# Vereinbarung zur Auftragsverarbeitung

## 1. Allgemein

Die Regelungen dieser Vereinbarung zur Auftragsverarbeitung gelten zwischen der Deutschen Post AG – nachfolgend „Auftragsverarbeiter“ genannt – und ihren Kunden – nachfolgend „Verantwortlicher“ genannt – für die über die zur Erbringung von Postdienstleistung erforderliche Datenverarbeitung hinausgehende Verwaltung von personenbezogenen Daten im DHL Geschäftskundenportal.

## 2. Gegenstand der Verarbeitung

Der Auftragsverarbeiter stellt dem Verantwortlichen mit dem DHL Geschäftskundenportal die zusätzliche – nicht für die Erbringung von Postdienstleistungen notwendige – Funktion „Verfolgen Brief“ zur Sendungsverfolgung zur Verfügung. Mit der Funktion erhält der Kunde eine Übersicht zu den bei der DPAG eingelieferten Sendungen einschließlich der Empfängerdaten, des aktuellen Sendungsstatus und der Sendungsverläufe zur Verfügung gestellt.

## 3. Laufzeit

Diese Vereinbarung zur Auftragsverarbeitung ist an die Laufzeit des Hauptvertrages gekoppelt.

## 4. Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang I aufgeführt.

## 5. Pflichten der Parteien

1. Weisungen
   a. Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren. Da es sich bei der Funktion „Verfolgen Brief“ um einen standardisierten Service für eine Vielzahl von Kunden handelt, behält sich der Auftragsverarbeiter das Recht zur fristlosen Kündigung des Vertrags über die Bereitstellung und Nutzung des Service „Verfolgen Brief“ durch die Deutsche Post AG vor, wenn die Weisungen des Verantwortlichen im Rahmen des standardisierten Verfahrens nicht befolgt werden können.
   b. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.
2. Zweckbindung

   Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang I genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.
3. Sicherheit der Verarbeitung
   a. Der Auftragsverarbeiter ergreift mindestens die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.
   b. Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
4. Dokumentation und Einhaltung der Klauseln
   a. Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.
   b. Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.
   c. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten, wenn

- 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;
- sich ein Sicherheitsvorfall ereignet hat;
- eine solche Prüfung von der für den Verantwortlichen zuständigen Aufsichtsbehörde gefordert wird.

Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d. Ungeachtet des Vorstehenden kann der Nachweis für die Einhaltung der Vorschriften folgendermaßen erbracht werden:
   - Einhaltung der genehmigten Verhaltensregeln und/oder
   - Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Artikel 42 DSGVO und/oder
   - 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.

e. Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt. Führt der Verantwortliche ein Audit in den Räumlichkeiten oder Einrichtungen des Auftragsverarbeiters durch, so erfolgt dies unter den folgenden Bedingungen:
   - nach vorheriger Ankündigung von mindestens zehn (10) Arbeitstagen,
   - das Audit erfolgt nur während der üblichen Geschäftszeiten und nicht mehr als einmal jährlich,
   - das Audit beschränkt sich auf die für den Verantwortlichen relevanten Daten,
   - der Verantwortliche vermeidet jede Störung des normalen Geschäftsbetriebes des Auftragsverarbeiters,
   - der Verantwortliche gewährleistet, soweit gesetzlich zulässig, die Vertraulichkeit aller gesammelten Informationen, die aufgrund ihrer Natur vertraulich sein sollten.
   - Jede Partei trägt die ihr entstandenen Kosten. Sofern die Prüfung seitens des Auftragsverarbeiters oder eines anderen Auftragsverarbeiters Aufwendungen bedeutet, die über einen Geschäftstag hinausgehen, ist der Verantwortliche damit einverstanden, jeden darüber hinausgehenden Tag zu erstatten.

f. Die Parteien stellen der/den zuständige(n) Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

5. Einsatz von Unterauftragsverarbeitern

a. Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern. Die Liste der Unterauftragsverarbeiter findet sich in Anhang III. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens vier (4) Wochen im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann. Die Liste der Unterauftragsverarbeiter findet sich in Anhang III. Die Parteien halten Anhang III jeweils auf dem neuesten Stand.

b. Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 unterliegt.

c. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten, gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

6. Internationale Datenübermittlungen

a. Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 im Einklang stehen.

b. Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener

Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

## 6. Unterstützung des Verantwortlichen

1. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
2. Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a) und b) befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.
3. Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 6 Buchstabe b) zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:
   a. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
   b. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
   c. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
   d. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679].
4. Die Parteien legen in Anhang II die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

## 7. Meldungen von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

   a. bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);
   b. bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:
      – die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
      – die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
      – die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

   Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;
   c. bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

   a. eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b. Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c. die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang II alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

## 8. Verstöße gegen die Klauseln und Beendigung des Vertrags

1. Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679– den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.
2. Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn
   a. der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
   b. der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 nicht erfüllt;
   c. der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 zum Gegenstand hat, nicht nachkommt.
3. Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.
4. Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

## I. ANHANG – BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden:
Kunden von DPDHL Kunden (Empfänger)

Kategorien personenbezogener Daten, die verarbeitet werden:

Sendungsdaten (Empfängername und Adresse)

## II. ANHANG – TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN, EINSCHLIESSLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

