Vertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter

Nutzer des Services TRACK&MATCH

nachfolgend der „Verantwortliche“

Deutsche Post AG
Charles-de-Gaulle-Str. 20
53113 Bonn

nachfolgend der „Auftragsverarbeiter“

nachfolgend zusammen als „**Partei**“/„**Parteien**“ bezeichnet

PRÄAMBEL:

A. Der Auftragsverarbeiter erbringt Dienstleistungen zur Realisierung des Services TRACK&MATCH.

B. Der Verantwortliche und der Auftragsverarbeiter haben einen Dienstleistungsvertrag zur Nutzung des Services TRACK&MATCH abgeschlossen, nach dem der Auftragsverarbeiter Dienstleistungen zur Realisierung des Services TRACK&MATCH anbietet.

C. Die Parteien möchten die Vereinbarung der Parteien 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.

D. 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 dem 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 Dienstleistungen, die unabhängig vom Gegenstand dieses Vertrags 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 Datenschutzgesetze 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 zur Nutzung von TRACK&MATCH, den die Parteien in Bezug auf die Erbringung von Dienstleistungen durch den Auftragsverarbeiter abgeschlossen haben.

1. Gegenstand/Umfang der Verarbeitung

Der Gegenstand/Umfang der vom Auftragsverarbeiter zu leistenden Datenverarbeitung ist im Dienstleistungsvertrag geregelt, worauf hiermit vollständig Bezug genommen wird.

2. Laufzeit

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Dienstleistungsvertrags.

3. Spezifikationen der Verarbeitung

(1) Art und Zweck der beabsichtigten Verarbeitung

Art und Zweck der Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen sind im Dienstleistungsvertrag festgelegt.

(2) Die Durchführung der vertraglich vereinbarten Datenverarbeitung erfolgt ausschließlich innerhalb der EU/des EWR. Jede einzelne Übermittlung personenbezogener Daten über die EU/den EWR hinaus erfordert die vorherige (schriftliche (auch per E-Mail)) Zustimmung des Verantwortlichen und erfolgt nur dann, wenn die in Artikel 44 ff. DSGVO dargelegten bestimmten Bedingungen erfüllt wurden.

(3) Arten von Daten

Der Gegenstand der Verarbeitung personenbezogener Daten beinhaltet die folgenden Arten/Kategorien von Daten (Auflistung/Beschreibung der Datenkategorien).

- Name
- Kontaktdaten
- Vertragsdaten
- Kundenhistorie
- Position/Funktion

(4) Betroffene Person

Die Kategorien von betroffenen Personen beinhalten:

- Kunden des Services TRACK&MATCH
- Kunden und Dienstleister von TRACK&MATCH-Kunden (Empfänger bzw. Druck- und Lettershops)

4. Technische und 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 und dem Verantwortlichen zur Genehmigung vorzulegen. 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. In jedem Fall müssen die technischen und organisatorischen Maßnahmen den Anforderungen der Informationssicherheits-Richtlinie von DPDHL entsprechen.

(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. Auf Verlangen hat der Auftragsverarbeiter eine angemessene Dokumentation vorzulegen.

5. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragsverarbeiter darf 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.

6. 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,

(1) 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.

(2) 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.

(3) einen Datenschutzbeauftragten zu ernennen oder, falls er nicht zur Ernennung eines Datenschutzbeauftragten verpflichtet ist, einen sonstigen Ansprechpartner zu ernennen, der für Fragen des Datenschutzes verantwortlich zeichnet. Die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen verantwortlichen Person sind dem Verantwortlichen mitzuteilen, damit dieser direkt Kontakt aufnehmen kann. Der Verantwortliche ist über etwaige diesbezügliche Änderungen unverzüglich in Kenntnis zu setzen.

(4) ein Verzeichnis aller Verarbeitungstätigkeiten zu führen.

(5) 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.

(6) 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.

(7) 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.

(8) 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.

7. Unterbeauftragung

(1) Der Auftragsverarbeiter darf ohne die vorherige ausdrückliche schriftliche Zustimmung des Verantwortlichen keinen weiteren Auftragsverarbeiter (d. h. Unterauftragnehmer) beauftragen.

