VEREINBARUNG ÜBER EINE AUFTRAGSVERARBEITUNG NACH ART 28 DSGVO

1. Gegenstand dieses Auftragsverarbeitungsvertrages

Gegenstand dieses Auftragsverarbeitungsvertrages ist die Datenverarbeitung im Zuge der Versandvorbereitung insbesondere mittels des Post-Versandmanagers (PVM) oder mittels Post Label Center (PLC)/BRAVO. Bei Verwendung dieser Dienstleistungen/Tools durch die Kunden / dessen Erfüllungsgehilfen tritt die Post als datenschutzrechtlicher Auftragsverarbeiter auf.

Im Rahmen dieses Auftragsverarbeitungsvertrages sind unter „personenbezogenen Daten", solche personenbezogenen Daten zu verstehen, die der Verantwortliche dem Auftragsverarbeiter im Rahmen dieses Auftragsverarbeitungsvertrages überlässt bzw. deren Verarbeitung dem Auftragsverarbeiter in jenem Vertrag aufgetragen wird.

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

2. Dauer des Auftragsverarbeitungsvertrages

Die Laufzeit der Vereinbarung richtet sich nach der Nutzung der Software lt. Punkt 1).

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 personenbezogene 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 vom 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 eingeht, 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 ein Monat 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.

6. 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 3000,- je Auftrag begrenzt.

7. 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 Vertragen 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.

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.

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

☒ Personenstammdaten	☒ Vor- und Nachname, ☒ akademische Titel ☒ Geburtsdatum ☒ Geschlecht
☒ Daten zur Identifikation	☒ Kundennummer
☒ Adressdaten	☒ Land ☒ Stadt / PLZ ☒ Straße ☒ Hausnummer ☒ Türnummer
☒ Es werden keine Daten besonderer Kategorie nach Art 9 DSGVO verarbeitet.	
☒ 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

☒ Alarmanlage	☒ Sicherheitspersonal
☒ Schlüsselregelung	☒ Videoüberwachung der Zugänge
☒ Sicherheitsschlösser	☒ Personenkontrolle beim Empfang
☒ Berechtigungsausweise	☒ Protokollierung Besucher

Zugangskontrolle - Schutz vor unbefugter Systembenutzung

☒ Rollenbasierte Zuordnung von Benutzerrechten	☒ Security Incident Management & Security Operation Center
☒ sichere Kennwörter/Passwortrichtlinie	☒ automatische Sperrmechanismen/Bildschirmsperre

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

☒ Berechtigungskonzept „need to know-Basis“	☒ sichere Aufbewahrung von Datenträgern
☒ Protokollierung von Zugriffen	☒ Pseudonymisierung
☒ Verschlüsselung von Datenträgern	☒ Firewall
☒ Verwaltung der Rechte durch Systemadministratoren	☒ datenschutzkonforme Entsorgung der Datenträger und Protokollierung
☒ Klassifikationsschema für Daten	☒ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
☒ VPN-Technologie	

2) INTEGRITÄT

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

☒ verschlüsselte Datenübertragung	☒ Dokumentation der Datenempfänger
☒ sichere Transportbehältnisse	☒ Anti-Viren-Software
☒ Datenträgerverschlüsselung	☒ Übersicht über regelmäßige Abruf - und Übermittlungsvorgänge
☒ Intrusion-Detection-System	

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

☒ Protokollierung	☒ Eingabevalidierung
☒ Dokumentenmanagement	

3) VERFÜGBARKEIT UND BELASTBARKEIT

Verfügbarkeitskontrolle - Schutz vor Zerstörung und Verlust von Daten

☒ Backup & Restore-Tests	☒ Feuer- und Rauchmeldeanlagen
☒ unterbrechungsfreie Stromversorgung	☒ Recovery-Konzept/Wiederaufbauplan
☒ Redundanzkonzepte/Notversorgungsplan	☒ Klimaanlage
☒ Löschungsfristen	☒ Meldewege und Notfallpläne

4) VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

☒ Datenschutz-Management	☒ regelmäßige Mitarbeiterschulungen
☒ Sicherheitsmanagement	☒ Security Checks auf Infrastruktur- und Applikationsebene

5) SONSTIGE

☒ datenschutzfreundliche Voreinstellungen/ Techniken	☒ Weisungsrecht
☒ eindeutige Vertragsgestaltung	☒ formalisiertes Auftragsmanagement
☒ sorgfältige Auswahl von Dienstleistern	☒ Kontroll-/Auditrecht
☒ Prüfung und Dokumentation von Sicherheitsmaßnahmen	☒ physische/logische Trennung von Daten
☒ Verpflichtung auf Datengeheimnis (z. B.Mitarbeiter)	☒ Trennung von Produktiv- und Testsystem

Anlage 3 – Sub-Auftragsverarbeiter

Der Auftragsverarbeiter ist befugt, folgende Sub-Auftragsverarbeiter heranzuziehen:

Name	Adresse	Art der Tätigkeit
ATOS IT Solutions and Services GmbH	Siemensstraße 92 1210 Wien	Speicherung und Verarbeitung von Daten in sicheren Rechenzentren gem ISAE3402 SOC 2