### 1. Kontrolle des physischen Zutrittes zu den Räumen (Zutrittskontrolle)

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

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 1. Festlegung befugter Personen (Betriebsangehörige und Betriebsfremde) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 2. Verbindlicher Prozess für die Erteilung und Übertragung von Zugangsberechtigungen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 3. Berechtigungsausweise | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 4. Schlüsselregelung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Für jedes Rechenzentrum muss eine Schließ- und Schlüsselordnung aufgestellt werden, welche die Ausgabe von Schlüsseln, Zutrittskarten und Zahlenkombinationen regelt. Sie muss auch lokale Regelungen für Ausnahmefälle (z. B. Abwesenheit des Schlüsselinhabers, Wartungsarbeiten außerhalb der Arbeitszeit oder Fehlalarm) enthalten. |
| Ja | 5. Regelung für Firmenfremde | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 6. Anwesenheitsaufzeichnungen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Um sicherzustellen, dass nur befugtem Personal der Zutritt gewährt wird, sollten Sicherheitsbereiche durch entsprechende Zugangskontrollen geschützt werden.<br>Eine Vorgehensweise zur Verwaltung der Schlüsselausgabe, der Zutrittskarten und der Zahlenkombinationen muss für jedes Rechenzentrum dokumentiert werden. Jeder Standort muss Regeln für Sonderfälle, wie beispielsweise die Abwesenheit des Schlüsselinhabers, Wartungsarbeiten außerhalb der Arbeitszeit oder Fehlalarm, definieren. |
| Ja | 7. Besucherausweise | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Besucher von Rechenzentren müssen sich selbst authentifizieren. Nach Erhalt eines Lichtbildausweises (z. B. gültiger Führerschein oder Pass) wird ihnen ein Besucherausweis ausgestellt. |
| Ja | 8. Richtlinie für die Begleitung von Besuchern | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Besucher dürfen zu keiner Zeit unbewacht bleiben. Es muss sichergestellt werden, dass alle Besucher das Rechenzentrum vor Ende des Arbeitstags verlassen und ihren Besucherausweis zurückgeben. |
| Ja | 9. Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Zum Schutz von Bereichen, in denen sich entweder vertrauliche oder betriebswichtige Informationen oder informationsverarbeitende Einrichtungen befinden, sollten Sicherheitszonen festgelegt und verwendet werden. |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 10. Sicherheitsbereiche und wenige Zugangswege schaffen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Zum Schutz von Bereichen, in denen sich entweder vertrauliche oder betriebswichtige Informationen oder informationsverarbeitende Einrichtungen befinden, sollten Sicherheitszonen festgelegt und verwendet werden.<br>IT-Systeme zur Informationsverarbeitung müssen durch physische Sicherheitsgrenzen vor unbefugtem Zutritt geschützt werden. Netzwerkkomponenten müssen in Technikräumen am Standort, in Büros oder in gesicherten Schränken installiert werden. Server müssen in standort- oder bürobezogenen Technikräumen oder in regionalen/inländischen Rechenzentren stationiert werden. |
| Ja | 11. Protokollierung des Zutritts zu Sicherheitsbereichen und beschränkten Zugangswegen (inkl. der Möglichkeit, Log-Dateien im Bedarfsfall auszuwerten) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Der physische Zugriff von Mitarbeitern von Fremdunternehmen auf Räume, welche die DPDHL-Infrastruktur enthalten (z. B. Rechenzentren und Technikräume am Standort/Firmensitz) müssen in einem Protokollbuch dokumentiert werden. Die Verwaltung dieses Protokollbuchs ist die Pflicht der verantwortlichen Geschäftsabteilung. Zu dokumentierende Elemente beinhalten das Folgende:<br>a) Name und Unternehmen<br>b) Zeit des Zugriffserhalts und des Verlassens<br>c) Arbeitsgrund<br>d) Betroffene IT-Geräte oder -Systeme<br>e) Unterschrift des externen Mitarbeiters<br>f) Dienstvorgesetzter innerhalb des DPDHL-Unternehmensbereichs |
| Ja | 12. Gesicherter Eingang für An- und Ablieferung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Punkte, über die sich nicht autorisierte Personen Zugang zu den Betriebsgebäuden verschaffen könnten, sollten kontrolliert und nach Möglichkeit von informationsverarbeitenden Einrichtungen isoliert werden, um nicht autorisierten Zugriff zu verhindern. |
| Ja | 13. Türsicherung an Notausgängen und anderen Ein- und Ausgängen (elektrischer Türschließer, Ausweisleser, Fernsehmonitor, Pförtner) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>IT-Systeme zur Informationsverarbeitung müssen durch physische Sicherheitsgrenzen vor unbefugtem Zutritt geschützt werden. Netzwerkkomponenten müssen in Technikräumen am Standort, in Büros oder in gesicherten Schränken installiert werden. Server müssen in standort- oder bürobezogenen Technikräumen oder in regionalen/inländischen Rechenzentren stationiert werden. |
| Ja | 14. Einbau von Schleusen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Zum Schutz von Bereichen, in denen sich entweder vertrauliche oder betriebswichtige Informationen oder informationsverarbeitende Einrichtungen befinden, sollten Sicherheitszonen festgelegt und verwendet werden. |
| Ja | 15. Closed-Shop-Betrieb | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Zum Schutz von Bereichen, in denen sich entweder vertrauliche oder betriebswichtige Informationen oder informationsverarbeitende Einrichtungen befinden, sollten Sicherheitszonen festgelegt und verwendet werden. |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 16. Gegenseitige Überwachung (4-Augen-Prinzip) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Datensicherung, Richtigkeit und Konsistenz sind in Bezug auf Firewalls von besonderer Bedeutung. Aktuelle Datenspeicherungen aller Software, Regelwerke und Log-Dateien müssen verfügbar sein und ihre Wiederherstellbarkeit muss getestet werden. Um ein Informationssicherheits- oder Betriebsrisiko durch den Import von Daten oder inkonsistenten, nicht aktuellen Speicherungsversionen (z. B. Regelwerke von Firewalls) zu vermeiden, müssen wirksame Verfahren für den Test hinsichtlich Konsistenz und Aktualität sowie Notfallverfahren definiert und genutzt werden.<br>Informationssicherheitskritische operative Tätigkeiten auf Firewalls müssen unter Wahrung des 4-Augen-Prinzips durchgeführt werden. |
| Ja | 17. Entsprechende Ausgestaltung der Maßnahmen zur Objektsicherung (z. B. Spezialverglasung, Einbruchmeldesystem, Absicherung von Schächten, Geländebewachung) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 18. Zusätzliche Sicherheitsmaßnahmen im Rechenzentrum (z. B. Cages oder abschließbare Racks) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |

**2. Kontrolle des Zugriffs auf Datenverarbeitungssysteme (Zugangskontrolle)**

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

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 1. Verschlüsselung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 2. Identifizierung eines Terminals und/oder eines Terminalbenutzers gegenüber dem DV-System (z. B. durch Ausweisleser) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 3. Vergabe und Sicherung von Identifizierungsschlüsseln | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 4. Zuordnung einzelner Terminals und Identifizierungsmerkmale ausschließlich für bestimmte Funktionen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 5. Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals und Identifizierungsmerkmalen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 6. Regelung der Benutzerberechtigung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 7. Verpflichtung auf das Datengeheimnis | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Bei der Einstellung und Änderung bestehender Verträge müssen Mitarbeiter verpflichtetet werden, Verschwiegenheit hinsichtlich der im Rahmen ihrer beruflichen Tätigkeit erlangten Kenntnisse zu bewahren, sowie die in der Informationssicherheits-Richtlinie zusammengefassten Vorgaben und gesetzlichen Anforderungen einzuhalten. |
| Ja | 8. Einsatz von Benutzercodes für Daten und Programme | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 9. Einsatz von Verschlüsselungsroutinen für Dateien | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 10. Differenzierte Zugriffsregelung (z. B. durch Segmentzugriffssperren) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 11. Richtlinien für die Dateiorganisation | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 12. Protokollierung und Auswertung der Dateibenutzung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 13. Besondere Kontrolle des Einsatzes von Hilfsprogrammen, soweit diese geeignet sind, die Sicherungsmaßnahmen zu umgehen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 14. Kontrollierte Vernichtung von Datenträgern | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 15. Arbeitsanweisung und Bearbeitungsverfahren für Datenerfassungsvorlagen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 16. Prüf-, Abstimm- und Kontrollsysteme | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 17. Programmprüfungs- und Freigabeverfahren | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 18. Löschung oder Sperrung von Benutzerrechten nach Vertragsende | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Allgemeine Wechsel- und Kündigungsmaßnahmen (Erweiterung zum ISO Standard)<br>Alle durchgeführten Berechtigungslöschungen müssen bei einem Ausscheiden des Mitarbeiters nachvollziehbar dokumentiert werden. |
| Ja | 19. Netzwerktrennung zur erweiterten Sicherstellung der Zugriffsmöglichkeiten | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Gruppen von Informationsdiensten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden. |
| Ja | 20. Zugriff auf das interne Netzwerk von außen nur über eine verschlüsselte VPN-Verbindung (Virtual Private Network) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Hinsichtlich sicherheitsrelevanter Aspekte müssen die folgenden Anforderungen für Telearbeitsplätze geregelt werden:<br>Verschlüsselung der Kommunikation und Nutzung von „Virtual Private Networks“ (VPN) |
| Ja | 21. Intrusion Detection System (IDS) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 22. Intrusion Prevention System (IPS) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 23. Mobile Device Management System | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 24. Schutzmaßnahmen für Log-Dateien | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 25. Protokollierung des Fernzugriffs (Möglichkeit der Analyse von Protokolldateien, falls erforderlich) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 26. Regelmäßige Prüfung der Benutzerkonten auf Gültigkeit und Deaktivierung (nach einem bestimmten Zeitraum) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Assetinhaber (Asset Owners) müssen die Zugriffsrechte aller Konten wie folgt überprüfen und ggf. anpassen:<br>a) Persönliche Konten (Personal Accounts) und nicht-persönliche Konten (Non-Personal Accounts) mindestens alle zwölf Monate,<br>b) Administratorenkonten (Administrator Accounts) und privilegierte Konten (Privilged Accounts) mindestens alle sechs Monate.<br>Assetinhaber (Asset Owners) müssen auch die Zugriffsrechte überprüfen und ggf. anpassen, wenn sich der Kontoinhaber (Account Owner) ändert, z. B. bei Beförderung, Herabstufung, Wechsel der Rolle, Funktion, Abteilung oder des Unternehmensbereichs (Corporate Division) oder bei Beendigung des Arbeitsverhältnisses. |

### 3. Kontrolle des Datenzugriffs (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.

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 1. Verschlüsselung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 2. Datenstation mit Funktionsberechtigungsschlüssel | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 3. Regelung der Zugriffsberechtigung (z. B. Nutzergruppen) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 4. Überprüfung der Berechtigung, maschinell z. B. durch Identifizierungsschlüssel | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 5. Aufzeichnung von Benutzerzugriffen (z. B. Programmausführung, Schreiben, Lesen, Löschen, Verstöße) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 6. Auswertung von Protokollen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Nicht anwendbar (keine Terminals) | 7. Ausweisleser am Terminal | Nicht relevant |
| Ja | 8. Zeitliche Begrenzung der Zugriffsmöglichkeiten | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 9. Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Nicht anwendbar (keine Daten-archivierung) | 10. Zugriffsgeschützte Archivierung von Daten | Nicht relevant |
| Ja | 11. Clear Desk/Clear Screen Policy | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Es sollte eine Clean-Desk-Richtlinie („Clean Desk Policy“) für Dokumente und mobile Speichergeräte und eine Clean-Screen-Richtlinie für informationsverarbeitende Einrichtungen erlassen werden. |
| Ja | 12. Begrenzte Anzahl von Administratorkonten | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Aus Gründen der Verfügbarkeit sollten (vorzugsweise) zwei oder mehr Administratoren für die Systemverwaltung hochkritischer Anwendungen zugewiesen werden. |
| Ja | 13. Automatische Abmeldung oder Bildschirmsperre bei Inaktivität | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Clean-Screen-Richtlinien<br>a) Bildschirmschoner sollten manuell aktiviert werden, sobald ein Benutzer seinen Arbeitsplatz vorübergehend unbeaufsichtigt lässt<br>b) Bildschirminhalte sollten nach einer angemessenen Zeit der Inaktivität automatisch ausgeblendet und Tastaturen automatisch geblockt werden |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 14. Überwachung und/oder regelmäßige Kontrolle der Aktivitäten durch Benutzer mit umfassenden Zugriffsrechten (z. B. Superuser, Administratoren) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Für Benutzerkonten mit hohen Berechtigungen müssen folgende zusätzliche Maßnahmen getroffen werden: a) Administratoren dürfen ihre Administratorenkonten nur für Administrationstätigkeiten und nicht für andere Aktivitäten verwenden (z. B. E-Mail, im Internet surfen etc.), b) Alle Administratoraktivitäten müssen protokolliert werden, c) Alle Administratorenkonten müssen einer einzelnen eindeutigen Person zugeteilt werden. Geteilte oder Gruppen-Administratorenkonten sind nicht erlaubt, d) Wenn Administratoren mithilfe eines hochberechtigten Systemkontos (z. B. Root) bestimmte Aufgaben erfüllen müssen und wenn solch eine Möglichkeit im System existiert, müssen sich Administratoren zunächst mit ihrem nicht privilegierten Konto anmelden und einen nachvollziehbaren Benutzerwechsel in das Administratorenkonto vollziehen (z. B. in UNIX „su“ und / oder „sudo“), bevor sie Aufgaben mit Administrationsrechten durchführen, e) Zugriff auf zugriffsbeschränkte und/oder vertrauliche Bereiche muss auf Datei-, Verzeichnis- oder IP-Ebene beschränkt werden, f) Aus Gründen der Verfügbarkeit sollten (vorzugsweise) zwei oder mehr Administratoren für die Systemverwaltung hochkritischer Anwendungen zugewiesen werden. Wenn nur ein Administrator für das Systemmanagement dieser Anwendungen bestimmt wurde, muss es angemessene Maßnahmen für den Wiederanlauffall geben, um das [Administrator-]Passwort auf eine sichere und kontrollierte Art und Weise wiederherzustellen. |
| Ja | 15. Trennung von Berechtigungsfreigabe und Berechtigungsvergabe (unterschiedliche Funktionen) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Schutz von externen Identitäten, Kundendaten, Mitarbeiterdaten und Daten von Geschäftspartnern (Erweiterung zum ISO Standard)<br>Identitäten und Kundendaten, Mitarbeiterdaten und Daten von Partnern sind spezielle Arten von Informationen, die einen zusätzlichen Schutz erfordern. |
| Ja | 16. Vier-Augen-Prinzip bei der Erteilung von Berechtigungen für besonders sensible Datenbestände | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 17. Konzept für die Vergabe von und das Rollenmanagement für Zugriffsberechtigungen von Benutzern (insbesondere Superuser/Administratoren) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Ein formeller Anmeldungs- und Abmeldungsprozess für Konten (Accounts) muss implementiert werden, um die Zuweisung des Kontoinhabers (Account Owner) sowie der Vergabe und Entfernung der Zugriffsrechte zu ermöglichen. |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 18. IT-Sicherheitskonzept einschließlich konkreter Vorgabe für die Rechtevergabe („need to know“, „need to have“-Prinzipien) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Ein Sicherheitskonzept muss erstellt und gepflegt werden. Bevor eine neue Dienstleistung von einem externen Dienstleister ausgewählt wird, muss ein Prozess zum Management von Informationssicherheitsrisiken durchlaufen werden.<br>Ein formeller Anmeldungs- und Abmeldungsprozess für Konten (Accounts) muss implementiert werden, um die Zuweisung des Kontoinhabers (Account Owner) sowie der Vergabe und Entfernung der Zugriffsrechte zu ermöglichen.<br>Konten müssen mit Zugriffsrechten ausgestattet sein, die für die Erfüllung ihrer Aufgaben erforderlich sind, und zwar auf der Grundlage des Prinzips der geringsten Privilegien, des Need-to-Know Prinzips und der Aufgabentrennung. |
| Ja | 19. Prozess zur Protokollierung und Benachrichtigung bei Berechtigungsänderungen (relocations) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Jede Vergabe von Kontorechten muss im IT-System identifizierbar sein und die Umstände müssen aufgezeichnet werden, sodass sie auf Nachfrage jederzeit nachvollziehbar sind. Die folgenden Angaben müssen nachvollziehbar sein: a) Vor- und Nachname des Kontoinhabers (Account Owner), b) Konto-ID (Account ID), c) Konto-ID (Account ID) der Person, die den Zugriff auf das Konto gewährt, d) funktionale Rechtfertigung, e) gewährte Zugriffsrechte. |

