Vereinbarung über die Auftragsverarbeitung Online-Service für Print-Mailings gemäß Artikel 28 EU-Datenschutz-Grundverordnung (DSGVO)

zwischen

Auftragserteilendem Unternehmen

– im Folgenden „Verantwortliche/r“ genannt –

und

Deutsche Post Dialog Solutions GmbH
Charles-de-Gaulle Str. 20
53113 Bonn

– im Folgenden „Auftragsverarbeiter“ genannt –

– zusammen im Folgenden „die Parteien“ genannt –

PRÄAMBEL

A. Der Auftragsverarbeiter erbringt Dienstleistungen gemäß Angebot und Leistungsbeschreibung des Online-Service für Print-Mailings der Deutsche Post Dialog Solutions GmbH. Die Leistungen umfassen Druck- und Lettershop-, Adress- und Fullfillment- und Kommissionierungsleistungen sowie Response-Bearbeitung.

B. Die Parteien möchten die Vereinbarung in Bezug auf die Verarbeitung personenbezogener Daten unter Einhaltung der maßgeblichen Datenschutzgesetze und –vorschriften, insbesondere unter Einhaltung von Artikel 28 der EU-Datenschutz-Grundverordnung, abbilden.

C. In Bezug auf die Verarbeitung personenbezogener Daten ersetzen die Bestimmungen dieses Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter sämtliche vorherigen Übereinkommen und Vereinbarungen zwischen den Parteien. Bei Widersprüchen zwischen den Bestimmungen des Dienstleistungsvertrags und diesem Vertrag zwischen den Verantwortlichen und dem Auftragsverarbeiter ist Letzterer maßgebend.

DIES VORAUSGESCHICKT WIRD FOLGENDES VEREINBART:

1 Gegenstand/Umfang der Verarbeitung

Der Gegenstand des Auftrags ist die Verarbeitung personenbezogener Daten im Rahmen des Angebotes Online-Service für Print-Mailings der Deutsche Post Dialog Solutions GmbH.

2 Laufzeit

Die Laufzeit des Einzelauftrags beginnt mit dem Upload von Adressen und ist befristet bis zur vollständigen Auflieferung der produzierten Mailings bei der Deutschen Post AG. Bei kontinuierlichen, d.h., nicht einmaligen Mailingproduktionen ist die Laufzeit durch eine Einzelvereinbarung zu dieser Rahmenvereinbarung festgelegt.

3 Spezifikation der Verarbeitung

3.1 Art und Zweck der beabsichtigten Verarbeitung

Druck- und Lettershop-, Adress-(Adressvalidierung, Zielgruppenanalysen, Negativabgleich) und gegebenenfalls Fulfillment- und Kommissionierungsleistungen sowie Response-Bearbeitung.

Die oben genannten Leistungen erfolgen im Rahmen des Leistungsbereiches des Online-Service der Deutsche Post Dialog Solutions GmbH.
Nähere Regelungen zu den einzelnen Leistungen ergeben sich aus der aktuell geltenden Leistungsbeschreibung bzw. aus dem Angebot.

3.2 Die Durchführung der Datenverarbeitung erfolgt ausschließlich innerhalb der EU/des EWR. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44ff. DSGVO erfüllt sind.

3.3 Arten der Daten

Folgende Arten personenbezogener Daten werden verarbeitet:

- Name
- Kontaktdaten
- Vertragsdaten
- Position/Funktion
- optional beliebig viele Variablen mit ggf. personenbezogenen Daten

3.4 Betroffene Personen

- Kunden/Mitglieder
- Potenzielle Kunden/interessierte Kreise

- Optional Spenderadressen
- Optional Mitarbeiteradressen

3.5 Besonders sensible personenbezogene Daten

Besondere Kategorien personenbezogener Daten gemäß Artikel 9 EU DSGVO (z. B. Gesundheit, Familienstand, Gewerkschaftszugehörigkeit, politische Meinung, Rasse und ethnische Herkunft, religiöse oder weltanschauliche Überzeugung, strafrechtliche Verurteilung, genetische oder biometrische Daten) sowie personenbezogene Daten über strafrechtliche Verurteilungen und Straftagen gemäß Artikel 10 EU DSGVO werden in der Regel **nicht** verarbeitet. Falls vom Auftraggeber gewünscht, ist zunächst eine gesonderte schriftliche Anfrage durch den Auftraggeber (=Verantwortlicher) erforderlich. In diesem Fall hat der Verantwortliche eine Datenschutzfolgenabschätzung (DSFA) über diese Daten zu erstellen bzw. bereitzustellen. Ansprechpartner ist der unter Abschnitt 4 angeführte Datenschutzbeauftragte.

3.6 Art der Dateneinlieferung

Die Dateneinlieferung erfolgt über HTTPS. Bei Dateneinlieferung mit Daten aus einem Vorsystem ist neben HTTPS auch SFTP mit RSA Schlüssel oder Passwort möglich.

4 Der Datenschutz-Beauftragte der Deutsche Post Dialog Solutions GmbH

Rechtsanwalt Markus Giese
Dreizehnmorgenweg 6
53175 Bonn
Deutschland

Telefon +49 228 9482555
Telefax +49 228 9482556

E-Mail Rechtsanwalt.Giese@t-online.de

5 Datenschutz-Hinweise der Deutsche Post Dialog Solutions GmbH

In den unter https://www.deutschepost.de/de/d/dpds/datenschutz.html einsehbaren Datenschutz-Hinweisen gibt die Deutsche Post Dialog Solutions GmbH dem Verantwortlichen einen Überblick über die verarbeiteten personenbezogenen Daten der gegenüber dem Auftragsverarbeiter auftretenden Mitarbeiter bzw. Erfüllungsgehilfen des Veranwortlichen, welche zur Erfüllung des Vertrags bzw. der vorvertraglichen Tätigkeiten notwendig sind.

