VEREINBARUNG FÜR DIE AUFTRAGSVERARBEITUNG (STAND JANUAR 2019)

Allgemeines

Die Regelungen dieser Vereinbarung zur Auftragsverarbeitung gelten zwischen der DHL Paket GmbH - nachfolgend "Auftragsverarbeiter" genannt - und ihren Kunden - nachfolgend "Verantwortliche" genannt - für die über die zur Erbringung von Postdienstleistung erforderliche Datenverarbeitung hinausgehende Verwaltung von personenbezogenen Daten in den bereitgestellten Online-Systeme zur Versandvorbereitung. Diese Vereinbarung findet nur Anwendung, soweit "Verantwortliche" die von der DHL Paket GmbH bereitgestellten Adressbuchfunktionen zur dauerhaften und sendungsunabhängigen Verwaltung ihrer Kundenadressen nutzen.

Gegenstand der Verarbeitung

Die DHL Paket GmbH stellt den Verantwortlichen mit den Online-Systemen, insbesondere des DHL Geschäftskundenportals, DHL Abholportals, DHL Retourenportals und DHL Lieferantenportals zusätzliche - nicht für die Erbringung von Postdienstleistungen notwendige - Funktionen zur dauerhaften und sendungsunabhängigen Verwaltung ihrer Kundenadressen - nachfolgend "Adressbuchfunktionen" genannt - zur Verfügung.

Laufzeit

Diese Vereinbarung zur Auftragsverarbeitung gilt für einen unbegrenzten Zeitraum und kann vom Verantwortlichen jederzeit durch die Einstellung der Nutzung der Adressbuchfunktionen sowie Löschung aller gespeicherten Daten in den Adressbuchfunktionen beendet werden.

Spezifikationen der Verarbeitung

1. Art und Zweck der beabsichtigten Verarbeitung
   Die Nutzung der Adressbuchfunktionen ist optional und dient der dauerhaften und sendungsunabhängigen Verwaltung der Kundenadressen des Verantwortlichen. Die Eingabe, Änderung, Speicherung und Löschung erfolgt durch den Verantwortlichen selbst. Die Nutzung dieser Adressbuchfunktionen ist für die Erbringung von Postdienstleistungen nicht erforderlich, sondern unterstützt lediglich den Verantwortlichen bei der Verwaltung seiner Versandadressen.

2. Die Durchführung der 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:
   - Name
   - Kontaktdaten
   - Adresse

Betroffene Person

Die Kategorien von betroffenen Personen beinhalten:

- Vertragskunden von DHL Paket GmbH
- Kunden von Vertragskunden der DHL Paket GmbH
- Beauftragte von Vertragskunden der DHL Paket GmbH

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 dieser Vereinbarung, erfüllt. Der Auftragsverarbeiter erkennt hiermit die Rechte der betroffenen Personen, wie vorstehend angegeben, an und gewährleistet diese. Zu diesem Zweck und nach Maßgabe von Art. 32 DSGVO ergreift der Auftragsverarbeiter technische und organisatorische Maßnahmen und bestätigt hiermit deren Umsetzung.

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 dieser Vereinbarung vereinbarte Niveau sinken.

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 dieser Vereinbarung vereinbarte Sicherheit der Verarbeitung zu gewährleisten.

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 Vergessen werden" 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.

Pflichten des Auftragsverarbeiters

Neben den in dieser Vereinbarung 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.

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 dieser Vereinbarung 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 dieser Vereinbarung 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 Ver-

antwortlichen 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.

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 dieser Vereinbarung auferlegt.

3. Auf der Grundlage der in dieser Ziffer enthaltenen Bestimmungen stimmt der Verantwortliche zu, dass der Auftragsverarbeiter Unterauftragnehmer hinzuziehen kann. Vor Hinzuziehung oder Ersetzung der Unterauftragnehmer informiert der Auftragsverarbeiter den Verantwortlichen rechtzeitig mit angemessener Vorankündigung über einen neuen weiteren Auftragsverarbeiter (einschließlich der vollständigen Angaben zu der von dem neuen Auftragsverarbeiter vorgenommenen Verarbeitung). Die Vorankündigung erfolgt im DHL Geschäftskundenportal.