**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.

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 1. Verschlüsselungsstandards umgesetzt und verwendet, welche dem neuesten Stand der Technik entsprechen (bezogen auf das spezifische Risiko und das erforderliche Schutzniveau) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 2. Feststellung befugter Personen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 3. Gegenseitige Überwachung (4-Augen-Prinzip) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 4. Gesicherter RZ-Eingang für An- und Ablieferung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Anlieferungs- und Ladezonen<br>Maßnahme<br>Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Punkte, über die sich nicht autorisierte Personen Zugang zu den Betriebsgebäuden verschaffen könnten, sollten kontrolliert und nach Möglichkeit von informationsverarbeitenden Einrichtungen isoliert werden, um nicht autorisierten Zugriff zu verhindern. |
| Ja | 5. Protokollierung von Datenübertragungen (und ggf. Analyse) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| ja | 6. Schutz vor unbefugter, massiver Datenübertragung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Nicht anwendbar (keine Ausgabe von Datenträgern) | 7. Ausgabe von Datenträgern nur an autorisierte Personen (z. B. Auftragsquittung, Begleitpapier) | Nicht relevant |
| Ja | 8. Datenträger-Verwaltung | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Nicht anwendbar (keine fest montierten Plattenspeicher) | 9. Festmontierte Plattenspeicher | Nicht relevant |
| Ja | 10. Bestandskontrolle | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Nicht anwendbar (keine Ausgabe/Ausbau von Datenträgern) | 11. Gesonderter Verschluss vertraulicher Datenträger | Nicht relevant |
| Nicht anwendbar (keine Ausgabe/Ausbau von Datenträgern) | 12. Sicherheitsschränke | Nicht relevant |
| Ja | 13. Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken in die Sicherheitsbereiche | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 14. Kontrollierte Vernichtung von Datenträgern (z. B. Fehldrucke) | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 15. Regelung der Anfertigung von Kopien | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 16. Dokumentation der Abruf- und Übermittlungsprogramme | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 17. Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege (Konfiguration) | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 18. Bestimmte autorisierte Benutzer | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Nicht anwendbar (keine Ausgabe/Ausbau von Datenträgern) | 19. Verpackungs- und Versandvorschriften (Versandart z. B. in verschlossenen Behältnissen) | Nicht relevant |
| Nicht anwendbar (keine Ausgabe/Ausbau von Datenträgern) | 20. Direktabholung, Kurierdienst, Transportbegleitung | Nicht relevant |
| Ja | 21. Plausibilitätsprüfung | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 22. Vollständigkeits- und Richtigkeitsprüfung | DHL GROUP INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Nicht anwendbar (kein Austausch von phys. Datenträgern/ Cloud) | 23. Löschung von Datenresten vor Datenträgeraustausch | Nicht relevant |
| Nicht anwendbar (nur EU/EWR) | 24. Durchführung einer Datenschutz-Folgenabschätzung (DTIA) bei einer Datenübermittlung in Nicht-EU/EWR-Länder und/oder solche ohne gültigen Angemessenheitsbeschluss | Nicht relevant |
| Nicht anwendbar (nur EU/EWR) | 25. Festlegung und Prüfung von Mindestanforderungen an das Datenschutzniveau bei der Verarbeitung von Daten in Nicht-EU/EWR-Ländern und/oder solchen ohne gültigen Angemessenheitsbeschluss | Nicht relevant |

## 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.

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 1. Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Die folgenden Kontrollen müssen umgesetzt werden:<br>a) Bestehende Prüfmechanismen in Standardanwendungen sollten aktiviert werden (z. B. SAP)<br>b) Anwendung des Prinzips der doppelten Überprüfung bei kritischen Eingaben<br>c) Definition der Rollen, Verantwortlichkeiten und Prozesse als Teil des Dateneingabeprozesses<br>d) Technische Maßnahmen zur Aufdeckung von Angriffen und Alarmierung im Falle einer nicht erlaubten Eingabe auf einer Internetseite (z. B. „cross-site scripting“, „SQL-Injection“) bei kritischen IT-Anwendungen |
| Ja | 2. Protokollierung von Eingaben | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 3. Protokollierung der Dateibenutzung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 4. Verfahrens-, Programm- und Arbeitsablauforganisation | Verfahrens-, Programm- und Arbeitsablauforganisation werden gemäß interner Projektvorgehensmethoden angefertigt. |
| Ja | 5. Verpflichtung auf das Datengeheimnis | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Vertraulichkeitsvereinbarungen müssen mit den entsprechenden Rechtsvorschriften und Anforderungen für solche Vereinbarungen übereinstimmen, regelmäßig überprüft und, wann immer nötig, erneuert werden. |
| Ja | 6. Auswertung von Protokolldateien auf besondere Vorfälle | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 7. Kontrolle der Richtigkeit eingegebener Daten | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Basierend auf den Klassifizierungen der verarbeiteten Informationen und Geschäftsanforderungen müssen Maßnahmen in die Anwendungen aufgenommen werden, die die Richtigkeit bei der Verarbeitung sicherstellen, Dateneingaben validieren und Fehler, Datenverlust sowie nicht autorisierte Veränderung oder Missbrauch von Daten verhindern. |
| Ja | 8. Aufzeichnung von datenschutzrelevanten Aktivitäten der Administratoren | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 9. Beachtung des Prinzips der Datensparsamkeit durch das Prozess-Design, technische Maßnahmen oder durch die Begrenzung der Erhebung personenbezogener Daten | DHL GROUP<br>KONZERNDATENSCHUTZ RICHTLINIE<br>Die Datenverarbeitung hat sich an dem Ziel zu orientieren, nur die erforderlichen personenbezogenen Daten zu verarbeiten. Personenbezogene Daten müssen unter Berücksichtigung der Zweckbestimmung ihrer Verwendung angemessen und relevant sein und dürfen nicht über den erforderlichen Umfang hinausgehen (Datensparsamkeit). Personenbezogene Daten dürfen im Rahmen einer bestimmten Anwendung nur dann verarbeitet werden, wenn dies erforderlich ist (Datenvermeidung). |

