Vereinbarung über die Auftragsverarbeitung Print Mailing Automation gemäß Artikel 28 EU-Datenschutz-Grundverordnung (DSGVO)

zwischen

Auftragserteilendem Unternehmen

– im Folgenden „Verantwortliche/r“ genannt –

und

Deutsche Post Dialog Solutions GmbH
Koblenzer Straße 67
53177 Bonn

– im Folgenden „Auftragsverarbeiter“ genannt –

– zusammen im Folgenden „die Parteien“ genannt –

PRÄAMBEL

A. Der Auftragsverarbeiter erbringt Dienstleistungen gemäß Angebot und Leistungsbeschreibung der **Print-Mailing Automation** 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:

BEGRIFFSBESTIMMUNGEN UND AUSLEGUNG

„Vertrag“ bezeichnet diesen Vertrag samt den beigefügten Anhängen.

„Nebendienstleistungen“ bezeichnet die Dienstleistungen, die unabhängig vom Gegenstand dieses Vertrages sind, wie etwa Telekommunikationsdienste, Post-/Transportdienste, Instandhaltungs- und unterstützende Dienstleistungen für Nutzer oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hardware und Software von Datenverarbeitungsanlagen.

„Anhang“ bezeichnet jeden Anhang zu diesem Vertrag, der als Vertragsbestandteil anzusehen ist.

„Weiterer Auftragsverarbeiter“ bezeichnet einen von dem Auftragsverarbeiter im Lauf der Erbringung der Dienstleistungen beauftragten Datenverarbeiter.

„Verantwortlicher“ bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

„Datenschutzgesetze“ bezeichnet die EU-Datenschutzgesetze und, soweit anwendbar, die Datenschutzgesetzte eines anderen Landes.

„EWR“ bezeichnet den Europäischen Wirtschaftsraum und besteht aus sämtlichen Ländern der Europäischen Union, Liechtenstein, Norwegen und Island.

„DSGVO“ bezeichnet die VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

„Personenbezogene Daten“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person **(„betroffene Person“)** beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

„Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

„Auftragsverarbeiter“ bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

„Dienstleistungen“ bezeichnet sämtliche Dienstleistungen, die der Auftragsverarbeiter, wie im Rahmen des Dienstleistungsvertrags vereinbart, erbringt.

„Dienstleistungsvertrag“ bezeichnet den Vertrag, den die Parteien in Bezug auf die Erbringung von Dienstleistungen durch den Auftragsverarbeiter abgeschlossen haben.

1 Gegenstand/Umfang der Verarbeitung

Der Gegenstand des Auftrags ist die Verarbeitung im Rahmen des Angebotes Print-Mailing Automation 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- und gegebenenfalls Fulfillment
und Kommissionierungsleistungen sowie Response-Bearbeitung.

Die oben genannten Leistungen erfolgen im Rahmen des Leistungsbereiches der Print-Mailing Automation 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.

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
- Spenderadressen
- Mitarbeiteradressen

3.5 Besondere personenbezogene Daten

Bestimmte 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) werden in der Regel **nicht** verarbeitet. Falls doch, so erfolgt eine gesonderte Information darüber durch den Auftraggeber (=Verantwortlicher). 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. Der von dem Auftragsverarbeiter vorzunehmenden Maßnahmen orientieren hierbei an dem Schutzstufenkonzept ZAWAS der Landesbeauftragte für den Datenschutz Niedersachsen. Das Schutzstufenkonzept des Auftragsverarbeiters kann 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.

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.

