Vertrag zur Auftragsverarbeitung gemäß Artikel 28 DSGVO

zwischen dem
auftragserteilendem Unternehmen
- im Folgenden „Verantwortlicher" genannt -

und der

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

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

PRÄAMBEL

A. Der Verantwortliche und der Auftragsverarbeiter haben einen Dienstleistungsvertrag (Einzelvertrag) abgeschlossen, nach dem der Auftragsverarbeiter Dienstleistungen im Bereich der Auftragsverarbeitung nach Art. 28 DSGVO anbietet. Die Leistungen umfassen in der Regel Druck- und Lettershop- sowie Adressdienstleistungen. Weitere Leistungen, wie zum Beispiel Fulfillment- und Kommissionierungsleistungen sowie Response-Bearbeitung können hinzukommen und werden entsprechend in einem jeweiligen Einzelvertrag spezifiziert.

B. Dieser Auftragsverarbeitungsvertrag kommt, ohne dass es einer weiteren Unterzeichnung bedarf durch den Abschluss des jeweiligen Einzelvertrages und die jeweilige Auftragsübersicht zur Konkretisierung der Datenverarbeitung zustande.

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 Dienstleistungsvertrages (Einzelvertrag) und diesem Vertrag zwischen den Verantwortlichen und dem Auftragsverarbeiter ist Letzterer maßgebend.

Dies vorausgeschickt, wird das Folgende vereinbart:

Der Auftraggeber hat den Auftragnehmer im Rahmen der datenschutzrechtlich bestehenden Sorgfaltspflichten als Dienstleister ausgewählt. Diese Vereinbarung enthält nach dem Willen der Parteien den schriftlichen Auftrag zur Auftragsverarbeitung in dem vertraglich beschriebenen Umfang gemäß Einzelvertrag und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Auftragsverarbeitung.

1. Gegenstand, Art, Zweck, Umfang und Dauer der Auftragsverarbeitung

(1) Gegenstand des Auftragsverarbeitungsvertrages ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag und nach Weisung des jeweiligen Auftraggebers gemäß Einzelvertrag. Die Leistungen umfassen in der Regel Druck- und Lettershop-Leistungen. Optional zusätzlich und soweit Bestandteil des Einzelauftrages: Überprüfung/Korrektur von Adressen aus den Beständen des Verantwortlichen durch Abgleich gegen die Postreferenz-Datei der Deutschen Post Direkt GmbH sowie weiteren Quellen mit Umzugsinformationen über die ADDRESSFACTORY-Systeme. Weitere Leistungen, wie zum Beispiel Fulfillment- und Kommissionierungsleistungen sowie Response-Bearbeitung können hinzukommen. Die Konkretisierung der Datenverarbeitung erfolgt in der jeweiligen Auftragsübersicht zum Einzelvertrag.

(2) Die Tätigkeiten des Auftragnehmers im Rahmen dieser Vereinbarung sowie die vom Auftragnehmer zur Erfüllung der vertraglichen Verpflichtungen zu verwendenden Arten von Daten und die Kategorien der Betroffenen sind in dem jeweiligen Einzelvertrag zu diesem Rahmenvertrag festgelegt. In dem Einzelvertrag ist ferner geregelt, für welche verantwortliche Stelle (Auftraggeber) konkret die Auftragsverarbeitung erfolgt.

(3) Diese Vereinbarung gilt für die Dauer des (zivilrechtlichen) Einzelvertrages sowie der vorgesehenen Speicherdauer von in der Regel 90 Arbeitstage nach Postauflieferung (PAL).

(4) Allein der Auftraggeber ist für die Beurteilung der rechtlichen Zulässigkeit der im Rahmen des Auftragsverhältnisses durchgeführten Verarbeitung personenbezogener Daten durch den Auftragnehmer im Hinblick auf die jeweils anwendbaren Bestimmungen des Datenschutzrechts verantwortlich.

(5) Der Auftragnehmer verarbeitet die personenbezogenen Daten des Auftraggebers ausschließlich zur Erfüllung der Pflichten dieses Auftragsverarbeitungsvertrages, des Einzelvertrages und/oder ergänzender Einzelweisungen. Eine Verarbeitung für eigene Zwecke ist dem Auftragnehmer untersagt.

(6) Absatz (5) wird eingeschränkt, soweit der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(7) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, derzeit ausschließlich in der Bundesrepublik Deutschland, 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.