### 6. Verpflichtung und Kontrolle von Unterauftragsverarbeitern (Sub-Prozessor-Verträge)

Der Auftragsverarbeiter muss sicherstellen, dass die im Auftrag von Dritten verarbeiteten Daten streng nach den Anweisungen des Verantwortlichen verarbeitet werden. In jedem Fall hat der Auftragsverarbeiter nach Genehmigung der Unterverarbeitung durch den Verantwortlichen Dritte rechtlich zu verpflichten, angemessene TOMs zu erfüllen, die mit den eigenen Verpflichtungen vergleichbar und mindestens gleichwertig sind.

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 1. Beauftragung von Unterauftragsverarbeitern ausschließlich unter Zugrundelegung einer Datenschutzvereinbarung gemäß Artikel 28 DSGVO | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 2. Umfassende Überprüfung der vom Unterauftragnehmer gewährleisteten TOMs vor und regelmäßig während der Auftragsverarbeitung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Nicht anwendbar | 3. Überprüfung und Bewertung des Datenschutzniveaus in Nicht-EU/EWR-Ländern (falls zutreffend) | Nicht relevant |
| Ja | 4. Aufforderung und Freigabe von Erklärungen und Garantien zur Verpflichtung aller Mitarbeiter der Unterauftragnehmer auf die Einhaltung und Gewährleistung der Vorgaben zum Datenschutz und der Datensicherheit | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 5. Prozess zur Information und Benachrichtigung des Verantwortlichen vor der Beauftragung und/oder Verarbeitung von personenbezogenen Daten durch Unterauftragnehmer | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |

### 7. Kontrolle der Verfügbarkeit und Belastbarkeit (Verfügbarkeitskontrolle)

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

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 1. Dokumentiertes Konzept zur Datensicherung und -wiederherstellung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Die Betriebshandbücher müssen die folgenden Bereiche abdecken:<br>Datensicherung (z. B. Art, Umfang, Zeitplan, Durchführungsprozedur, Wiederherstellung, Aufbewahrungsfrist, Löschkonzept) und Job Scheduling, |
| Ja | 2. Redundante Speichersysteme | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Die Sicherungsdaten müssen an einem Ort mit anderen Bedrohungsprofilen gespeichert werden als der Ort mit den Produktionsdaten. |
| Ja | 3. Getrennte Speicherung von Daten und Sicherungsdaten | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Die Sicherungsdaten müssen an einem Ort mit anderen Bedrohungsprofilen gespeichert werden als der Ort mit den Produktionsdaten. |
| Ja | 4. Schutz vor Umweltschäden (z. B. Feuer, Wasser, Überspannung) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 5. Verfügbarkeit einer unterbrechungsfreien Energieversorgung und von Notstromversorgung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 6. Verfügbarkeit eines angemessenen Sicherheitskonzepts | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Alle entwickelten, konfigurierten oder integrierten Systeme und Anwendungen, die bei DPDHL eine Funktion erfüllen, müssen eindeutige technische und fachliche Kriterien erfüllen.<br>Sicherheitsanforderungen für Informationssysteme<br>Zielsetzung: Gewährleistung, dass Informationssicherheit über den gesamten Lebenszyklus von Informationssystemen hinweg fester Bestandteil dieser Systeme ist. Dies schließt die Anforderungen für Informationssysteme ein, die Dienste über öffentliche Netze bereitstellen.<br>Analyse und Spezifikation von Sicherheitsanforderungen, Maßnahmen:<br>1. Die die Informationssicherheit betreffenden Anforderungen sollten in die Anforderungen für neue Informationssysteme oder Verbesserungen bei bestehenden Informationssystemen aufgenommen werden.<br>2. Alle Informationssicherheits-Anforderungen und -Risiken für IT-Dienste, IT-Systeme und IT-Applikationen müssen in der Anforderungsdefinitionsphase eines Projektes (vor der Entwicklung und/oder Implementierung) identifiziert, begründet, akzeptiert werden. Die Sicherheit von IT-Diensten, IT-Systemen und IT-Applikationen muss regelmäßig verifiziert werden.<br>3. Das Sicherheitskonzept muss mindestens Folgendes beinhalten (* Hinweis auf Erweiterung des generischen Risiko-Assessments und der Risikobehandlung):<br>a) Ergebnis einer initialen Risikoidentifikation (*)<br>b) Ergebnis der Sicherheitsklassifizierung (*):<br>i) Klassifizierung von Informationen und Daten<br>ii) Klassifizierung von IT-Dienstleistungen, -Systemen, -Komponenten und -Anwendungen<br>c) Identifizierte Informationssicherheits-Anforderungen (z. B. technische, regulatorische und fachliche) (*)<br>d) Ergebnis des Risiko-Assessments und der Risikobehandlung<br>i) Strukturanalyse (*)<br>ii) Identifizierung relevanter Bedrohungen (*)<br>iii) Risikoklassifizierung durch Eintrittswahrscheinlichkeit und Auswirkung<br>e) Ergebnis der Risikobehandlung<br>i) Festgelegte Informationssicherheits-Maßnahmen (*)<br>ii) Umsetzungsstatus der Informationssicherheits-Maßnahmen (*)<br>iii) Spezifizierte verbleibende Risiken<br>4. Das Sicherheitskonzept und die identifizierten verbleibenden Risiken müssen durch den/die Risikoeigentümer übernommen werden.<br>5. Das Sicherheitskonzept muss, entsprechend den verbleibenden Risiken und den im Risiko-Assessment und in der Risikobehandlung definierten Klassen, regelmäßig überprüft und während der operativen Nutzung des IT-Systems, der IT-Dienstleistung oder während ihrer Entwicklung aktuell gehalten werden. Die Auslöser einer Überprüfung und einer Anpassung eines Sicherheitskonzepts beinhalten Veränderungen in:<br>a) Regulatorischen Anforderungen<br>b) der Bedrohungs- und Risikosituation sowie dem Risiko-Assessment<br>c) der Informationssicherheits-Anforderung (Risikoakzeptanz-Kriterien).<br>6. Das Sicherheitskonzept muss einer strikten Versions- und Änderungskontrolle unterzogen werden. |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 7. Verbindlicher Prozess für und Durchführung von Updates | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Zur Gewährleistung, dass die neuesten genehmigten Patches und Anwendungs-Updates für sämtliche zugelassene Software installiert sind, sollte ein Prozess zur Softwareaktualisierung implementiert werden. Alle Änderungen sollten vollständig getestet und dokumentiert werden, sodass sie gegebenenfalls für zukünftige Softwareaktualisierungen wiederverwendet werden können. |
| Ja | 8. Kontrolle der Verfügbarkeit, Funktionsfähigkeit, Sicherheit und Nutzbarkeit der verarbeiteten Daten | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Systemabnahmeprüfung Maßnahmen:<br>1. Für neue Informationssysteme, Upgrades und neue Versionen sollten Abnahmeprüfungsprogramme und dazugehörige Kriterien festgelegt werden.<br>2. Bevor ein IT-System abgenommen wird, müssen die Anforderungen des Sicherheitskonzepts umgesetzt und das Benutzerhandbuch bereitgestellt werden. Neue IT-Systeme, Sicherheitsanforderungen, Systemaktualisierungen und Softwareversionen müssen einem formellen Test- und Freigabeverfahren unterzogen werden, bevor sie in die Produktionsumgebung eingeführt werden. Kriterien, die mindestens die folgenden Aspekte abdecken, müssen für die Abnahme definiert werden:<br>a) Anforderungen an Dienstleistungsumfang und Computerleistung<br>b) Fehlerbehandlungs- und Wiederherstellungsprozess<br>c) Vorbereitung und Test der üblichen Betriebsabläufe gemäß den definierten Vorgaben<br>d) Maßnahmen für die Aufrechterhaltung der betrieblichen Abläufe unter Berücksichtigung dieser Vorlagen<br>e) Nachweis dafür, dass die Installation des neuen IT-Systems bestehende IT-Systeme nicht zum Nachteil beeinflusst, insbesondere zu Spitzenzeiten wie bei Monatsabschlüssen<br>f) Nachweis dafür, dass das neue IT-System nicht nachteilig die übergreifende Sicherheit der DPDHL-Informationsverarbeitung beeinflusst<br>g) Einweisung für Betrieb oder Anwendung des neuen IT-Systems<br>h) Compliance mit der Richtlinie und den Vorgaben der Informationssicherheit und mit den relevanten regulatorischen Anforderungen<br>3. Die Überprüfung sollte in einer realitätsnahen Testumgebung durchgeführt werden, um sicherzustellen, dass das System keine Schwachstellen in der Betriebsumgebung der Organisation verursacht und dass die Überprüfungen zuverlässig sind. |
| Ja | 9. Kontrolle und Überprüfung von Sicherungskopien der verarbeiteten Daten | Datensicherungen Maßnahmen:<br>1. Basierend auf der Informationssicherheits-Risikobewertung müssen die Daten aller IT-Plattformen und -Technologien, die in der Produktion verwendet werden, gesichert und die Effektivität der Wiederherstellung der Sicherung (Backup) getestet werden.<br>2. Sicherungen (Backups) dürfen nur für autorisierte Zwecke verwendet werden und der Zugriff auf die Sicherungen (Backups) darf nur autorisiertem Personal gestattet werden.<br>3. Die Sicherungsdaten müssen an einem Ort mit anderen Bedrohungsprofilen gespeichert werden als der Ort mit den Produktionsdaten. |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 10. Einsatz und Verfügbarkeit von Sicherheitssystemen zum Schutz vor u. a. Cyber-Attacken (z. B. DDoS), Eindringen (z. B. Hard- und/oder Software-Firewall), Schädigung (Anti-Virus-Schutz), Erpressung (z. B. Malware-Locks) und ähnlichem | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>1. Wenn technisch machbar, muss ein Malware-Schutz mit gleicher und konsistenter Wirksamkeit in allen Systemen der DPDHL vorhanden sein, die üblicherweise anfällig für Malware-Infektionen sind, was im Allgemeinen mindestens die folgenden Systeme umfasst:<br>a) Windows OS basierte Systeme (z. B. Server, Laptop, Desktop),<br>b) Datei- und Dokumentenspeicher, z. B. Network Area Storage (NAS) oder webbasierte Anwendungen für Dokumentenmanagement und Zusammenarbeit,<br>c) Messaging-Lösungen, wie z. B. E-Mail-Dienste oder Instant Messenger,<br>d) Wechseldatenträger, wie USB-Laufwerke oder andere tragbare Speicher,<br>e) Netzwerkverkehr in Richtung Endnutzergeräte und Server (hier kann ein solcher Schutz durch Intrusion Prevention Systeme [IPS] erfolgen),<br>f) Benutzer-Internetverkehr (hier kann ein solcher Schutz durch Secure Web Gateway [SWG] alias Internet Proxy bereitgestellt werden).<br>2. Wenn mehrere Anti-Malware-Schutzschichten in einer Linie verwendet werden, müssen diese unterschiedlich gestaltet sein (von verschiedenen Herstellern stammen), um das Defense-in-Depth-Prinzip möglichst effektiv anzuwenden (z. B. unterschiedliche Anti-Malware-Lösungen für Netzwerk, IT-Anwendung, Server, Desktop usw.).<br>3. Die eingesetzte Anti-Malware-Software und deren Malware-Definitionen müssen verwaltet und unverzüglich aktualisiert werden.<br>4. Basierend auf den Ergebnissen einer Informationssicherheits-Risikobewertung müssen neben Anti-Malware-Schutzsysteme auch technische Maßnahmen zum Host- und/oder Netzwerkschutz (z. B. Intrusion Detection System [IDS], Intrusion Prevention System [IPS]) eingesetzt werden.<br>5. Anti-Malware-Protokolle der letzten 90 Tage (aktiv + Archiv) müssen zu Berichts- und Untersuchungszwecken aufbewahrt werden.<br>6. Die automatische Ausführung von Makros aus nicht vertrauenswürdigen Quellen durch Desktop-Anwendungen (z. B. MS Office) muss deaktiviert werden.<br>7. Alle IT-Systeme, einschließlich, aber nicht beschränkt auf Endnutzergeräte, ohne angemessenen Malware-Schutz (z. B. veraltete Signaturdateien) müssen in einem eigenen Netzwerksegment isoliert werden.<br>8. Für IT-Systeme müssen Indikatoren für eine Kompromittierung definiert werden und es müssen regelmäßige Scans zur Analyse aller Indikatoren durchgeführt werden.<br>9. Alle eingehenden elektronischen Nachrichten (z. B. E-Mails, Chat-Nachrichten) aus dem Internet oder anderen Quellen außerhalb von DPDHL müssen vor der Zustellung an den vorgesehenen Empfänger auf Malware gescannt werden.<br>10. Basierend auf der Informationssicherheits-Risikobewertung und der technischen Machbarkeit müssen andere elektronische Nachrichten vor der Zustellung an den vorgesehenen Empfänger auf Malware gescannt werden.<br>11. Die Wirksamkeit der Anti-Malware-Maßnahmen muss regelmäßig gemessen und berichtet werden (z. B. Bereitstellung der Wartung der Anti-Malware-Schutzsysteme für Signaturen, Software-Updates und Patches, insbesondere Versions- und Signatur-Status). |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 11. Regelmäßige Wartung von IT-Systemen (Hard- und/oder Software) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Schutzmechanismen zu Informationsverlust sollten regelmäßig aktualisiert und kontinuierlich weiterentwickelt werden, um sicherzustellen, dass ihre Konfigurationen (z. B. Regeln) den sensiblen Daten, die geschützt werden sollen, entsprechen |
| Ja | 12. Konzeption und Umsetzung eines angemessenen und dem Stand der Technik entsprechenden Konzeptes zur unterbrechungsfreien Funktion (Hard- und/oder Software) | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Die Betriebshandbücher müssen die folgenden Bereiche abdecken:<br>a) Sicherheitskonfigurationen (z. B. Systemhärtungs-Basiskonfiguration),<br>b) Patch-Verwaltung,<br>c) Datensicherung (z. B. Art, Umfang, Zeitplan, Durchführungsprozedur, Wiederherstellung, Aufbewahrungsfrist, Löschkonzept) und Job Scheduling,<br>d) Unterweisung im Umgang mit Informationsmedien (z. B. Verwendung von speziellem Briefpapier, Umgang mit streng vertraulichen Ausgaben einschließlich Verfahren zur sicheren Entsorgung von Ausgaben aus fehlgeschlagenen Aufträgen),<br>e) Störungsmanagement (z. B. Notfall-, Alternativ- und Wiederanlaufpläne sowie Support- und Eskalationskontakte). |