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 der Online-Applikation Print-Mailing Automation die Deutsche Post IT Services GmbH, Wielandstr. 4, 53173 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 IT-Leistungen zur Auftragsabwicklung der DPDS: Plusserver, Niederlassung Düsseldorf, In der Steele 37, 40599 Düsseldorf.
- 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; Deutsche Post E-Post Solutions GmbH, Hansestraße 2,37574 Einbeck; Rehms Druck GmbH, Landwehr 52, 46325 Borken; mrd Oliver Homrich e.K., Siegener Str. 411, 57258 Freudenberg; MSP Druck und Medien GmbH, Stahlwerkstraße 36, 57555 Mudersbach; PowerPrinting, Bussardweg 18, 41468 Neuss
- Die Adressvalidierung erfolgt 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: The unbelievable Machine Company GmbH, Grolmanstr. 40, 10623 Berlin.

9.1 Der Auftragsverarbeiter hat dem Verantwortlichen rechtzeitig mit angemessener (schriftlich oder per E-Mail erfolgter) 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 zwei Arbeitstagen nach 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 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, Plusserver GmbH: min. 3 Wochen, 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 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.

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.

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 und Sanktionen

14.1 Die gesetzliche Bestimmungen, insbesondere Artikel 82 DSGVO, gelten im Fall von Schadensersatz- und Haftungsanforderungen.

14.2 Der Verantwortliche ist verpflichtet, den Auftragsverarbeiter von sämtlichen Forderungen Dritter freizustellen, falls dem Auftragsverarbeiter ein Schaden aus Datenschutzverstößen entstehen sollte, die der Verantwortliche zu vertreten hat.

14.3 Für sonstige Haftungs- und (Schadensersatz-)Forderungen gelten die gesetzlichen Bestimmungen, und zwar insbesondere die des Zivil- und Strafrechts.

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 13.12.2021

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 der Print-Mailing Automation rechtsverbindlich zu.

Bei Nutzung der Print-Mailing Automation mit Daten aus einem Vorsystem stimmt der/die Verantwortliche mit seiner/ihrer Unterschrift einer Einzelvereinbarung zu dieser Rahmenvereinbarung rechtsverbindlich zu.

Anhang 1 – Technische und organisatorische Maßnahmen

1. Technisch Organisatorische Maßnahmen der Deutschen Post Dialog Solutions GmbH (DPDS)

Die nachfolgend beschriebenen Technisch Organisatorischen Maßnahmen (TOMs) gemäß Artikel 32 DSGVO gelten für die Leistungen der Deutschen Post Dialog Solutions GmbH, im Folgenden DPDS genannt. 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 Leistungen angemessenes Schutzniveau zu gewährleisten. Die nachfolgend beschriebenen TOMs gelten auch für die von der DPDS eingesetzten Unterauftragnehmer. Zusätzliche Maßnahmen, die ausschließlich für die DPDS gelten, sind als solche gekennzeichnet.

2. Vertraulichkeit

Artikel 32 Absatz 1 Buchstabe b DSGVO.

2.1. Physische Zutrittskontrolle

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

2.1.1. Umgesetzte Maßnahmen

- Anweisungen für Maßnahmen zur Zutrittskontrolle.
- Sicherheitsschlösser mit Schlüsselverwaltung.
- Codekarten sowie Ausweisleser und Wachdienst für die Gebäude der DPDS.
- Zutrittsregelungen für betriebsfremde Personen (Zutritt nur in Begleitung).
- Schaffung von Sicherheitsbereichen und Beschränkung der Zutrittswege (Zutrittskontrolle, Verschließen der Räume).

- Ablage der zentralen Daten in Rechenzentren, die DIN ISO 27001 zertifiziert sind, bei Verarbeitung durch die DPDS.
- Gebäudesicherung
- Sicherung durch Alarmanlage.