4. 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 dieser Vereinbarung, dem Dienstleistungsvertrag und nach anwendbarem Recht vorgeschriebene Schutzniveau für die personenbezogenen Daten des Verantwortlichen zu bieten.

5. Hat der Verantwortliche berechtigte Einwendungen gegen den Einsatz eines weiteren Auftragsverarbeiters durch den Auftragsverarbeiter, hat der Verantwortliche dies dem Auftragsverarbeiter umgehend schriftlich innerhalb von fünf 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.

6. 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 von dieser Vereinbarung durch Löschen aller gespeicherten Daten und Einstellung der Nutzung der Adressbuchfunktionen zurücktreten.

7. 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.

Prüfrechte

1. Nach angemessener Vorankündigung von mindestens 10 Geschäftstagen seitens des Verantwortlichen und um die Einhaltung der technischen und organisatorischen Sicherheitsmaßnahmen sowie der aus dieser Vereinbarung erwachsenden Pflichten sicherzustellen und zu überprüfen, hat der Auftragsverarbeiter dem Verantwortlichen oder einem von dem Verantwortlichen beauftragten Prüfer die Durchführung regelmäßiger Prüfungen zu gestatten, wenn
   (a) der Verantwortliche die begründete Vermutung hat, dass der Auftragsverarbeiter nicht im Einklang mit den technisch-organisatorischen Maßnahmen und / oder den Verpflichtungen aus dieser Vereinbarung 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 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 dieser Vereinbarung 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 Wettbewerbsverhältnis zum Auftragsverarbeiter stehen.

4. Sofern die Prüfung seitens des Auftragsverarbeiters oder eines anderen Auftragsverarbeiters Aufwendungen bedeutet, die über einen Geschäftstag hinausgehen, ist der Verantwortliche damit einverstanden, jeden darüber hinaus gehenden Tag zu erstatten.

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.

Löschung und Rückgabe personenbezogener Daten

1. Nach Abschluss der Auftragsarbeiten oder vorher auf Verlangen des Verantwortlichen, jedoch spätestens bei Beendigung der Nutzung der Adressbuchfunktionen, hat der Auftragsverarbeiter dem Verantwortlichen die Löschung der personenbezogenen Daten anzuzeigen.

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.

Streitbeilegung

Ausschließlicher Gerichtsstand für Streitigkeiten aus dieser Vereinbarung und aus allen einzelnen Frachtverträgen in seinem Anwendungsbereich ist Bonn. Es gilt deutsches Recht.

Schlussbestimmungen

1. 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.

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

3. Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland.

Anhang 1: Technische und organisatorische Maßnahmen

Innerhalb ihres Verantwortungsbereichs ergreift die DHL Paket GmbH bei der Verarbeitung personenbezogener Daten die folgenden technischen und organisatorischen Maßnahmen.

1. Zutrittskontrolle

Ziel:
Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt.

Grundsätze:

- Einrichtung von unterschiedlichen Sicherheitszonen (SK1 - SK4). Grundsätzlich wird unterschieden zwischen öffentlichen Bereichen, Büroflächen und Technikflächen (Data Center, Netzwerkräume).
- Es findet eine angemessene Zutrittskontrolle zwischen den Sicherheitszonen mit unterschiedlicher Schutzklassifizierung statt.
- Es ist ein formales Verfahren zur Vergabe/Änderung/Entzug von Zutrittsberechtigungen implementiert.
- Es ist ein formales Verfahren zur Begleitung von Besuchern und Fremdpersonal implementiert.

Maßnahmen:

- Überwachte Personenschleusen zu den Sicherheitsbereichen
- Sicherheitsbereiche sind definiert
- Eine Identifikation des zugangsberechtigten Personenkreises erfolgt mittels maschinenlesbarer Ausweise
- Schließregel gemäß Hausordnung
- Das Tragen von Unternehmensausweisen wird von den Sicherheitskräften ständig überwacht.
- Außenhautsicherung durch spezielle bauliche Maßnahmen, Alarmanlagen, Einbruchmeldesystem, Wachdienst
- Protokollierung der Zu- und Abgänge

2. Zugangskontrolle

Ziel:
Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Grundsätze:

- Die individuelle Identifikation von Benutzern erfolgt grundsätzlich personenbezogen.
- Die Authentifizierung, d.h. die Verifikation der vorgetragenen Identifikation, erfolgt mindestens mittels Passwort.
- Die Qualität (Aufbau, Länge, etc.) der Passwörter und die Rahmenbedingungen ihres Einsatzes (Speicherung, Übertragung, etc.) entsprechen den geltenden Sicherheitsstandards.
- Die Zugangs- und Zugriffsberechtigungen werden regelmäßig mindestens einmal im Jahr auf Aktualität und Gültigkeit überprüft. Die Ergebnisse werden revisionssicher protokolliert.
- Das Einrichten, Löschen oder Verändern der Zugangs- und Zugriffsberechtigungen erfolgt über etablierte Betriebsprozesse.