**8. Zweckbindungskontrolle**

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

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 1. Mandantentrennung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Anforderungen zur Informationssicherheit bezüglich technischer Architektur müssen geregelt werden, um die erforderlichen Verfügbarkeiten zu garantieren; es muss sichergestellt werden, dass eine wirksame Trennung von Datenverarbeitung und Datenspeicherung verschiedener Kunden gegeben ist und auch eine separate mandantenorientierte Datenspeicherung durch den Anbieter vorliegt. |
| Ja | 2. Funktionstrennungen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Anforderungen zur Informationssicherheit bezüglich technischer Architektur müssen geregelt werden, um die erforderlichen Verfügbarkeiten zu garantieren; es muss sichergestellt werden, dass eine wirksame Trennung von Datenverarbeitung und Datenspeicherung verschiedener Kunden gegeben ist und auch eine separate mandantenorientierte Datenspeicherung durch den Anbieter vorliegt. |
| ja | 3. Datenbanktrennung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Anforderungen zur Informationssicherheit bezüglich technischer Architektur müssen geregelt werden, um die erforderlichen Verfügbarkeiten zu garantieren; es muss sichergestellt werden, dass eine wirksame Trennung von Datenverarbeitung und Datenspeicherung verschiedener Kunden gegeben ist und auch eine separate mandantenorientierte Datenspeicherung durch den Anbieter vorliegt. |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| ja | 4. Konzept zur Clientnutzung / Einschränkung der Nutzung | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Schutz von externen Identitäten, Kundendaten, Mitarbeiterdaten und Daten von Geschäftspartnern (Erweiterung zum ISO Standard)<br>Identitäten und Kundendaten, Mitarbeiterdaten und Daten von Partnern sind spezielle Arten von Informationen, die einen zusätzlichen Schutz erfordern. |
| Ja | 5. Verfahren zur Speicherung, Änderung, Löschung, Übermittlung von Daten für unterschiedliche Zwecke | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Schutz von externen Identitäten, Kundendaten, Mitarbeiterdaten und Daten von Geschäftspartnern (Erweiterung zum ISO Standard)<br>Identitäten und Kundendaten, Mitarbeiterdaten und Daten von Partnern sind spezielle Arten von Informationen, die einen zusätzlichen Schutz erfordern. |

**9. Prozess zur regelmäßigen Prüfung, Bewertung und Beurteilung von Datenschutzmaßnahmen ( Datenschutz-Management-System)**

Maßnahmen, mit denen die Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen langfristig sichergestellt wird, einschließlich aller Maßnahmen zur Sicherstellung einer strukturierten Datenschutzorganisation, abgesichert durch ein angemessenes Datenschutzmanagementsystem. Dazu sind mindestens Organisationsstrukturen (z. B. Rollen und Verantwortlichkeiten), organisatorische Maßnahmen des Ablaufs (z. B. Prozesse und Verfahren) sowie dokumentierte Richtlinien einschließlich zugehöriger Definitionen der Prozesse erforderlich.

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 1. Datenschutz-Management-System verfügbar und umgesetzt | DPDHL PRIVACY PORTAL<br>Das Privacy Portal basiert auf der Software „One Trust“. Mit dem Privacy Portal werden datenschutzrechtliche Prüfungen von IT-Systemen und Datenschutzorganisationsaudits durchgeführt und das Verzeichnis von Verarbeitungstätigkeiten geführt. |
| Ja | 2. Datenschutzbeauftragter und IT-Sicherheitsbeauftragter benannt und in die Strukturen des Auftragsverarbeiters eingebunden | DHL GROUP<br>KONZERNDATENSCHUTZ RICHTLINIE<br>Für jedes Konzernunternehmen ist ein unabhängiger Datenschutzansprechpartner (Datenschutzbeauftragter Datenschutzkoordinator) zu benennen. Der Datenschutzansprechpartner ist für die Umsetzung von Standards zuständig und wirkt auf die Beachtung der relevanten Vorschriften hin. |
| Ja | 3. Unabhängigkeit des Datenschutzbeauftragten bei der Erteilung von Weisungen im Rahmen der Ausübung seiner Aufgaben ist gewährleistet | DHL GROUP<br>KONZERNDATENSCHUTZ RICHTLINIE<br>Für jedes Konzernunternehmen ist ein unabhängiger Datenschutzansprechpartner (Datenschutzbeauftragter/ Datenschutzkoordinator) zu benennen. Der Datenschutzansprechpartner ist für die Umsetzung von Standards zuständig und wirkt auf die Beachtung der relevanten Vorschriften hin. |
| Ja | 4. Regelmäßige Kontrolle, Prüfung und Optimierung der getroffenen technischen und organisatorischen Maßnahmen | DHL GROUP<br>KONZERNDATENSCHUTZ RICHTLINIE<br>Bereitstellung eines Prozesses zur regelmäßigen Prüfung, Bewertung und Bewertung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 5. Unverzügliche Benachrichtigung des Verantwortlichen bei Sicherheitsvorfällen und/oder Datenpannen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Falls Informationen als personenbezogene Daten oder personenbezogene Daten besonderer Art gekennzeichnet werden: Die Rechtmäßigkeit des Austauschs/der Übermittlung solcher Informationen oder Daten muss mit dem Datenschutzbeauftragten abgestimmt werden.<br>Jeder Verlust der Daten oder ein Kenntniserlangen unbefugter Dritter muss unverzüglich als Informationssicherheits-Vorfall gemeldet werden. |
| Ja | 6. Auswertung von Hinweisen und Meldungen zu ungewöhnlichen Ereignissen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 7. Regelmäßige fachliche Schulung der IT-Verantwortlichen und des Datenschutzbeauftragten | DHL GROUP<br>KONZERNDATENSCHUTZ RICHTLINIE<br>Die Beschäftigten von Konzernunternehmen sind im Datenschutz und bezüglich der Anwendung der Konzerndatenschutzrichtlinie in angemessener Weise zu schulen.<br>----------<br>DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Alle Mitarbeiter müssen über die Existenz, die Verbindlichkeit und den Inhalt der Informationssicherheits-Richtlinie und jeder zusätzlichen Richtlinie informiert werden. Ferner müssen die Mitarbeiter für Informationssicherheit und Datenschutz bei DPDHL sensibilisiert, ausreichend informiert und gegebenenfalls eingewiesen werden. |
| Ja | 8. Schulung der Mitarbeiter zu Themen des Datenschutzes und der Informationssicherheit | DHL GROUP<br>KONZERNDATENSCHUTZ RICHTLINIE<br>Die Beschäftigten von Konzernunternehmen sind im Datenschutz und bezüglich der Anwendung der Konzerndatenschutzrichtlinie in angemessener Weise zu schulen. |
| Ja | 9. Einrichtung eines Vorfallsmanagement- und Meldeprozesses | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE |
| Ja | 10. Prozess zur Feststellung und Meldung von Sicherheitsvorfällen und/oder Datenverletzungen dokumentiert | DHL GROUP<br>KONZERNDATENSCHUTZ RICHTLINIE<br>Wird ein Informationssicherheits-Vorfall erkannt oder besteht der Verdacht, dass ein solcher vorliegt, so muss jedem Mitarbeiter klar sein, dass DPDHL erwartet, dass der zuständige „User Help Desk“ sofort informiert oder eine andere Schnittstelle für die Meldung genutzt wird. |
| Ja | 11. Aufzeichnung und Untersuchung von Sicherheitsvorfällen und/oder Datenschutzverletzungen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Management von Informationssicherheitsvorfällen und Verbesserungen:<br>1. Jeder Verlust der Daten oder Kenntniserlangung durch unbefugte Dritte muss als Informationssicherheits-Vorfall gemeldet werden und, falls personenbezogene Daten betroffen sind, auch unverzüglich als eine Datenschutzverletzung.<br>2. Durch organisatorische Maßnahmen oder Prozesse einschließlich des Berichtswesens muss die rechtzeitige Verarbeitung von Schwachstellen sichergestellt werden. Alle Sicherheitslücken (einschließlich bereits beseitigter) müssen dem Informationssicherheits-Management berichtet werden.<br>Bewertung von und Entscheidung über Informationssicherheitsereignisse, Maßnahmen:<br>Informationssicherheitsereignisse sollten bewertet werden, und es sollte darüber entschieden werden, ob sie als Informationssicherheitsvorfälle einzustufen sind. |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 12. Festlegung, Dokumentation und Gewährleistung von verbindlichen Datenschutz- und Informationssicherheitsrichtlinien | DHL GROUP<br>KONZERNDATENSCHUTZ<br>RICHTLINIE<br>Die DHL Group Konzerndatenschutzrichtlinie1 gilt für die Verarbeitung personenbezogener Daten natürlicher Personen, insbesondere der Daten von Kunden, Beschäftigten, Aktionären und Geschäftspartnern. Ziel ist die Schaffung eines angemessenen Datenschutzstandards für die Übermittlung personenbezogener Daten von Konzernunternehmen aus der Europäischen Union (EU) an Konzernunternehmen in Drittländern ohne ein angemessenes Datenschutzniveau. |
| ja | 13. Durchführung von Audits bei Unterauftragnehmern im Hinblick auf die Anforderungen im Bereich des Datenschutzes und der Informationssicherheit | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>In der Regel durch externe Audits oder Zertifizierungen, z. B. ISO<br>Überwachung und Prüfung von Lieferantendienstleistungen, Maßnahmen:<br>Organisationen sollten die Dienstleistungserbringung durch Lieferanten regelmäßig überwachen, prüfen und auditieren.<br>Die von Dritten erbrachten Dienstleistungen, Berichte und Aufzeichnungen müssen regelmäßig überwacht und überprüft werden und Compliance-Assessments sollten regelmäßig durchgeführt werden. |
| Ja | 14. Schutz vor Übertragung und Verwendung von Echtdaten an/in Test- oder Entwicklungssystemen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Schutz von Testdaten, Maßnahmen:<br>1. Testdaten sollten gewissenhaft ausgewählt, geschützt und kontrolliert werden. Funktionale und betriebliche Abnahmetests erfordern normalerweise umfangreiche Mengen von Daten, die den betrieblichen Daten so ähnlich wie möglich sein müssen.<br>2. Die Nutzung von operativen Daten, die persönliche Informationen enthalten, und die Nutzung von Echtdaten zum Test ist grundsätzlich nicht erlaubt. Wo die Nutzung von Echtdaten nicht vermieden werden kann, sollten die folgenden Maßnahmen angewendet werden, um Daten für den Testzweck zu schützen:<br>a) Alle Sicherheitskontrollen, die für betriebliche Daten gelten, müssen in gleicher Weise für die Daten im Test angewendet werden<br>b) Die Zugriffskontrollverfahren, die für betriebliche Anwendungssysteme gelten, müssen in gleicher Weise für Anwendungssysteme im Test angewendet werden<br>c) Sofern nicht vermeidbar, sollte das Kopieren und die Nutzung von Echtdaten durch zusätzliche spezielle Nutzerkonten ausgeführt und zudem protokolliert werden, damit ein Prüfnachweis (Audit Trail) bereitgehalten werden kann<br>d) In dem Ausnahmefall, dass Echtdaten verwendet werden müssen, müssen diese vorher anonymisiert oder pseudonymisiert werden<br>e) Es muss sichergestellt werden, dass Anonymisierung oder Pseudonymisierung ausreichend ist und keine Bedrohung durch Datenverrat („Data Leakage“) vorhanden ist, z. B. wenn externe IT-Dienstleister involviert sind<br>f) Informationen von IT-Systemen im regulären Betrieb [(sog. