Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen nach Art. 28 / 29 DSGVO (Auftragsverarbeitung)

zwischen dem Auftraggeber (Verantwortlicher)

und der

letterei.de Postdienste GmbH
Maybachstraße 9
21423 Winsen
Auftragnehmer -

I. Gegenstand der Vereinbarung

1. Der Auftragnehmer erhebt und verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

2. Der Auftrag umfasst Folgendes:

   Gegenstand des Auftrages (Definition der Aufgaben)
   Drucken, Verarbeiten und Posteinliefern von personalisierten Postsendungen

   Dauer des Auftrags
   Der Vertrag wird auf unbestimmte Zeit geschlossen und ist jederzeit kündbar.

   Umfang, Art und Zweck der Datenerhebung und -verarbeitung
   Personalisieren von Briefsendungen

   Art der Daten
   Namen, Anschriften und Zuordnungsmerkmale (u.a. KdNr) von Postsendungs-Empfängern

II. Rechte und Pflichten des Auftraggebers (Verantwortlicher)

1. Für die Beurteilung der Zulässigkeit der Datenerhebung und –verarbeitung, sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

2. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und entsprechend Nr. I.2 dieser Vereinbarung schriftlich festzulegen.

3. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Die schriftliche Bestätigung der mündlichen Weisungen sollte von Auftraggeber und Auftragnehmer so aufbewahrt werden, dass alle maßgeblichen Regelungen jederzeit verfügbar sind.

   Weisungsberechtigte Personen des Auftraggebers sind die beim Auftragnehmer hinterlegten Angebots- und Rechnungsempfänger, sowie diese, die von diesen Personen autorisiert wurden.

   Weisungsempfänger beim Auftragnehmer sind die in Angeboten und Rechnungen genannten Mitarbeiter, die Geschäftsleitung oder die von diesem Personenkreis autorisierten Mitarbeiter.

4. Bei einem Wechsel oder einer längerfristigen Verhinderung des Ansprechpartners ist dem anderen Vertragspartner unverzüglich schriftlich der Nachfolger bzw. der Vertreter mitzuteilen. Falls Weisungen die unter Nr. I. 2 dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Festlegung erfolgt.

5. Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen (s. Nr. IV) zu überzeugen. Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen.

6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

7. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

III. Pflichten des Auftragnehmers (Auftragsverarbeiter)

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Er hat personenbezogene Daten zu löschen und zu sperren, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt.

2. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden - automatisierten - Verwaltung. Eingang und Ausgang werden dokumentiert.

3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

4. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32-36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen.

5. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

6. Die Verarbeitung von personenbezogenen Daten in Privatwohnungen ist nicht zulässig.

7. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder ein von ihm beauftragter Dritter jederzeit berechtigt ist, sich von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann über die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO oder eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO erfolgen.

8. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder dem Auftraggeber auszuhändigen.

9. Der Auftragnehmer beauftragt keine Subunternehmen. Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers zugelassen, es sei denn, es handelt sich nicht um die Verarbeitung von personenbezogenen Daten. Der Auftragnehmer hat im Falle der Weitergabe von personenbezogenen Daten an Subunternehmer vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmern gelten. Er hat die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 28 / 29 DSGVO erfüllt hat. Hiervon nicht berührt ist die Weitergabe von Daten an Postbeförderungsunternehmen oder sogenannten Konsolidierer.

10. Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, 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. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, EU-Standarddatenschutzklauseln, genehmigte Verhaltensregeln). Falls ein Subunternehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich zu den Bestimmungen in Nr. III.8. Hiervon ausgenommen ist die Weitergabe von Postsendungen an Postbeförderungsunternehmen mit dem Ziel, die entsprechenden Postsendungen im Ausland zuzustellen.

IV. Datenschutzbeauftragte des Auftragnehmers

1. Der vom Auftragnehmer freiwillig benannte Datenschutzbeauftragte ist im Impressum namentlich mit Kontaktmöglichkeit genannt, obgleich der Auftragnehmer nach Art. 37 DSGVO nicht zur Benennung eines Datenschutzbeauftragten verpflichtet ist.

V. Sicherheit der Verarbeitung, Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

1. Der Auftragnehmer verfügt im Falle einer Datenpanne über ein wirksames Incident Response Management. Hierzu gehören regelmäßige Schulungen und Sensibilisierungen der Mitarbeiter in Bezug auf Datenschutz und eine definierte Meldekette im „Verdachtsfall", wie auch die Dokumentation von Incidents. Die IT-Abteilung des Auftragnehmers führt eine permanente Überwachung der Systeme durch, sodass Vorfälle unmittelbar erkannt und deren Folgen behoben werden können.

2. Der Auftragnehmer verarbeitet durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung nur für den Verarbeitungszweck erforderlich sind (Art. 25 Abs. 2 DSGVO).

3. Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass die zur Durchführung der Arbeiten beschäftigten Mitarbeiter ausschließlich auf Weisung des Arbeitgebers personenbezogene Daten verarbeiten und er diese schriftlich zur Vertraulichkeit verpflichtet hat (Art. 28 Abs. 3 lit. b). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

4. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

VI. Technische und organisatorische Maßnahmen nach Art. 24 und Art. 32 Abs. 1 DSGVO

1. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

2. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber das vereinbarte Sicherheitsniveau nicht unterschreiten.

3. Soweit die beim Auftragnehmer getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Entsprechendes gilt für Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie bei Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten.

VII. Vertragsdauer

1. Der Vertrag wird auf unbestimmte Zeit geschlossen und ist jederzeit kündbar.

VIII. Vergütung

1. Die Vergütung richtet sich nach den AGB und den aktuell gültigen Preislisten des Auftragnehmers, sowie individuell vereinbarten Konditionen, soweit sie schriftlich vereinbart wurden.

IX. Haftung

1. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung schuldhaft verursachen. Näheres regeln die AGB des Auftragnehmers.

2. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.

X. Sonstiges

1. Des Weiteren gelten die aktuellen AGB des Auftragnehmers.

2. Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

3. Für Nebenabreden ist die Schriftform erforderlich.

XI. Wirksamkeit der Vereinbarung

1. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Beschreibung der technischen und organisatorischen Maßnahmen zu VI

Datensicherungsmaßnahmen

1. **Zutrittskontrolle**
   Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

- Kontrollierte Schlüsselvergabe (elektronische Schlüssel)
- Schlüssel ist jedem einzelnen Mitarbeiter zugeordnet
- Jeder Zutritt wird elektronisch festgehalten
- Zutritt zu Datenverarbeitungs- und Produktionsanlagen nur unter Aufsicht von verpflichtetem Personal
- Videoüberwachung der Ein- und Ausgänge, sowie des Postausgangs und der Warenannahme

2. **Zugangskontrolle**
   Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Kennwortgeschützter Zugang zu allen Systemen
- Keine unbefugte Systembenutzung
- Firewall
- Zugriff auf personenbezogene Daten nur verschlüsselt im internen Netz oder über VPN

3. **Zugriffskontrolle**
   Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Kennwortgeschützter Zugang
- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
- Zugriffsbeschränkung durch strikte Rechtevergabe

4. **Weitergabekontrolle**
   Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Verschlüsselte SSL-Übertragung (2048Bit)
- Verschlüsselte- bzw. passwortgeschützte Dateien
- Kontrollierte und sachgemäße Vernichtung der Datenträger und der Fehldrucke

5. **Eingabekontrolle**
   Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

- Elektronisches Logbuch
- Adressdaten werden nur in Kopie verarbeitet, Originale bleiben erhalten

6. **Auftragskontrolle**
   Maßnahmen, die gewährleisten, dass die Auftragsdatenverarbeitung weisungsgemäß erfolgt und die Kompetenzen zwischen Auftraggeber und Auftragnehmer abgegrenzt werden:

- Erfassung der Auftragsdaten in internem Kundenverwaltungssystem
- Formalisierte Auftragserteilung (Auftragsformular)
- Auf Wunsch des Auftraggebers werden Korrekturabzüge gefertigt
- Bei onlinebrief24.de: Elektronisches Sendungsprotokoll

7. **Verfügbarkeitskontrolle**
   Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Sicherungsverfahren RAID 6
- Zusätzlich komplette Spiegelung der Daten
- Externe Aufbewahrung der Backups (verschlüsselt)
- USV, damit bei Stromausfall nicht gespeicherte Daten erhalten bleiben
- Firewall und permanenter Virenschutz

8. **Trennungskontrolle**
   Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Speicherung der übermittelten Daten in getrennten, logischen Auftragsordnern
- Dazugehörige Aufträge erhalten intern eigene Auftragsnummern zwecks Zuordnung
- Bei onlinebrief24.de erhält jede einzelne Sendung eine einmalige Auftragsnummer und einen entsprechenden Datamatrixcode