6 Technische und organisatorische Maßnahmen

6.1 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ist der Auftragsverarbeiter verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, und zwar auf eine Art und Weise, dass die Verarbeitung personenbezogener Daten die Anforderungen des anwendbaren Datenschutzrechts, insbesondere der DSGVO und dieses Vertrages, erfüllt. Der Auftragsverarbeiter erkennt hiermit die Rechte der betroffenen Personen, wie vorstehend angegeben, an und gewährleistet diese. Zu diesem Zweck und nach Maßgabe von Artikel 32 DSGVO hat der Auftragsverarbeiter die spezifischen Maßnahmen zu dokumentieren und dem Verantwortlichen zur Genehmigung vorzulegen. Nach einvernehmlicher Vereinbarung werden die technischen und organisatorischen Maßnahmen integraler Bestandteil des Vertrags.

6.2 Die vorzunehmenden Maßnahmen sind Maßnahmen der Datensicherheit und Maßnahmen, die ein angemessenes Schutzniveau in Bezug auf das Risiko betreffend Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gewährleisten. Stand der Technik, Implementierungskosten, Art, Umfang und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere eines Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Artikel 32 Absatz 1 DSGVO sind zu berücksichtigen. Die von dem Auftragsverarbeiter vorzunehmenden Maßnahmen orientieren hierbei an den Datenkritikalität-Klassifizierungen (low, medium, high, very high) gemäß DHL Group-Konzernklassifizierung. Die Kritierien für die Einstufung der Datenkritikalität von Kundendaten durch den Auftragsverarbeiter können auf Verlangen des Verantwortlichen übersandt werden.

6.3 Die technischen und organisatorischen Maßnahmen ändern sich mit dem technischen Fortschritt und werden beständig weiterentwickelt. In diesem Zusammenhang kann der Auftragsverarbeiter geeignete alternative Maßnahmen ergreifen. Das Sicherheitsniveau der genannten Maßnahmen darf jedoch nicht unter das in diesem Vertrag vereinbarte Niveau sinken. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen sind dem Verantwortlichen in Text- oder Schriftform mitzuteilen.

6.4 Daher und nach Maßgabe dieser Ziffer 4 bestätigt der Auftragsverarbeiter hiermit die Umsetzung der technischen und organisatorischen Maßnahmen, wie in Anhang 1 dieses Vertrages angegeben und ausgeführt.

6.5 Unbeschadet des Vorstehenden hat der Auftragsverarbeiter ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen einzuführen, um die in diesem Vertrag vereinbarte Sicherheit der Verarbeitung zu gewährleisten.

7 Berichtigung, Einschränkung und Löschung von Daten

7.1 Der Auftragsverarbeiter sowie seine Unterauftragsverarbeiter dürfen personenbezogene Daten nur auf Weisung des Verantwortlichen berichtigen, löschen oder sperren. Beantragt eine betroffene Person die Berichtigung oder Löschung direkt beim Auftragsverarbeiter, hat der Auftragsverarbeiter diesen Antrag unverzüglich an den Verantwortlichen weiterzuleiten.

7.2 Der Auftragsverarbeiter hat den Verantwortlichen nach Möglichkeit bei der Erfüllung der Pflicht des Verantwortlichen zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Person zu unterstützen. Zu diesen Rechten zählen das „Recht auf Vergessenwerden“ sowie die Rechte auf Berichtigung, Datenübertragbarkeit und Auskunft.

7.3 Der Auftragsverarbeiter haftet nicht dafür, dass der Antrag einer betroffenen Person nicht, nicht korrekt oder nicht rechtzeitig seitens des Verantwortlichen beantwortet worden ist, sofern dies nicht durch einen Verstoß oder Fehler des Auftragsverarbeiters begründet ist.

8 Pflichten des Auftragsverarbeiters

Neben den in diesem Vertrag enthaltenen Regelungen und Pflichten hat der Auftragsverarbeiter die gesetzlichen Vorschriften nach Artikel 28-33 DSGVO zu beachten. Dies vorausgeschickt, verpflichtet sich der Auftragsverarbeiter insbesondere dazu,

- personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen zu verarbeiten, sofern er nicht durch das anwendbare Recht, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist, in einem solchen Fall teilt der Auftragsverarbeiter, sofern gesetzlich gestattet, dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung der personenbezogenen Daten mit. Der Auftragsverarbeiter hat mündliche Weisungen unverzüglich schriftlich oder per E-Mail zu bestätigen,

- den Verantwortlichen unverzüglich in Kenntnis zu setzen, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht oder –vorschriften verstößt. In diesem Fall ist der Auftragsverarbeiter berechtigt, die Ausübung der jeweiligen Weisungen auszusetzen, bis der Verantwortliche diese bestätigt oder ändert,

- einen Datenschutzbeauftragten zu ernennen,

- ein Verzeichnis aller Verarbeitungstätigkeiten zu führen,

- Zugang zu den personenbezogenen Daten nur zu gewähren, wenn und soweit dieser Zugang für die Erbringung der Dienstleistungen vorgeschrieben und erforderlich ist und sofern die entsprechenden Mitarbeiter und Berater angemessene Vertraulichkeitsvereinbarungen unterzeichnet und sich zur Vertraulichkeit verpflichtet haben.