Maßnahmen:

- Absicherung der Übertragungsleitungen durch besondere bauliche Maßnahmen
- Maßnahmen zu Benutzer- und Zugangskontrolle für alle Komponenten des Betriebs
- Das Netz ist über Firewall-Systeme gegenüber dem Internet und anderen Netzen abgesichert
- Kennwortverfahren zur sicheren Identifikation mit anschließender Authentifizierung des Nutzers
- Verbindliche Regelung zur Sperrung von Workstations bei Verlassen des Arbeitsplatzes (z.B. Kennwort oder Pausenschaltung)
- Benutzerverwaltung mit Berechtigungsstufen
- Verbindlicher Prozess für Vergabe, Kontrolle und Entzug von Zugangsberechtigungen
- Der administrative Zugang zu Systemen wird auf Netzwerkebene abgesichert

3. Zugriffskontrolle

Ziel:
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.

Grundsätze:

- Der Standard-Benutzer hat keinen schreibenden Zugriff auf Systemdateien und besitzt keine administrativen Privilegien.
- Die Benutzerverwaltung erfolgt zentral, wenn technisch realisierbar.
- Administrative Konten wie z.B. root und DBA werden personalisiert. Sofern dies bei den eingesetzten Objekten nicht möglich ist, werden geeignete Verfahren oder Tools wie etwa Sudo bei Unix eingesetzt.
- Der administrative Zugang zu Systemen in Kunden-Umgebungen wird auf Netzwerkebene durch geeignete Sicherheitsmechanismen abgesichert.

Maßnahmen:

- Definierte, revisionsfähige Berechtigungskonzepte für System-, Datenbank- und Anwendungsebene
- Berechtigungskonzepte beinhalten u.a. die Prozessbeschreibung der Rechtevergabe und des Rechteentzugs unter Anwendung des 4-Augen-Prinzips sowie „Need to know"-Prinzips für den Zugang auf Ressourcen und Informationen
- Differenzierte Zugriffsberechtigungen (Profile, Rollen)
- Verbindlicher Prozess für Vergabe, Kontrolle und Entzug von Zugriffsberechtigungen
- Identifikation und Authentifizierung der Benutzer gem. den Berechtigungskonzepten und Prozessabläufen zur Änderung von Berechtigungskonzepten. Identifikation und Authentifizierung der System- u. Datenbankadministratoren.
- Passwortrichtlinien mit definierten Gültigkeitszeiträumen und Historiendokumentationen
- Protokollierung der zugriffsberechtigten Personen und deren AN-/Abmeldungen
- Verschlüsselung von Dateien im Bedarfsfall

4. Weitergabekontrolle

Ziel:
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 welcher Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Grundsätze:

- Sicherheitsrelevante systembezogene Ereignisse und Zugänge zum System werden protokolliert (Systemlog) und die Loginformationen für 90 Tage vorgehalten. Eine darüber hinausgehende benutzerbezogene Protokollierung von Aktivitäten findet nicht statt.
- Die Auswertung der Loginformationen erfolgt anlassbezogen unter Berücksichtigung rechtlicher Vorgaben.
- Loginformationen werden über das reguläre Backup Verfahren gesichert. Ein Wiederherstellen der Loginformationen erfolgt ausschließlich über das etablierte Change-Verfahren.
- Als Basis für die eingesetzten Verschlüsselungstechnologien werden bewährte und anerkannte Standardverfahren und vorgeschlagene Mindestlängen der Schlüssel verwendet.
- Die Anwendung muss eine Veränderung der Schlüssellänge berücksichtigen können.
- Auf mobilen Datenträgern dürfen vertrauliche Daten ausschließlich verschlüsselt abgelegt werden.