2. Technisch-organisatorische Maßnahmen

(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 Vertrags, 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 angemessen zu dokumentieren. Nach einvernehmlicher Vereinbarung werden die technischen und organisatorischen Maßnahmen integraler Bestandteil des Vertrags.

(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.

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

(4) 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. Weitere Einzelheiten finden sich in der Anlage 1.

(5) Die in der Anlage 1 beschriebene Auswahl der technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit nach Art. 32 DSGVO, passend zum vom Verantwortlichen angegebenen Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik, orientiert sich hierbei an den Datenkritikalitätsklassifizierungen (low, medium, high, very high) gemäß DHL Group-Konzernklassifizierung. Die Kriterien für die Einstufung der Datenkritikalität von Kundendaten können auf Verlangen des Verantwortlichen übersandt werden und sind unter www.deutschepost.de/datenschutz-dpds einsehbar.

(6) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen sind dem Verantwortlichen in Textform mitzuteilen.

3. Berichtigung, Einschränkung und Löschung von Daten

(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.

(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.

(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.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Die Kontaktdaten des Datenschutzbeauftragten enthält die Anlage 1. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(2) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 lit. c, 32 DSGVO. Weitere Einzelheiten finden sich in der Anlage 1.

(4) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer wird den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, informieren. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(5) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(6) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

Führung der Verarbeitungsübersichten gem. den Anforderungen nach Art. 30 Abs. 2 DSGVO.

(7) 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.

5. Unterauftragsverhältnisse

(1) Der Auftragsverarbeiter darf weitere Auftragsverarbeiter (d. h. Unterauftragnehmer) beauftragen.

(2) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen und bei denen die Datenverarbeitung einen wichtigen (Kern-)Bestandteil ausmacht. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen und Tätigkeiten der Berufsgeheimnisträger (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer) in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu ergreifen.

(3) Falls der Auftragsverarbeiter im Namen des Verantwortlichen einen weiteren Auftragsverarbeiter (Unterauftragsverarbeiter) mit bestimmten Verarbeitungstätigkeiten beauftragt, werden diesem

weiteren Unterauftragsverarbeiter im Wege eines schriftlichen Vertrags dieselben Pflichten wie in diesem Vertrag auferlegt.

(4) Der oder die jeweiligen Unterauftragsverarbeiter sind in der jeweiligen Auftragsübersicht zur Konkretisierung der Datenverarbeitung benannt und gelten mit Unterzeichnung des Einzelvertrages als vom Verantwortlichen genehmigt.

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

(6) Bevor ein weiterer Unterauftragsverarbeiter zum ersten Mal personenbezogene Daten des Verantwortlichen verarbeitet, hat der Auftragsverarbeiter eine angemessene Due-Diligence-Prüfung durchzuführen, um sicherzustellen, dass der weitere Unterauftragsverarbeiter in der Lage ist, dass in diesem Vertrag, dem Dienstleistungsvertrag und nach anwendbarem Recht vorgeschriebene Schutzniveau für die personenbezogenen Daten des Verantwortlichen zu bieten.

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

(8) Unbeschadet des Vorstehenden kommen die Parteien bei Einwendungen des Verantwortlichen gegen die Beauftragung eines weiteren Unterauftragsverarbeiters zusammen, um nach Treu und Glauben über eine geeignete Lösung zu beraten. Der Auftragsverarbeiter kann insbesondere beschließen, (i) den vorgesehenen Unterauftragsverarbeiter nicht einzusetzen oder (ii) von dem Verantwortlichen verlangte Korrekturmaßnahmen zu ergreifen und den Unterauftragsverarbeiter zu beauftragen. Ist keine genannte oder sonstige Option vernünftigerweise durchführbar und hat der Verantwortliche nach wie vor berechtigte Einwendungen, kann der Verantwortliche den Vertrag mit einer Frist von 30 Geschäftstagen schriftlich kündigen.

(9) 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) Der Auftragnehmer hat 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 Auftragnehmer berechtigt, die Ausübung der jeweiligen Weisungen auszusetzen, bis der Verantwortliche diese bestätigt oder ändert.

(11) Die Rechenzentren des Auftragsverarbeiters haben folgende Standorte:

Land	**Anschrift**
Tschechien	Deutsche Post IT Services GmbH c/o DHL Information Services (Europe) Prague s.r.o., V Parku 2308/10, 14800 Praha 4, Chodov, Czech Republic

6. Unterstützungspflichten

(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.

