherung der dem Auftragsverarbeiter überlassenen personenbezogenen Daten und Verarbeitungsergebnisse bis längstens 2 Jahre nach Durchführung des Auftrags.

Anschließend hat der Auftragsverarbeiter sämtliche vertragsgegenständliche personenbezogene Daten zu löschen oder diese nach Aufforderung des Verantwortlichen vor Durchführung der Löschung sicher zu verwahren. Dies gilt insbesondere, soweit der Auftragsverarbeiter zu einer weiteren Aufbewahrung von personenbezogenen Daten nicht aufgrund zwingender gesetzlicher Bestimmungen verpflichtet ist. Über Ersuchen des Verantwortlichen bestätigt der Auftragsverarbeiter die Datenlöschung schriftlich.

Wenn der Auftragsverarbeiter die personenbezogenen Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die personenbezogenen Daten nach Beendigung des Auftrags entweder in diesem Format oder nach Wunsch des Auftragsverarbeiters in dem Format, in dem er die personenbezogenen Daten vom Verantwortlichen erhalten hat oder in einem anderen gängigen Format herauszugeben.

## **7. Haftung**

Die Haftung für die Datenverarbeitung im Zusammenhang mit dieser Vereinbarung richtet sich nach gesetzlichen Vorschriften.

Die Haftung für leichte Fahrlässigkeit ist ausgeschlossen. Die Haftsumme ist mit EUR 50,-- je Auftrag begrenzt.



## 8. Allgemeine Vertragsbestimmungen

Sämtliche Streitigkeiten aus und im Zusammenhang mit diesem Vertrag unterliegen österreichischem Recht, unter Ausschluss des UN-Kaufrechts und kollisionsrechtlicher Bestimmungen. Für sämtliche Streitigkeiten wird das für 1030 Wien sachlich und örtlich zuständige Gericht vereinbart.

Vereinbarungen im Rahmen dieses Verträgen bedürfen für ihre Verbindlichkeit der Schriftform, es wurden keine mündlichen Nebenabreden getroffen und sämtliche zwischen den Vertragspartnern vor Vertragsunterfertigung abgeschlossenen Vereinbarungen werden mit Unterfertigung dieses Vertrages unwirksam. Änderungen und Ergänzungen der Vereinbarung bedürfen zu ihrer Gültigkeit der Schriftform, dies gilt auch für ein Abgehen vom Formerfordernis der Schriftlichkeit. Sämtliche Rechte und Pflichten aus dieser Vereinbarung gehen auf allfällige Rechtsnachfolger beider Vertragsparteien über.

Diese Vereinbarung geht in Bezug auf die personenbezogene Datenverarbeitung und allen datenschutzrechtlichen Belangen den Bestimmungen des Hauptleistungs-/Rahmenvertrages vor. Die Parteien vereinbaren, den Abschluss dieser Vereinbarung und deren Inhalt vertraulich zu behandeln. Dies gilt, insoweit die gegenständliche Vereinbarung keine entgegenstehenden Bestimmungen enthält und keine gesetzlichen Auskunftspflichten bestehen.

Der Verantwortliche verpflichtet sich, (i) dass sich seine gesetzlichen Vertreter, Mitarbeiter und eingesetzte und/oder beauftragte Subunternehmer an sämtliche geltenden gesetzlichen Bestimmungen im Zusammenhang mit Anti-Korruptionsvorschriften halten sowie (ii) geeignete Maßnahmen zu setzen, um die Einhaltung der Anti-Korruptionsvorschriften sicherzustellen. Ein Verstoß gegen Anti-Korruptionsvorschriften berechtigt den Auftragsverarbeiter – unbeschadet sonstiger Rücktritts- und Kündigungsrechte – zur fristlosen außerordentlichen Kündigung der Vereinbarung sowie zur Geltendmachung allfälliger Schadenersatzansprüche.

Sollten einzelne Bestimmungen der Vereinbarung ungültig oder unwirksam sein oder werden, so werden die Vertragsparteien einvernehmlich eine gültige bzw. wirksame Bestimmung festlegen, die den ungültigen bzw. unwirksamen Bestimmungen wirtschaftlich am nächsten kommt. Die Ungültigkeit oder Unwirksamkeit einzelner Bestimmungen hat keine Auswirkung auf die Gültigkeit bzw. Wirksamkeit des gesamten Vertrages.

Dieser Vertrag wird in zwei Originalen errichtet, von denen jeder Vertragspartner eines erhält.

Die Anlagen 1, 2 und 3 gelten als integrierte Bestandteile des Vertrages.

### Anlage 1 – Kategorien personenbezogener Daten und betroffener Personen

a) Folgende Kategorien personenbezogener Daten werden verarbeitet

<input checked="" type="checkbox"/> Personenstammdaten	<input checked="" type="checkbox"/> Vor- und Nachname, <input checked="" type="checkbox"/> akademische Titel <input checked="" type="checkbox"/> Geburtsdatum <input checked="" type="checkbox"/> Geschlecht
--	---



<input checked="" type="checkbox"/> Daten zur Identifikation	<input checked="" type="checkbox"/> Kundennummer
<input checked="" type="checkbox"/> Adressdaten	<input checked="" type="checkbox"/> Land <input checked="" type="checkbox"/> Stadt / PLZ <input checked="" type="checkbox"/> Straße <input checked="" type="checkbox"/> Hausnummer <input checked="" type="checkbox"/> Türnummer
<input checked="" type="checkbox"/> Es werden keine Daten besonderer Kategorie nach Art 9 DSGVO verarbeitet.	
<input checked="" type="checkbox"/> Es werden keine Daten nach Art 10 DSGVO verarbeitet.	

b) Zu folgenden Kategorien betroffener Personen werden personenbezogene Daten verarbeitet

Betroffene des Geschäftskunden (Kunden, Interessenten, Mitarbeiter, Geschäftspartner, ...)