Maßnahmen:

- Versand von Datenträgern erfolgt in versiegelten Transportbehältern
- Gesicherte bzw. verschlüsselte Übertragungswege
- Protokollierung durch aktive Netzkomponenten und im Bedarfsfall Auswertung durch das Netzzentrum
- Kontrollierte Vernichtung von Datenträgern
- Verschlüsselungsverfahren nach Stand der Technik

5. Eingabekontrolle

Ziel:

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

Grundsätze:

- Für den sicheren Betrieb einer Anwendung ist ein Sicherheitskonzept vorhanden, das mindestens folgende Punkte einschließt:
    - Ein Berechtigungskonzept ist erstellt und eine entsprechende Benutzerverwaltung eingerichtet.
    - Benutzerkonten in der Anwendung nutzen weder fest programmierte Passwörter noch fest zugeordnete User-IDs.
    - Passworte werden kryptographisch verschlüsselt gespeichert und übertragen.
- Sicherheitsfeatures der jeweiligen Programmiersprachen und Tools sind zu nutzen und dürfen die Sicherheit des zugrunde liegenden Systems nicht gefährden oder beeinflussen.
- Sämtliche entwicklungs- bzw. testspezifischen Protokollierungsprozesse werden vor Freigabe der Software in den Betriebsprozess deaktiviert bzw. entfernt.

- Sicherheitsrelevante systembezogene Ereignisse und Zugänge zum System werden protokolliert (Systemlog) und die Loginformationen für 90 Tage vorgehalten. Eine darüber hinausgehende benutzerbezogene Protokollierung von Aktivitäten findet nicht statt.
- Die Auswertung der Loginformationen erfolgt anlassbezogen unter Berücksichtigung vertraglicher und rechtlicher Vorgaben.
- Loginformationen werden über das reguläre Backup Verfahren gesichert. Ein Wiederherstellen der Loginformationen erfolgt ausschließlich über das etablierte Changeverfahren.

Maßnahmen:

- Führung von Nachweisen der organisatorisch festgelegten Zuständigkeiten für die Eingabe
- Identifikation und Authentifizierung der Benutzer gemäß den Berechtigungskonzepten
- Authentifizierungskonzept
- Protokollierung und Protokollauswertung
- Sicherung der Protokolldateien gegen unbefugte Nutzung und Veränderung

6. Auftragskontrolle

Ziel:

Gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Grundsätze:

- Der Auftragsverarbeiter folgt gemäß Art. 28 DSGVO bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten ausschließlich den Weisungen des Auftraggebers. Außerhalb von Weisungen verwendet der Auftragsverarbeiter die ihr zur Erhebung, Verarbeitung oder Nutzung überlassenen Daten weder für eigene Zwecke noch für Zwecke Dritter (Zweckbindungsgrundsatz). Verstößt eine Weisung nach Ansicht des Auftragsverarbeiters gegen Datenschutzbestimmungen, weist der Auftragsverarbeiter den Auftraggeber schriftlich darauf hin.
- Der Auftragsverarbeiter setzt ausschließlich Mitarbeiter ein, die angemessene Vertraulichkeitsvereinbarungen unterzeichnet und gemäß § 39 PostG auf das Postgeheimnis sowie (im Anwendungsbereich des TKG) gemäß § 88 TKG auf das Fernmeldegeheimnis verpflichtet sind. Die Verpflichtungserklärungen werden als Muster auf Nachfrage zu Prüfungszwecken im Rahmen von Audits im Original vorgelegt.
- Der Auftragsverarbeiter informiert den Auftraggeber bei Störungen des Verarbeitungsablaufes, bei Verdacht auf Datenschutzverletzungen und anderen Unregelmäßigkeiten bei der Verarbeitung von personenbezogenen Daten des Auftraggebers schriftlich.
- Der Auftraggeber ist berechtigt, die Einhaltung der geltenden Datenschutzvorschriften und der Datensicherungsmaßnahmen in Bezug auf die Verarbeitung seiner Daten nach vorheriger Abstimmung mit der Datenschutzorganisation des Auftragsverarbeiters zu überprüfen.
- Der Auftragsverarbeiter beauftragt Lieferanten mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ausschließlich im Rahmen eines Vertrages zur Auftragsverarbeitung nach Art. 28 DSGVO.
- Die Auftragskontrolle erfolgt auf Basis eines beim Auftragsverarbeiter etablierten Frameworks zur Umsetzung der gesetzlichen und Konzernanforderungen bei der Auftragsverarbeitung (AV).