(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.

7. Kontrollrechte des Auftraggebers

(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 IT-Services Prag: min. 6 Wochen. Besondere Vorkommnisse sind:

   a. Der Verantwortliche hat die begründete Vermutung, 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.

(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 Verant-

wortlichen 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.

(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.

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

8. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Die Weisungsberechtigten auf Seiten des Auftraggebers und die Weisungsempfänger auf Seiten des Auftragnehmers werden im jeweiligen Einzelvertrag festgelegt, bzw. deren Unterzeichnenden gelten als Weisungsberechtigte.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der Auftragsarbeiten (in der Regel 90 Arbeitstage nach Postauflieferungstermin (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 zerstören bzw. zu löschen. Gleiches gilt für Testdaten, Datenmüll sowie überflüssiges und verworfenes Datenmaterial. Das Protokoll zur Zerstörung oder Löschung ist auf Verlangen vorzuzeigen.

(3) 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.

10. Haftung

(1) Bei Verstößen gegen datenschutzrechtliche Bestimmungen gelten die Regelungen des Artikels 82 DSGVO.

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

11. Sonstiges

(1) Erweist sich eine Bestimmung dieser Vereinbarung als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen dieser Vereinbarung nicht. Beide Vertragsparteien sind in diesem Falle verpflichtet, unverzüglich in eine nachträgliche Zusatzbestimmung einzuwilligen, die nach Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.

(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.

(3) Auftraggeber und Auftragnehmer sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

(3) Für Ansprüche, die eine betroffene Person wegen einer nach den Datenschutzvorschriften unzulässigen oder unrichtigen Verarbeitung im Rahmen des Auftragsverhältnisses gegenüber Auftragnehmer oder Auftraggeber geltend macht, ist stets der Verursacher verantwortlich. Handelt der Auftragnehmer auf und im Rahmen der Weisung des Auftraggebers, ist stets der Auftraggeber Verursacher im vorgenannten Sinne. Der Verursacher stellt den anderen Vertragspartner von allen Ansprüchen frei, die die betroffenen Personen gegenüber dem anderen Vertragspartner aufgrund von Verletzungen geltend macht, die durch oder im Rahmen der Auftragsdatenverarbeitung gemäß diesem Vertrag erfolgten. Dies gilt entsprechend für die Freistellung gegenüber weiteren Dritten, z.B. Wettbewerbern oder Aufsichtsbehörden. Im Falle einer Pflichtverletzung des Auftragnehmers kann der Auftraggeber den Auftrag zur Verarbeitung bis zur Beseitigung des Verstoßes vorübergehend ganz oder teilweise aussetzen.

(4) Mündliche Nebenabreden sind nicht getroffen. Die Kündigung und die Aufhebung des Vertrags bedürfen der Schriftform. Eine gesonderte Kündigung dieses Vertrags unabhängig vom Bestehen des Einzelvertrages ist nicht möglich. Dies gilt auch für Änderungen oder Ergänzungen, sofern und soweit vorstehend nichts Abweichendes vereinbart ist. Dasselbe gilt bezüglich der vorstehenden Schriftformklausel selbst. Die E-Mail reicht zur Wahrung der Schriftform nicht aus.

(5) Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrags den Regelungen des (zivilrechtlichen) Einzelvertrages vor.

(6) Sämtliche der unten aufgeführten Anlagen sind wesentlicher Bestandteil dieses Vertrags.

Die jeweils aktuelle Fassung dieser Vereinbarung ersetzt alle vorangegangenen Fassungen.

Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland.

Bonn, Mai 2024

Rick, Joachim, DPDS GmbH, Bonn

Digital unterschrieben von Rick, Joachim, DPDS GmbH, Bonn
Datum: 2024.05.13 13:04:59 +02'00'

Corvers, Rainer, DPDS GmbH, Bonn

Digital unterschrieben von Corvers, Rainer, DPDS GmbH, Bonn
Datum: 2024.05.13 12:48:43 +02'00'

Deutsche Post Dialog Solutions GmbH

Auftragsverarbeiter

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	low

Verarbeitung, in der Regel nach der Postauflieferung bei druckbezogenen Verarbeitungen.	
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 Werkseinstellungen - 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 • Dokumentation von Organisationsprozessen (u.a. Release- / Freigabeprozess / Inbetriebnahme, Anforderungsanalyse) mit definierten Rollen / Verantwortlichkeiten. • Issue- / Bugtracking	low