(2) Falls der Auftragsverarbeiter im Namen des Verantwortlichen einen weiteren Auftragsverarbeiter mit bestimmten Verarbeitungstätigkeiten beauftragt, werden diesem weiteren Auftragsverarbeiter im Wege eines schriftlichen Vertrags dieselben Pflichten wie in diesem Vertrag auferlegt.

(3) Auf der Grundlage der in dieser Ziffer enthaltenen Bestimmungen erteilt der Verantwortliche seine Zustimmung zu dem/den folgenden weiteren Auftragsverarbeiter(n):

Firma	**Anschrift**	**Beschreibung der Dienstleistungen**
Deutsche Post Dialog Solutions GmbH	Koblenzer Str. 67 53177 Bonn	Wartung und Betrieb TRACK&MATCH Backend
Plusserver Niederlassung Düsseldorf	In der Steele 37 40599 Düsseldorf	Rechnerstandort TRACK&MATCH Backend
DHL IT Services	V Parku 2308/10, Prag Prag 148 00 Tschechische Republik	Rechnerstandort TRACK&MATCH Frontend

Deutsche Post IT Services GmbH	Wielandstraße 4 53173 Bonn Germany	Wartung und Betrieb TRACK&MATCH Frontend

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

(5) Bevor ein weiterer Auftragsverarbeiter zum ersten Mal personenbezogene Daten des Verantwortlichen verarbeitet, hat der Auftragsverarbeiter eine angemessene Due-Diligence-Prüfung durchzuführen, um sicherzustellen, dass der weitere Auftragsverarbeiter 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 Auftragsverarbeiters durch den Auftragsverarbeiter, hat der Verantwortliche dies dem Auftragsverarbeiter umgehend schriftlich innerhalb von 14 Geschäftstagen 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 sei 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 verstoßen hat) oder ein Wettbewerber des Verantwortlichen ist.

(7) 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, (i) den vorgesehenen Auftragsverarbeiter nicht einzusetzen oder (ii) 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, kann der Verantwortliche den Vertrag mit einer Frist von 30 Tagen 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.

8. Prüfrechte

(1) Nach angemessener Vorankündigung von mindestens 5 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. Dies umfasst auch Vor-Ort-Prüfungen. Der Auftragsverarbeiter hat nach schriftlicher Aufforderung des Verantwortlichen innerhalb einer angemessenen Frist dem Verantwortlichen sämtliche Informationen, Unterlagen und sonstigen 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.

9. 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. Zu den mindestens zu übermittelnden Informationen zählen die Art der Verletzung des Schutzes personenbezogener Daten, die Kategorien und die Zahl der

betroffenen Personen, die Kategorien und die Zahl der Datensätze sowie die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

(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.

10. Löschung und Rückgabe personenbezogener Daten

(1) Nach Abschluss der Auftragsarbeiten oder vorher auf Verlangen des Verantwortlichen, jedoch spätestens bei Beendigung des Dienstleistungsvertrags, 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 auszuhändigen oder – nach vorheriger Zustimmung – zu zerstören. 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.

11. Schlussbestimmungen

(1) Eine Änderung oder Ergänzung dieses Vertrags bedarf der Schriftform und der Unterzeichnung der ordnungsgemäß bevollmächtigten Vertreter beider Parteien.

(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) 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.

(4) Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland.

Bonn, den 04.03.2020

Anhang 1 – Technische und organisatorische Maßnahmen

(1) Vertraulichkeit (Artikel 32 Absatz 1 Buchstabe b DSGVO)

- Physische Zugangskontrolle

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

- 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

- Interne Zugangskontrolle (Nutzerrechte für den Zugang zu und die Änderung von Daten)

  Kein unbefugtes Lesen, Kopieren, Ändern oder Löschen von Daten im System, z. B. Berechtigungskonzept, Zugangsrechte auf Need-to-know-Basis, Zugangsprotokollierung

- Trennung nach Zweck

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

- 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) Integrität (Artikel 32 Absatz 1 Buchstabe b DSGVO)

- 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 (Virtual Private Networks, VPN), elektronische Signaturen

- 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) Verfügbarkeit und Belastbarkeit (Artikel 32 Absatz 1 Buchstabe b DSGVO)

- 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

- Rasche Wiederherstellung (Artikel 32 Absatz 1 Buchstabe c DSGVO)