Maßnahmen:

- Anwendung stellt sicher, dass Erhebung, Verarbeitung und Nutzung personenbezogener Daten ausschließlich innerhalb des Vertrauensbereichs des Verantwortlichen erfolgt
- Formalisierte Auftragserteilung
- Maßnahmen zur Überprüfung der ordnungsgemäßen Vertragsausführung

7. Verfügbarkeitskontrolle

Ziel:
Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Grundsätze:

- Datenträger werden ausschließlich im Robotersystem bzw. im Sicherheitsarchiv gelagert.
- Alle ein- und ausgehenden Datenträger werden im Sicherheitsarchiv gelagert.

Maßnahmen:

- Ein Datensicherungskonzept ist erstellt

8. Zweckbindungskontrolle

Ziel:
Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Grundsätze:

- Jedes neu entwickelte System bzw. jede Applikation muss das PSA-Verfahren (Privacy & Security Assessment) durchlaufen. Sämtliche Änderungen müssen im Review des PSA berücksichtigt werden.
- Freigabeverfahren zur Übergabe in die Produktion werden eingesetzt.
- Die Entwicklung wird auf Standardsystemen mit aktuellen Patch-Ständen und Standard-Sicherheitseinstellungen betrieben, sofern technisch realisierbar und vom Kunden freigegeben.
- Abhängigkeiten zum Betriebssystem bzw. zur verwendeten Middleware werden abgestimmt und dokumentiert.
- Applikationsspezifische sicherheitsrelevante Einstellungen werden im Sicherheitskonzept der Anwendung entsprechend dokumentiert.
- Entwicklungs-, Test- und Abnahme-Systeme werden, sofern technisch sinnvoll möglich und vertraglich geregelt, in unabhängigen Netzsegmenten betrieben.
- Test- und Produktionsdaten werden getrennt gehalten.
- Personenbezogene Daten werden vor Einsatz als Testdaten anonymisiert bzw. pseudonymisiert, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Maßnahmen:

- Logische Trennung des Datenbestandes
- Physikalische Trennung der Datenspeicher
- Anonymisierung bzw. Pseudonymisierung von Testdaten
- Trennung von Test-, Entwicklungs- und Produktionsumgebungen
- Richtlinien und Arbeitsanweisungen für Entwicklung und Betrieb

Begriffsbestimmungen und Auslegung

Begriff	Zweck
Anhang	"Anhang" bezeichnet jeden Anhang zu dieser Vereinbarung, der als Vereinbarungsbestandteil anzusehen ist.
Auftragsverarbeiter	"Auftragsverarbeiter" bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Datenschutzgesetze	"Datenschutzgesetze" bezeichnet die EU-Datenschutzgesetze und, soweit anwendbar, die Datenschutzgesetze eines anderen Landes.
Dienstleistungen	"Dienstleistungen" bezeichnet sämtliche Dienstleistungen, die der Auftragsverarbeiter, wie im Rahmen dieser Dienstleistungsvereinbarung vereinbart, erbringt.
Dienstleistungsvereinbarung	"Dienstleistungsvereinbarung" bezeichnet die Vereinbarung, die die Parteien in Bezug auf die Erbringung von Dienstleistungen durch den Auftragsverarbeiter abgeschlossen haben.
DSGVO	"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).
EWR	"EWR" bezeichnet den Europäischen Wirtschaftsraum und besteht aus sämtlichen Ländern der Europäischen Union, Liechtenstein, Norwegen und Island.
Nebendienstleistungen	"Nebendienstleistungen" bezeichnet Dienstleistungen, die unabhängig vom Gegenstand dieser Vereinbarung 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.
Personenbezogene Daten	"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.
Verantwortlicher	"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.
Verarbeitung	"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.
Vereinbarung	"Vereinbarung" bezeichnet diese Vereinbarung samt den beigefügten Anhängen.
Weiterer Auftragsverarbeiter	"Weiterer Auftragsverarbeiter" bezeichnet einen von dem Auftragsverarbeiter im Lauf der Erbringung der Dienstleistungen beauftragten Datenverarbeiter.