## Anlage 2 – Technisch - organisatorische Maßnahmen

### 1) VERTRAULICHKEIT

**Zutrittskontrolle** - Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen

<input checked="" type="checkbox"/> Alarmanlage	<input checked="" type="checkbox"/> Sicherheitspersonal
<input checked="" type="checkbox"/> Schlüsselregelung	<input checked="" type="checkbox"/> Videoüberwachung der Zugänge
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input checked="" type="checkbox"/> Personenkontrolle beim Empfang
<input checked="" type="checkbox"/> Berechtigungsausweise	<input checked="" type="checkbox"/> Protokollierung Besucher

**Zugangskontrolle** - Schutz vor unbefugter Systembenutzung

<input checked="" type="checkbox"/> Rollenbasierte Zuordnung von Benutzerrechten	<input checked="" type="checkbox"/> Security Incident Management & Security Operation Center
<input checked="" type="checkbox"/> sichere Kennwörter/Passwortrichtlinie	<input checked="" type="checkbox"/> automatische Sperrmechanismen/Bildschirm Sperre

**Zugriffskontrolle** - Schutz vor unbefugtem Lesen, Kopieren, Verändern od. Entfernen innerhalb des Systems

<input checked="" type="checkbox"/> Berechtigungskonzept „need to know-Basis“	<input checked="" type="checkbox"/> sichere Aufbewahrung von Datenträgern
---	---



<input checked="" type="checkbox"/> Protokollierung von Zugriffen	<input checked="" type="checkbox"/> Pseudonymisierung
<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern	<input checked="" type="checkbox"/> Firewall
<input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministratoren	<input checked="" type="checkbox"/> datenschutzkonforme Entsorgung der Datenträger und Protokollierung
<input checked="" type="checkbox"/> Klassifikationsschema für Daten	<input checked="" type="checkbox"/> Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
<input checked="" type="checkbox"/> VPN-Technologie	

## 2) INTEGRITÄT

**Weitergabekontrolle** - Schutz vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen bei Übermittlung

<input checked="" type="checkbox"/> verschlüsselte Datenübertragung	<input checked="" type="checkbox"/> Dokumentation der Datenempfänger
<input checked="" type="checkbox"/> sichere Transportbehältnisse	<input checked="" type="checkbox"/> Anti-Viren-Software
<input checked="" type="checkbox"/> Datenträgerverschlüsselung	<input checked="" type="checkbox"/> Übersicht über regelmäßige Abruf - und Übermittlungsvorgänge
<input checked="" type="checkbox"/> Intrusion-Detection-System	

**Eingabekontrolle** - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

<input checked="" type="checkbox"/> Protokollierung	<input checked="" type="checkbox"/> Eingabevalidierung
<input checked="" type="checkbox"/> Dokumentenmanagement	

## 3) VERFÜGBARKEIT UND BELASTBARKEIT

**Verfügbarkeitskontrolle** - Schutz vor Zerstörung und Verlust von Daten

<input checked="" type="checkbox"/> Backup & Restore-Tests	<input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen
<input checked="" type="checkbox"/> unterbrechungsfreie Stromversorgung	<input checked="" type="checkbox"/> Recovery-Konzept/Wiederaufbauplan
<input checked="" type="checkbox"/> Redundanzkonzepte/Notversorgungsplan	<input checked="" type="checkbox"/> Klimaanlage
<input checked="" type="checkbox"/> Lösungsfristen	<input checked="" type="checkbox"/> Meldewege und Notfallpläne



#### 4) VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

<input checked="" type="checkbox"/> Datenschutz-Management	<input checked="" type="checkbox"/> regelmäßige Mitarbeiterschulungen
<input checked="" type="checkbox"/> Sicherheitsmanagement	<input checked="" type="checkbox"/> Security Checks auf Infrastruktur- und Applikationsebene

#### 5) SONSTIGE

<input checked="" type="checkbox"/> datenschutzfreundliche Voreinstellungen/ Techniken	<input checked="" type="checkbox"/> Weisungsrecht
<input checked="" type="checkbox"/> eindeutige Vertragsgestaltung	<input checked="" type="checkbox"/> formalisiertes Auftragsmanagement
<input checked="" type="checkbox"/> sorgfältige Auswahl von Dienstleistern	<input checked="" type="checkbox"/> Kontroll-/Auditrecht
<input checked="" type="checkbox"/> Prüfung und Dokumentation von Sicherheitsmaßnahmen	<input checked="" type="checkbox"/> physische/logische Trennung von Daten
<input checked="" type="checkbox"/> Verpflichtung auf Datengeheimnis (z. B. Mitarbeiter)	<input checked="" type="checkbox"/> Trennung von Produktiv- und Testsystem

#### Anlage 3 – Sub-Auftragsverarbeiter

Der Auftragsverarbeiter ist befugt, folgende Sub-Auftragsverarbeiter heranzuziehen:

Firmenname (korrekter Firmenwortlaut)	Adresse und Website	Land der Verarbeitung	Rechtsgrundlage(n) bei Drittlandsverarbeitung
ondot solutions GmbH	Brown-Boveri-Straße 8/1, 2351 Wiener Neudorf	Österreich	keine Drittlandsübermittlung