2.2. Elektronische Zugangskontrolle

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

2.2.1. Umgesetzte Maßnahmen

- Auf allen betrieblich relevanten IT-Systemen der DPDS ist ein Zugangskontrollsystem etabliert, das eine Authentisierung durch Abfrage einer Benutzer-ID und eines Passworts verlangt.
- Verbindliche Passwortrichtlinie bei der DPDS mit Anforderungen zu komplexen Passwörtern.
- Passwortregeln bei Konfiguration der DPDS-IT-Systeme werden, wenn technisch nicht anders abbildbar, über Dienstanweisung umgesetzt.
- Einsatz von Verschlüsselungsroutinen für Dateien bei der Übertragung und beim Transport.
- Besondere Kontrolle des Einsatzes von Utilities durch Installationsberechtigung auf Arbeitsplätzen der DPDS nur für Administratoren. Regelmäßiges Einspielen von Sicherheitspatches auf den Systemen.
- Abschließbarkeit der DV-Anlagen und -Geräte (z.B. PC) der DPDS.
- Ausgabe von Datenträgern nur an autorisierte Personen (mit Begleitpapieren, Auftragsquittungen).
- Kontrollierte Lagerung der Datenträger in einem Sicherheitsbereich (z.B. Tresore).
- Anweisung zur Bildschirmsperre beim Verlassen des Arbeitsplatzes – automatische Bildschirmsperre bei Inaktivität.
- Abschottung interner Netzwerke gegen ungewollte Zugriffe von draußen (Firewall).
- Absicherung der Übertragungsleitungen durch verschlüsselte Übertragung von Kundendaten. Auf Anforderung für streng vertrauliche Daten end2end-Verschlüsselung.

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

- Auf allen betrieblich relevanten IT-Systemen der DPDS ist ein Zugriffskontrollsystem etabliert, das für den folgerichtigen Schutz von Ressourcen sorgt, indem es die berechtigten Systembenutzer identifiziert und authentisiert, den Zugriff auf die Einrichtungen des Systems kontrolliert, die Integrität von Ressourcen schützt sowie die Benutzung von Ressourcen beschränkt.
- Regelung zur Erteilung, Verwaltung und Überwachung von Zugriffsberechtigungen.
- Mandanten- / Rollen-Trennung auf Anwendungsebene.

2.4. Trennung nach Zweck

Getrennte Verarbeitung von Daten, die für verschiedene Zwecke erhoben werden, z.B. Unterstützung des Verantwortlichen zu mehreren Zwecken, Sandboxing-Technik.

2.4.1. Umgesetzte Maßnahmen

- Trennung von Produktion und Testsysteme (z.T. auch Staging bzw. Referenzsysteme).

2.5. 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.

2.5.1. Umgesetzte Maßnahmen

- Sofern Livedaten im Testsystem der DPDS verwendet werden müssen, werden diese anonymisiert oder pseudonymisiert.

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

- Vernichtung, Löschung oder Rückgabe von Dateien oder Datenträgern (z.B. Fehldrucke), spätestens 90 Arbeitstage nach Beendigung der Verarbeitung.
- Protokollierung der durch die DPDS ausgelösten Datenübermittlungen sowie der Empfänger bei Dateiübertragungen mittels sftp-logging.
- Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden bei durch die DPDS ausgelösten Dateiübertragungen gezielt feststellen zu können.
- Gesicherte Datenleitungen (VPN, SSL-Tunnel) zwischen der DPDS und deren Rechenzentren sowie auch den Unterauftragnehmern.
- Daten werden – sofern sie auf Datenträgern versandt werden – auf Wunsch des Auftraggebers und nach Absprache mit kryptographischen Verfahren verschlüsselt und ausschließlich über zuverlässige Transportunternehmen mit dokumentierter Übergabe befördert.
- Auf Anforderung end2end-Verschlüsselung für strengvertrauliche Daten.

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

- Organisatorisch festgelegte Zuständigkeit für die Dateneingabe.
- Die Prozesse der DPDS zur Datenänderung sind dokumentiert, weiterhin existiert ein fachliches Logging, aus denen u.a. Änderungszeitpunkte von Datensätzen hervorgehen.
- Sämtliche administrativen Tätigkeiten der DPDS werden geloggt und vor Veränderung geschützt.

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

- Ablage der zentralen Daten der DPDS in Rechenzentren, die DIN ISO 27001 zertifiziert sind.
- Regelmäßige Durchführung von Datensicherungen.
- Lagerung der Sicherungskopien an besonders geschützten Orten außerhalb des Rechenzentrums.
- Prüfsummenverfahren bei der DPDS, wo etabliert.
- Brandschutzmaßnahmen
- Unterbrechungsfreie Stromversorgung (USV).
- Einsatz von Datenbank-Clustern.
- Datenspiegelung relevanter Datenträger.

4.2. Rasche Wiederherstellung

Artikel 32 Absatz 1 Buchstabe c DSGVO

4.2.1. Umgesetzte Maßnahmen

- Regelmäßige Überprüfung der Sicherungs- und Wiederherstellbarkeit.

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

- Betrieb eines Information Security Management System innerhalb der DPDS, welches wesentliche Teile des Datenschutzmanagements umfasst (z.B. Prozesse bei Datenschutzvorfällen, Prozesse bei Notfällen oder Krisen).

5.2. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Artikel 25 Absatz 2 DSGVO

5.2.1. Umgesetzte Maßnahmen

- Privacy-by-design:

  Die Entwicklung neuer Systeme innerhalb der DPDS erfolgt unter Einbezug des betrieblichen Datenschutzbeauftragten.

- Privacy-by-default:

  Sofern Standardsoftware zum Einsatz kommt, werden Werkseinstellungen sofern durch die DPDS veränderbar, so eingestellt, dass diese Datenschutz-freundlich ausgestaltet sind.

5.3. Auftrags- oder Vertragskontrolle bei der DPDS

5.3.1. Umgesetzte Maßnahmen

- Verarbeitung durch Dritte bzw. Unterauftragnehmer nach Maßgabe von Artikel 28 DSGVO ausschließlich auf entsprechende Weisungen des Verantwortlichen.
- Klare und eindeutige vertragliche Vereinbarungen mit Dienstleistern.
- Strenge Kontrollen bei der Auswahl der Dienstleister.
- Regelmäßige Lieferantenaudits.

5.4. Organisationskontrolle

5.4.1. Umgesetzte Maßnahmen

- Das Schutzstufenkonzept bei der Deutschen Post Dialog Solutions GmbH in Anlehnung an das ZAWAS-Modell der Landesbeauftragte für den Datenschutz Niedersachsen (Sonderdokument kann bei DPDS angefordert werden)
- Zutrittsberechtigungen
- Zugangsberechtigungen
- Zugriffsberechtigungen: Kundendaten sind bei der DPDS vor unberechtigtem Zugriff mit einem Berechtigungskonzept nach Nutzergruppen geschützt.
- Datenübertragung:
  Datenübertragungen von Kundendaten werden grundsätzlich SSL-verschlüsselt vorgenommen.
- Verpflichtung der DPDS-Mitarbeiter auf das Datengeheimnis.
- Aufklärung und Schulung der DPDS-Mitarbeiter mit Arbeitsaufnahme.
- Bestellung eines betrieblichen Datenschutzbeauftragten gemäß Vorgaben des § 38 BDSG.

- Einhaltung der Grundsätze zur Funktionstrennung und klare Verantwortungsbereiche.
- Anweisungen und Richtlinien zur Anwendungsentwicklung und Produktion bei der DPDS.
- Systemdokumentation
- Trennung von Test und Produktion.
- Regelungen zu Test und Freigabe.
- Regelungen zu System- und Programmprüfung bei der DPDS sowie zum Löschungskonzept. Anwendungen werden erst nach erfolgter Qualitätssicherung und Freigabe in Betrieb genommen.
- DPDS-Datensicherungskonzept, -plan und -katalog.
- Wartungs- und Reparaturarbeiten:
  Wartungsarbeiten finden in geplanten Wartungsfenstern statt.
- 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
    - Dokumentation von Organisationsprozessen (u.a. Release- / Freigabeprozess / Inbetriebnahme, Anforderungsanalyse) mit definierten Rollen / Verantwortlichkeiten
    - Issue- / Bugtracking