Der Auftragsverarbeiter und jede dem Auftragsverarbeiter und/oder dem Verantwortlichen unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie rechtlich zur Verarbeitung verpflichtet sind,

- den Verantwortlichen unverzüglich über Prüfungen, Untersuchungen und/oder Verwaltungsmaßnahmen seitens einer Aufsichtsbehörde in Kenntnis zu setzen, soweit sie den Gegenstand dieses Vertrags betreffen und dies rechtlich zulässig ist,
- falls der Verantwortliche Gegenstand einer Untersuchung der Aufsichtsbehörde, eines Verfahrens wegen Ordnungswidrigkeiten oder eines Strafverfahrens, eines Haftungsanspruchs seitens einer betroffenen Person oder eines Dritten bzw. eines sonstigen Anspruchs in Verbindung mit diesem Vertrag und der Datenverarbeitung durch den Auftragsverarbeiter wird, sich nach Kräften zu bemühen, den Verantwortlichen zu unterstützen,
- den Verantwortlichen so bald wie möglich über etwaige Beschwerden, Anträge bzw. Ersuchen oder sonstige Mitteilungen von betroffenen Personen, Datenschutzbehörden oder Dritten in Verbindung mit der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter und/oder den Verantwortlichen in Kenntnis zu setzen. Sofern der Verantwortliche nach geltendem Datenschutzrecht verpflichtet ist, auf einen Antrag einer betroffenen Person in Verbindung mit der Verarbeitung der Daten dieser betroffenen Person zu antworten, hat der Auftragsverarbeiter den Verantwortlichen bei der Übermittlung der verlangten Informationen zu unterstützen. Allerdings hat der Auftragsverarbeiter nicht direkt auf Anträge betroffener Personen zu antworten, sondern diese betroffenen Personen an den Verantwortlichen zu verweisen.

9 Unterbeauftragung

Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (d.h. Unterauftragnehmer) beauftragen. Diese Unterauftragsverarbeiter sind über einen Rahmenvertrag verpflichtet. Falls der Auftragsverarbeiter im Namen des Verantwortlichen einen weiteren Auftragsverarbeiter mit bestimmten Verarbeitungstätigkeiten beauftragt, werden diesem weiteren Auftragsverarbeiter im Wege eines schriftlichen Vertrages dieselben Pflichten wie in diesem Vertrag auferlegt. Der Auftragsverabeiter sowie eventuell dessen weitere Auftragsverarbeiter sind berechtigt, für untergeordnete Tätigkeiten (z.B. IT-Support und/oder -Maintenance) zusätzliche Auftragsverarbeiter zu beauftragen. Allen diesen Auftragnehmer sind im Wege eines schriftlichen Vertrages diesselben Verpflichtungen auferlegt worden. Auf der Grundlage der in dieser Ziffer enthaltenen Bestimmungen erteilt der Verantwortliche u.a. seine Zustimmung zu dem/den folgenden Auftragsverarbeiter(n):

- Für Support und IT-Betrieb des Online-Services für Print-Mailings die Deutsche Post IT Services GmbH, Fritz-Erler-Straße 5, 53113 Bonn sowie deren Unterauftragnehmer Chili Publish, Korte Keppestraat 9-b11, BE-9320 Erembodegem; NIC Services and Support GmbH, Schillerstraße 21, 73054 Eislingen
- Für Server-Dienstleistungen für die Online-Applikation: DHL IT Services, V Parku 2308/10, Prag, Prag 148 00, Tschechische Republik.
- Für alle Hosting- und IT-Serviceleistungen die Deutsche Post IT Services GmbH, Fritz-Erler-Straße 5, 53113 Bonn; das Hosting erfolgt bei deren Tochtergesellschaft DHL Information Services (Europe) s.r.o., V Parku 2308/10, 14800 Praha 4, Chodov in der Tschechischen Republik; das Rechenzentrum Prag der DHL Information Services (Europe) s.r.o ist nach ISO/IEC 27001:2013 (Zertifikatsnummer 278697-2018-AIS-CZS-UKAS-CC1) von der Zertifizierungsstelle DNV – Business Assurance, London, UK zertifiziert; .
- Für Support und IT-Betrieb zur Auftragsabwicklung über E-POST docuguide und E-POSTBUSINESS API die NIC Services and Support GmbH, Schillerstr. 21, 73054 Esslingen.

- Für Druck- und Postauflieferung wählt die DPDS den geeignetsten Druckdienstleister aus einer Menge von Dienstleistern nach den Erfordernissen des jeweiligen Druckauftrages aus. Folgende Druckdienstleister stehen derzeit zur Auswahl: Atrikom Fulfillment Gesellschaft für Projekt-Dienstleistungen mbH, Haagweg 12, 65462 Ginsheim-Gustavsburg; b+g mailing.de gmbH, Werkstraße 501, 19061 Schwerin; dataform dialog solutions GmbH, Otto-Hahn-Straße 18, 26919 Brake; Deutsche Post E-Post Solutions GmbH, Hansestraße 2,37574 Einbeck; Grunewald GmbH, Lindenbergstraße 44, 34123 KasselKüpper Druck GmbH & Co. KG, Toyotaallee 21, 50858 Köln; Mediengruppe Oberfranken GmbH & Co. KG, Gutenbergstraße 1, 96050 Bamberg; mrd GmbH, Siegener Str. 411, 57258 Freudenberg; MSP Druck und Medien GmbH, Stahlwerkstraße 36, 57555 Mudersbach; O/D Ottweiler Druckerei und Verlag GmbH, Johannes-Gutenberg-Straße 14, 66564 Ottweiler; Power Printing GmbH, Bussardweg 18, 41468 Neuss; primaid GmbH, Engeldorfer Str. 25, 50321 Brühl ; Rehms Druck GmbH, Landwehr 52, 46325 Borken; Sattler Direct Mail GmbH & Co. KG, Daimlerring 2, 31135 Hildesheim; service&verlag GmbH, Schinderstraßl 38, 84030 Ergolding, Wirtz Druck GmbH & Co. KG, Stemmbrückenstraße 1, 45711 Datteln.
  - Die Adressvalidierung, Analysen zur Zielgruppenbestimmung und Abgleiche mit Bestandskunden und Sperrlisten erfolgen durch Deutsche Post Direkt GmbH, Junkersring 57, 53844 Troisdorf sowie deren Unterauftragnehmer: Datacenter Berlin, Nonnendammallee 15, 13599 Berlin; Facility Management: e-shelter facility services GmbH, Nonnendammallee 15, 13599 Berlin; IT-Infrastruktur/Techn. Betrieb: Orange Business Services GmbH, Grolmanstr. 40, 10623 Berlin.

9.1 Der Auftragsverarbeiter hat dem Verantwortlichen rechtzeitig mit angemessener (schriftlich oder per E-Mail erfolgter) mit mindestens 14 Tagen Vorankündigung über einen neuen weiteren Auftragsverarbeiter (einschließlich vollständigen Angaben zu der von dem neuen Auftragsverarbeiter vorgenommen Verarbeitung) oder über Änderungen der bestehenden Liste der weiteren Auftragsverarbeiter in Kenntnis zu setzen.

9.2 Hat der Verantwortliche berechtigte Einwendungen gegen den Einsatz eines weiteren Auftragsverarbeiters durch den Auftragsverarbeiter, hat der Verantwortliche dies dem Auftragsverarbeiter umgehend schriftlich innerhalb von vierzehn Tagennach Zugang der Mitteilung des Auftragsverarbeiters mitzuteilen. Zur Klarstellung: Die Parteien vereinbaren, dass Einwendungen des Verantwortlichen nicht berechtigt sind, wenn der weitere Auftragsverarbeiter der Sicherheitsprüfung für Lieferanten des Auftragsverarbeiters standgehalten hat – es sein denn, der Verantwortliche kann nachweisen, dass der neue Auftragsverarbeiter ein unangemessenes Risiko für den Schutz personenbezogener Daten darstellt (z.B. wenn der weitere Auftragsverarbeiter in der Vergangenheit gegen Sicherheitsbestimmungen vorstoßen hat) oder ein Wettbewerber des Verantwortlichen ist.

9.3 Unbeschadet des Vorstehenden kommen die Parteien bei Einwendungen des Verantwortlichen gegen die Beauftragung eines weiteren Auftragsverarbeiters zusammen, um nach Treu und Glauben über eine geeignete Lösung zu beraten.

Der Auftragsverarbeiter kann insbesondere beschließen, den vorgesehenen Auftragsverarbeiter nicht einzusetzen oder von dem Verantwortlichen verlangte Korrekturmaßnahmen zu ergreifen und den Auftragsverarbeiter zu beauftragen. Ist keine genannte oder sonstige Option vernünftigerweise durchführbar und hat der Verantwortliche nach wie vor berechtigte Einwendungen, können beide Parteien den Vertrag mit einer Frist von 14 Tagen schriftlich kündigen.

Sofern und soweit ausgelagerte Nebendienstleistungen (z.B. Telekommunikationsdienste und Post-/Transportdienste) betroffen sind, ist der Auftragsverarbeiter verpflichtet, angemessene und rechtsverbindliche vertragliche Vereinbarungen abzuschließen sowie angemessene Kontrollmaßnahmen zu ergreifen, um adäquate Maßnahmen für den Schutz und die Sicherheit der Daten des Verantwortlichen zu gewährleisten.

10 Prüfrechte

10.1 Nach angemessener Vorankündigung von mindestens 14 Tagen seitens des Verantwortlichen und um die Einhaltung der technischen und organisatorischen Sicherheitsmaßnahmen sowie der aus diesem Vertrag erwachsenden Pflichten sicherzustellen und zu überprüfen, hat der Auftragsverarbeiter dem Verantwortlichen oder einem von dem Verantwortlichen beauftragten Prüfer

die Durchführung regelmäßiger Prüfungen zu gestatten. Bei besonderen Vorkommnissen hat der Verantwortliche das Recht, ohne eine Vorankündigung von 14 Tagen die Einhaltung bei dem Auftragsverarbeiter Deutsche Post Dialog Solutions GmbH zu überprüfen. Bei folgenden Unterauftragsverarbeitern der Deutschen Post Dialog Solutions GmbH gelten hierzu folgende Abweichungen: Deutsche Post E-Post Solutions GmbH Standort Einbeck: mind. 10 Tage, Deutsche Post IT-Services GmbH und DHL IT-Services Prag: min. 6 Wochen. Besondere Vorkommnisse sind:

a. Der Verantwortliche die begründete Vermutung hat, dass der Auftragsverarbeiter nicht im Einklang mit den technisch-organisatorischen Maßnahmen und / oder den Verpflichtungen aus diesem Vertrag handelt.

b. Sich ein Sicherheitsvorfall ereignet hat.

c. Eine solche Prüfung durch die für den Verantwortlichen zuständige Aufsichtsbehörde gefordert wird.

10.2 Ungeachtet des Vorstehenden kann der Nachweis für die Einhaltung der Vorschriften folgendermaßen erbracht werden:

a. Einhaltung der genehmigten Verhaltensregeln und/oder

b. Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Artikel 42 DSGVO und/oder

c. aktuelle Zertifikate von Prüfern, Berichte oder Auszüge aus Berichten unabhängiger Stellen. Auf Verlangen des Verantwortlichen hat der Auftragsverarbeiter dem Verantwortlichen eine Abschrift des von dem externen Prüfer unterzeichneten Prüfungsberichts zur Verfügung zu stellen, sodass der Verantwortliche angemessen überprüfen kann, ob der Auftragsverarbeiter die technischen und organisatorischen Maßnahmen und Pflichten dieses Vertrages umsetzt bzw. erfüllt.