(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Absatz 1 Buchstabe d DSGVO; Artikel 25 Absatz 1 DSGVO)

- Datenschutzmanagement
- Reaktionsmanagement
- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Artikel 25 Absatz 2 DSGVO)
- Auftrags- oder Vertragskontrolle

  Verarbeitung durch Dritte nach Maßgabe von Artikel 28 DSGVO ausschließlich auf entsprechende Weisungen des Verantwortlichen, z. B. klare und eindeutige vertragliche Vereinbarungen, formalisierte Auftragsverwaltung, strenge Kontrollen bei der Auswahl der Dienstleister, verpflichtende Vorab-Evaluierung, Nachkontrollen zur Überwachung.

Konkrete technische und organisatorische Maßnahmen

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Maßnahme	**Kommentar**
1. Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde) und regelmäßige Überprüfung von vergebenen Zutrittsrechten	
2. Berechtigungsausweise	
3. Schlüsselregelung	
4. Regelung für Firmenfremde	
5. Anwesenheitsaufzeichnungen	
6. Besucherausweise	
7. Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz	
8. Türsicherung (elektrischer Türschließer, Ausweisleser, Fernsehmonitor, Pförtner)	
9. Einbau von Schleusen	
10. Entsprechende Ausgestaltung der Maßnahmen zur Objektsicherung (Einbruchmeldesystem, regelmäßige Kontrollrundgänge)	

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Maßnahme	**Kommentar**
1. Vergabe und Sicherung von personifizierten Zugangsdaten und SSH-Keys zur Authentifizierung	
2. Zeitlich beschränkte Nutzung von personifizierten Zugangsdaten; regelmäßiger Passwortwechsel	
3. Regelung der Benutzerberechtigung: regelmäßige Überprüfung der Zugangsrechte	
4. Verpflichtung der Mitarbeiter auf das Datengeheimnis	
5. Verschlüsselung von Notebooks und Laptops	
6. Kontrollierte Vernichtung von Datenträgern	
7. Arbeitsanweisung und Bearbeitungsverfahren für Datenerfassungsvorlagen	
8. Prüf- und Kontrollsysteme	Anti-Viren-Software, Firewalls, Event-Logs, VPN bei Remote-Zugriffen
9. Definierte Prozesse zur Rechteverwaltung	

3. Zugriffskontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Maßnahme	**Kommentar**
1. Verschlüsselung von Kommunikationswegen	
2. Regelung der Zugriffsberechtigung	
3. Überprüfung der Berechtigung, maschinell z. B. durch Identifizierungsschlüssel	
4. Auswertung von Protokollen	
5. Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen	
6. Differenzierte Zugriffsregelung	Minimalprinzip etabliert
7. Protokollierung von fehlerhaften Zugriffsversuchen	

4. Weitergabekontrolle

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

Maßnahme	**Kommentar**
1. Verschlüsselung	
2. Feststellung befugter Personen	
3. Festmontierte Plattenspeicher	
4. Bestandskontrolle	
5. Gesonderter Verschluss vertraulicher Datenträger	
6. Sicherheitsschränke	
7. Protokollierung von Zugriffen auf Anwendungen und IT-Systeme	
8. Bestimmte autorisierte Benutzer	
9. Plausibilitätsprüfung	
10. Vollständigkeits- und Richtigkeitsprüfung	
11. Löschung von Datenresten vor Datenträgeraustausch über Datenlöschsoftware	DBAN und Secure Erase
12. Entmagnetisierung von Datenträgern vor Entsorgung	

5. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahme	**Kommentar**
1. Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe	
2. Protokollierung von Eingaben	
3. Protokollierung der Dateibenutzung	
4. Verfahrens-, Programm- und Arbeitsablauforganisation	
5. Verpflichtung auf das Datengeheimnis	

6. Auftragskontrolle

Es ist zu gewährleisten, dass der Auftragnehmer den Auftraggeber bei der Durchführung der in dem Vertrag geregelten Kontrollen unterstützt.

7. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahme	**Kommentar**
Regelmäßige Backups von Produktivsystemen	
Anlagen zur Brandbekämpfung, autonomen Stromversorgung und Klimakontrolle	

8. Zweckbindungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Maßnahme	**Kommentar**
1. Mandantentrennung	
2. Funktionstrennungen	