Vertrag zur Auftragsverarbeitung gemäß Artikel 28 DSGVO

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

und der

Deutsche Post Dialog Solutions GmbH
Koblenzer Straße 67
53177 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.

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 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) 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.

(4) 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.

(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. Weitere Einzelheiten finden sich in der Anlage 1.

(6) Die in der Anlage 1 beschriebene Auswahl der technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit nach Art. 32 DSGVO, passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik, orientiert sich an der Schutzstufe C des von der Landesbeauftragten für den Datenschutz Niedersachsen (LfD) entwickelten Prozesses zur Auswahl angemessener Sicherungsmaßnahmen (ZAWAS). Die Schutzstufe C deckt die Anforderungen an die Datenverarbeitung auf der Grundlage dieser Vereinbarung ab.

(7) 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.

3. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft sind nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

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 der 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.

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

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.

(2) 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.

(3) 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.

(4) 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.

(5) 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, das in diesem Vertrag, dem Dienstleistungsvertrag und nach anwendbarem Recht vorgeschriebene Schutzniveau für die personenbezogenen Daten des Verantwortlichen zu bieten.

(6) 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.

(7) 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.

(8) 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.

(9) 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.

6. Kontrollrechte des Auftraggebers

(1) Nach angemessener Vorankündigung von in der Regel sieben Geschäftstagen 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. Dies umfasst auch Vor-Ort-Prüfungen. Auf den regulären Geschäftsbetrieb des Auftragnehmers und gegebenenfalls der jeweiligen Unterauftragnehmer ist dabei angemessen Rücksicht zu nehmen. Der Auftragsverarbeiter hat nach schriftlicher Aufforderung des Verantwortlichen innerhalb einer angemessenen Frist dem Verantwortlichen sämtliche Informationen, Unterlagen und sonstige für die Prüfung erforderlichen Nachweise zu erbringen. Das Prüfungsergebnis ist angemessen zu dokumentieren.

(2) Darüber hinaus 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 im Rahmen dieses Vertrags umsetzt bzw. erfüllt.

   (3) Nimmt der Verantwortliche eine Vor-Ort-Prüfung vor, hat der Auftragsverarbeiter den Verantwortlichen bei dessen Prüfungsprozess angemessen zu unterstützen.

7. Mitteilung bei Verstößen des Auftragnehmers

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

Hierzu gehören u.a.

(a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen,
(b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
(c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen,
(d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,
(e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde,

(2) Für Unterstützungsleistungen, die nicht in dem Einzelvertrag enthalten sind kann der Auftragnehmer eine Vergütung beanspruchen. Gleiches gilt für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind.

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.

(1) 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 zerstören bzw. zu löschen. Gleiches gilt für Testdaten, Datenmüll sowie überflüssiges und verworfenes Datenmaterial. Das Protokoll zur Zerstörung oder Löschung ist auf Verlangen vorzuzeigen.

(2) 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 und Sanktionen

(1) Die gesetzlichen Bestimmungen, insbesondere Artikel 82 DSGVO, gelten im Fall von Schadensersatz- oder Haftungsforderungen.

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

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) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der Datenschutz-Grundverordnung liegen.

(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.

(7) 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.

(8) Die jeweils aktuelle Fassung dieser Vereinbarung ersetzt alle vorangegangenen Fassungen.

Bonn, den 01.12.2021

Rick, Joachim, DPDS GmbH, Bonn

Digital unterschrieben von Rick, Joachim, DPDS GmbH, Bonn
Datum: 2022.01.04 08:16:51 +01'00'

Rainer Corvers

Digital unterschrieben von Rainer Corvers
Datum: 2022.01.03 10:43:18 +01'00'

Deutsche Post Dialog Solutions GmbH

(Auftragsverarbeiter)

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.

Der externe, betriebliche Datenschutz-Beauftragte der Deutschen Post Dialog Solutions GmbH ist:

Herr Rechtsanwalt Markus Giese
Dreizehnmorgenweg 6, 53175 Bonn
Telefon +49 228 948 25 55
Telefax +49 228 948 25 56
Mobil +49 171 722 34 44
E-Mail markus.giese.extern@postdirekt.de
E-Mail rechtsanwalt.giese@t-online.de

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

- 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.
- Sofern personenbezogene Daten nur noch für statistische Zwecke der DPDS benötigt werden, werden diese anonymisiert.

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 datenschutzfreundlich 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 Landesbeauftragten für den Datenschutz Niedersachsen (Sonderdokument kann bei der 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-neu.
- 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.
- Information Security Management System der DPDS in Anlehnung an DIN ISO 27001.