10.3 Prüfungen werden zu den üblichen Geschäftszeiten, in angemessenem Umfang und ohne Störung des Betriebsablaufs durchgeführt. Für den Fall, dass der Verantwortliche die Prüfung durch einen von ihm beauftragten unabhängigen Prüfer durchführen lässt, hat dieser zuvor eine Verschwiegenheitserklärung zu unterzeichnen. Zudem darf der unabhängige Prüfer nicht in einem unmittelbaren Wettbewerbsverhältnis zum Auftragsverarbeiter stehen.

10.4 Sofern die Prüfung seitens des Auftragsverarbeiters oder eines anderen Auftragsverarbeiters Aufwendungen bedeutet, die über einen Geschäftstag hinausgehen, ist der Auftraggeber damit einverstanden, jeden darüber hinaus gehenden Tag zu erstatten. Dies gilt nicht, wenn die Prüfung aufgrund eines begründeten Verdachts eines Gesetzes- oder Vertragsverstoßes seitens des Auftragsverarbeiters erforderlich wird.

11 Standort des Rechenzentrums

Der Auftragsverarbeiter ist nicht berechtigt, die Instanz des Verantwortlichen ohne dessen vorherige (schriftliche oder per E-Mail erteilte) Zustimmung in ein Rechenzentrum außerhalb der Europäischen Union zu migrieren. Hat der Auftragsverarbeiter die Absicht, die Instanz des Verantwortlichen in ein Rechenzentrum innerhalb der Europäischen Union zu migrieren, benachrichtigt der Auftragsverarbeiter den Verantwortlichen schriftlich oder per E-Mail.

12 Unterstützungspflichten

12.1 Der Auftragsverarbeiter hat den Verantwortlichen bei der Erfüllung der Pflichten betreffend die Sicherheit personenbezogener Daten, die Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten, die Datenschutz-Folgenabschätzungen und vorherige Konsultationen nach Maßgabe von Artikel 33 bis 36 DSGVO zu unterstützen. Dies umfasst insbesondere

a. die Pflicht, eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen zu melden,

b. die Pflicht, den Verantwortlichen im Hinblick auf die Pflicht des Verantwortlichen zur Bereitstellung von Informationen zur betroffenen Person zu unterstützen und dem Verantwortlichen unverzüglich sämtliche relevanten Informationen zur Verfügung zu stellen,

c. die Unterstützung des Verantwortlichen bei einer Datenschutz-Folgenabschätzung,

d. die Unterstützung des Verantwortlichen in Bezug auf das Verzeichnis der Verarbeitungstätigkeiten,

e. die Unterstützung des Verantwortlichen in Bezug auf die Konsultation der Aufsichtsbehörde.

12.2 Der Auftragsverarbeiter kann für die unter Absatz 1 lit. (c) und (d) genannten Unterstützungsleistungen Ersatz verlangen, sofern die Unterstützung nicht aufgrund eines Gesetzes- oder Vertragsverstoßes seitens des Auftragsverarbeiters erforderlich wird.

13 Löschung und Rückgabe personenbezogener Daten

Nach Abschluss der Auftragsarbeiten (in der Regel 90 Arbeitstage nach PAL), hat der Auftragsverarbeiter dem Verantwortlichen sämtliche Dokumente, Verarbeitungs- und Nutzungsergebnisse sowie Datensätze im Zusammenhang mit dem Vertrag, die in seinen Besitz gelangt sind, nach Maßgabe der datenschutzrechtlichen Vorschriften zu löschen oder zu zerstören. Gleiches gilt für Testdaten, Datenmüll sowie überflüssiges und verworfenes Datenmaterial. Das Protokoll zur Zerstörung oder Löschung ist auf Verlangen vorzuzeigen.

Ausgenommen sind Daten und Unterlagen, die aufgrund einer gesetzlichen Verpflichtung gespeichert werden müssen. Diese werden nach Ablauf der Speicherfristen gelöscht.

Unterlagen, die als Nachweis für die ordnungsgemäße Datenverarbeitung dienen, sind von dem Auftragsverarbeiter gemäß den entsprechenden Speicherbestimmungen aufzubewahren. Der Auftragsverarbeiter kann sie dem Verantwortlichen nach Beendigung der Dienstleistung aushändigen, um von seinen diesbezüglichen Pflichten befreit zu werden.

14 Haftung

14.1 Bei Verstößen gegen datenschutzrechtliche Bestimmungen gelten die Regelungen des Artikels 82 DSGVO.

14.2 Für sonstige Haftungs- und (Schadensersatz-)Forderungen gelten die Bestimmungen des jeweiligen Leistungsvertrages, und ergänzend die gesetzlichen Bestimmungen.

15 Schlussbestimmungen

15.1 Eine Änderung oder Ergänzung dieses Vertrags bedarf der Schriftform und der Unterzeichnung der ordnungsgemäß bevollmächtigten Vertreter beider Parteien. Vorgenommen wird eine Änderung oder Ergänzung immer im jeweiligen Einzelauftrag zu dieser Rahmenvereinbarung.

15.2 Werden Daten des Verantwortlichen Gegenstand einer Durchsuchung und Beschlagnahme, eines Pfändungsbeschlusses, einer Einziehung im Rahmen eines Konkurs- oder Insolvenzverfahrens bzw. ähnlicher Ereignisse oder Maßnahmen Dritter, während sie im Verantwortungsbereich des Auftragsverarbeiters sind, so hat der Auftragsverarbeiter den Verantwortlichen hierüber unverzüglich in Kenntnis zu setzen. Der Auftragsverarbeiter hat sämtlichen Beteiligten dieser Maßnahme unverzüglich mitzuteilen, dass sich hiervon betroffene Daten ausschließlich im Eigentum des Verantwortlichen befinden und in dessen Verantwortungsbereich liegen, dass der Verantwortliche das alleinige Verfügungsrecht über diese Daten hat und dass der Verantwortliche für die Anwendung des Datenschutzrechts zuständig ist.

15.3 Sollte eine Bestimmung dieses Vertrags gleich aus welchem Grund für ungültig, rechtswidrig oder undurchsetzbar befunden werden, wird die betreffende Bestimmung ausgenommen und bleiben die übrigen Bestimmungen dieses Vertrags so in vollem Umfang in Kraft und rechtswirksam, als wäre dieser Vertrag ohne die ungültige Bestimmung geschlossen worden.

15.4 Dieser Vertrag unterliegt dem Recht der Europäischen Union.

Bonn, den 01. Januar 2025

Deutsche Post Dialog Solutions GmbH
(Auftragsverarbeiter)

Anmerkung:

Bei Nutzung der Online-Applikation stimmt der/die Verantwortliche dieser Vereinbarung durch Anhaken der Checkbox vor Upload von Adressdaten auf der Webseite des Online-Service rechtsverbindlich zu.

Bei Nutzung des Online-Service stimmt der/die Verantwortliche mit seiner/ihrer Unterschrift einer Einzelvereinbarung zu dieser Rahmenvereinbarung rechtsverbindlich zu.

Anhang 1 – Technische und organisatorische Maßnahmen

1. Technische und organisatorische Maßnahmen der Deutschen Post Dialog Solutions GmbH (DPDS)

Die nachfolgend beschriebenen technischen und organisatorischen Maßnahmen (TOMs) gemäß Artikel 28 Abs. 2 lit. c), 32 DSGVO gelten für alle Verarbeitungen personenbezogener Daten durch die Deutsche Post Dialog Solutions GmbH, im Folgenden DPDS genannt, als Auftragsverarbeiter gem. Art. 28 DSGVO. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft die DPDS nachfolgende dargestellte TOMs, um ein dem Risiko der Verarbeitung ein angemessenes Schutzniveau zu gewährleisten. Dabei wird bei Auftragsverarbeitungen gemäß Artikel 28 DSGVO insbesondere Wert darauf gelegt, ein dem vom Verantwortlichen benanntes Risiko (Angabe der Datenkritikalität) ein entsprechendes Schutzniveau durch adäquate technische und organisatorische Maßnahmen entgegenzusetzen. Es werden dabei u.a. anhand der vom Verantwortlichen genannten Klassifizierungen (low, medium, high, very high gemäß DHL Group-Konzernklassifizierung) geeignete Unterauftragnehmer mit einem angemessenem Schutzniveau bzw. technische und organisatorischen Maßnahmen ausgewählt und eingesetzt.

Beachten Sie bitte folgende **wichtige Hinweise**:

- Werden vom Verantwortlichen keine Angaben zur Datenkritikalität gemacht, gehen wir von der Klassifizierung „low“ aus.
- Datenkategorien nach Artikel 9 und 10 DSGVO müssen der DPDS vor Verarbeitung angezeigt werden, damit hiernach eine Einstufung der Datenkritikalität im konkreten Einzelfall erfolgen kann.
- Die nachfolgend dargestellten Maßnahmen nach Datenkritikalität umfassen nicht die Klassifizierung „very high“. Hierfür sind gesonderte Vereinbarungen mit der DPDS zu treffen.

2. Vertraulichkeit

Artikel 32 Absatz 1 Buchstabe b DSGVO.

2.1. Physische Zutrittskontrolle

Kein unbefugter Zugang zu Datenverarbeitungseinrichtungen, z.B. Magnet- oder Chipkarten, Schlüssel, elektronische Türöffner, Mitarbeiter der Gebäudesicherheitsdienste und/oder für Eingangskontrollen, Alarmsysteme, Videoüberwachungssysteme.

2.1.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	**Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation**
Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde)	low
Verbindlicher Prozess für die Erteilung und Übertragung von Zugangsberechtigungen	low
Zutrittsregelungen für betriebsfremde Personen	low
Schlüsselregelung	low
Anwesenheitsaufzeichnung	medium
Berechtigungsausweise	medium
Besucherausweise	medium
Codekarten sowie Ausweisleser und Wachdienst bei der DPDS und ausgewählten Unterauftragnehmern	medium
Schaffung von Sicherheitsbereichen und Beschränkung der Zutrittswege (Zutrittskontrolle, Verschließen der Räume).	medium
Für die DPDS: Hosting im Rechenzentrum (DIN ISO 27001 zertifiziert).	low
Gebäudesicherung	low
Gesicherter Eingang für An- und Ablieferung	low

Sicherung durch Alarmanlage	medium
Türsicherungen an Notausgängen und anderen Ein- und Ausgängen (elektrischer Türschließer, Ausweisleser, Videoüberwachung, Empfang).	medium bis high
Entsprechende Ausgestaltung der Maßnahmen zur Objektsicherung (z.B. Spezialverglasung, Einbruchmeldesystem, Absicherung von Schächten, Geländeüberwachung).	medium bis high

2.2. Elektronische Zugangskontrolle

Keine unbefugte Nutzung der Systeme zur Datenverarbeitung und -speicherung, z.B. (sichere) Passwörter, automatische Sperr- / Schließmechanismen, Verschlüsselung von Datenträgern / Speichermedien.

2.2.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	**Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation**
Auf allen relevanten IT-Systemen ist ein Zugangskontrollsystem etabliert, das eine Authentisierung durch Abfrage einer Benutzer-ID und eines Passworts verlangt.	low
Verbindliche Passwortrichtlinie mit Anforderungen zu komplexen Passwörtern.	low
Passwortregeln bei Konfiguration werden, wenn technisch nicht anders abbildbar, über Dienstanweisung umgesetzt.	low
Einsatz von Verschlüsselungsroutinen für Dateien bei der Übertragung und beim Transport.	low
Besondere Kontrolle des Einsatzes von Utilities durch Installationsberechtigung auf Arbeitsplätzen nur für Administratoren. Regelmäßiges Einspielen von Sicherheitspatches auf den Systemen.	medium
Abschließbarkeit der Räumlichkeiten für Server-Anlagen und -Geräte.	medium
Ausgabe von Datenträgern nur an autorisierte Personen (mit Begleitpapieren, Auftragsquittungen).	low

Kontrollierte Lagerung der Backup-Datenträger in einem Sicherheitsbereich (z.B. Tresor).	low
Anweisung zur Bildschirmsperre beim Verlassen des Arbeitsplatzes – automatische Bildschirmsperre bei Inaktivität.	low
Abschottung interner Netzwerke gegen ungewollte Zugriffe von draußen (Firewall).	low
Absicherung der Übertragungsleitungen durch verschlüsselte Übertragung von Kundendaten.	medium
Zugriff auf das interne Netzwerk von außen nur über eine verschlüsselte VPN-Verbindung (Virtual Private Network).	medium
Regelmäßige Prüfung der Benutzerkonten auf Gültigkeit und Deaktivierung nach einem bestimmten Zeitraum.	medium

2.3. Interne Zugriffskontrolle (Nutzerrechte für den Zugriff auf und die Änderung von Daten)

Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten im System, z.B. Berechtigungskonzept, Zugriffsrechte auf Need-to-know-Basis, Zugangs- und Zugriffsprotokollierung.

2.3.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	**Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation**
Auf allen betrieblich relevanten IT-Systemen ist ein Zugriffskontrollsystem etabliert, das für den folgerichtigen Schutz von Ressourcen sorgt, indem es die berechtigten Systembenutzer authentisiert und autorisiert, den Zugriff auf die Einrichtungen des Systems kontrolliert, die Integrität von Ressourcen schützt sowie die Benutzung von Ressourcen beschränkt.	low
Regelung zur Erteilung, Verwaltung und Überwachung von Zugriffsberechtigungen.	low
Löschung oder Sperrung von Benutzerrechten nach Vertrags- bzw. Beschäftigungsende.	low

Mandantentrennung auf Druckdienstleisterebene	low
Begrenzte Anzahl von Administratorenaccounts	low

2.3.2. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	**Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation**
Trennung von Produktion und Testsystem (z.T. auch Staging bzw. Referenzsysteme).	low

2.4. Pseudonymisierung

Artikel 32 Absatz 1 Buchstabe a DSGVO, Artikel 25 Absatz 1 DSGVO

Eine Methode / Art, personenbezogene Daten so zu verarbeiten, dass die Daten nur mithilfe zusätzlicher Informationen einer bestimmten betroffenen Person zugeordnet werden können; diese zusätzlichen Informationen sind dabei getrennt zu speichern und mit angemessenen technischen und organisatorischen Maßnahmen zu schützen.

2.4.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	**Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation**
Sofern Livedaten im Testsystem verwendet werden müssen, werden diese anonymisiert oder pseudonymisiert.	low
Sofern personenbezogene Daten nur noch für statistische Zwecke benötigt werden, werden diese anonymisiert.	low

3. Integrität

Artikel 32 Absatz 1 Buchstabe b DSGVO

3.1. Kontrolle der Datenübermittlung

Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten bei deren elektronischer/m Übermittlung oder Transport, z.B. Verschlüsselung, Virtuelle Private Netze (VPN), elektronische Signaturen.

3.1.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation
Vernichtung, Löschung oder Rückgabe von Dateien oder Datenträgern spätestens 90 Arbeitstage nach Beendigung der Verarbeitung, in der Regel nach der Postauflieferung bei druckbezogenen Verarbeitungen.	low
Entsorgung von Fehldrucken bzw. Makulaturen in besonders gesicherten Entsorgungsbehältern und Vernichtung in gesicherter Umgebung.	low
Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden bei durch die DPDS ausgelösten Dateiübertragungen gezielt feststellen zu können.	low
Gesicherte Datenübertragung (VPN, SSL-Tunnel) zwischen der DPDS und deren Rechenzentren sowie auch den Unterauftragnehmern.	low
Auf Anforderung end2end-Verschlüsselung für strengvertrauliche Daten.	medium - high
Clear Desk/Clear Screen Policy bei der DPDS	low

3.2. Kontrolle der Dateneingabe

Überprüfung, ob und von wem personenbezogene Daten in ein Datenverarbeitungssystem eingegeben bzw. in diesem geändert oder gelöscht werden, z.B. Protokolle, Dokumentenmanagement.

3.2.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation
Organisatorisch festgelegte Zuständigkeit für die Dateneingabe.	low
Die Prozesse der DPDS zur Datenänderung sind dokumentiert, weiterhin existiert ein fachliches Logging, aus denen u.a. Änderungszeitpunkte von Datensätzen hervorgehen.	medium
Sämtliche technisch-administrativen Tätigkeiten der DPDS werden geloggt und vor Veränderung geschützt.	medium

4. Verfügbarkeit und Belastbarkeit

Artikel 32 Absatz 1 Buchstabe b DSGVO

4.1. Verfügbarkeitskontrolle

Prävention gegen versehentliche(n) oder absichtliche(n) Zerstörung oder Verlust, z.B. Back-up-Strategie (online / offline; vor Ort / außerhalb des Standortes), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldeverfahren und Notfallplanung.

4.1.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation
Ablage der zentralen Daten der DPDS in einem DHL-Konzern-Rechenzentrum (DHL Information Services (Europe) s.r.o., V Parku 2308/10, 14800 Praha 4, Chodov in der Tschechischen Republik, Zertifikat ISO/IEC 27001:2013 (Zertifikatsnummer 278697-2018-AIS-CZS-UKAS-CC1, Zertifizierungsstelle DNV – Business Assurance, London, UK.)	low
Nutzung von Datenverarbeitung/IT- und Hostingservices durch Unterauftragnehmer (Druck- und Lettershop-Dienstleister etc.) zertifiziert nach DIN ISO 27001.	high
Regelmäßige Durchführung von Datensicherungen.	low
Lagerung der Sicherungskopien an besonders geschützten Orten außerhalb des Rechenzentrums.	low
Brandschutzmaßnahmen	low
Unterbrechungsfreie Stromversorgung (USV)	low
Datenspiegelung relevanter Datenträger	low

4.2. Rasche Wiederherstellung

Artikel 32 Absatz 1 Buchstabe c DSGVO

4.2.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation

Regelmäßige Überprüfung der Sicherungs- und Wiederherstellbarkeit.	low

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Artikel 32 Absatz 1 Buchstabe d DSGVO; Artikel 25 Absatz 1 DSGVO

5.1. Datenschutz- und Reaktionsmanagement

5.1.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	**Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation**
Einsatz eines Information Security Management System (ISMS (= „Management von IT- und Datenschutzvorfällen bei der DPDS“)) in Anlehnung an die DIN ISO 27001, welches wesentliche Teile des Datenschutzmanagements umfasst (z.B. Prozesse bei Datenschutzvorfällen, Prozesse bei Notfällen oder Krisen). Nutzung analoger Vorgaben bzw. Systeme bei den eingesetzten Unterauftragnehmern.	low

5.2. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Artikel 25 Absatz 2 DSGVO

5.2.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	**Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation**
Privacy-by-design: Die Entwicklung neuer Systeme erfolgt unter Einbezug des betrieblichen Datenschutzbeauftragten.	low

Privacy-by-default: Sofern Standardsoftware zum Einsatz kommt, werden Werks-einstellungen - sofern veränderbar - , so eingestellt, dass diese datenschutzfreundlich ausgestaltet sind.	low

5.3. Auftrags- oder Vertragskontrolle bei der DPDS

5.3.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation
Verarbeitung durch Dritte bzw. Unterauftragnehmer nach Maßgabe von Artikel 28 DSGVO, u.a. mit einem Vertrag zur Auftragsverarbeitung (§ 28 (3)).	low
Verarbeitung personenbezogener Daten nur auf Weisung des Verantwortlichen.	low
Klare und eindeutige vertragliche Vereinbarungen mit Dienstleistern.	low
Regelmäßige Lieferantenaudits.	low

5.4. Organisationskontrolle

5.4.1. Umgesetzte Maßnahmen

Maßnahmen nach Datenkritikalität	Mindestabdeckung gemäß Datenkritikalität nach DHL-Klassifikation
Zutrittsberechtigungen nur für autorisierte Personen.	low
Zugangsberechtigungen nur für autorisierte Personen.	low

Zugriffsberechtigungen: Kundendaten werden vor unberechtigtem Zugriff mit einem Berechtigungskonzept nach Nutzergruppen geschützt.	low
Datenübertragungen von Kundendaten werden grundsätzlich verschlüsselt vorgenommen.	low
Verpflichtung der Mitarbeitenden bei der DPDS als auch bei den eingesetzten nationalen Unterauftragnehmern bei Arbeitsaufnahme auf das Datengeheimnis gemäß Art. 5 Abs. 2, 28 Abs. 3 lit. B), 29, 32 Abs. 4 DSGVO sowie § 88 Abs. 1 des Telekommunikationsgesetzes, § 206 Abs. 5 Satz 2 StGB.	low
Bestellung eines betrieblichen Datenschutzbeauftragten gemäß Vorgaben des § 38 BDSG.	low
Einhaltung der Grundsätze zur Funktionstrennung und klare Verantwortungsbereiche.	low
Trennung von Test und Produktion.	low
Regelungen zu Test und Freigabe.	low
Regelungen zu System- und Programmprüfung bei der DPDS sowie zum Löschungskonzept. Anwendungen werden erst nach erfolgter Qualitätssicherung und Freigabe in Betrieb genommen.	low
Wartungs- und Reparaturarbeiten: Wartungsarbeiten finden in geplanten Wartungsfenstern statt.	low
Dokumentation von IT-Verfahren, Software und IT-Konfiguration der DPDS: Software: • Fachliche Beschreibung von Anwendungsfällen • Technische Konzeption / Architekturdokumentation (je nach Anwendung unterschiedlich im Umfang). • Releasedokumentation • Dokumentation von Testfällen / Testläufen. • Prozesse / IT-Verfahren	low

• Dokumentation von Organisationsprozessen (u.a. Release- / Freigabeprozess / Inbetriebnahme, Anforderungsanalyse) mit definierten Rollen / Verantwortlichkeiten. • Issue- / Bugtracking	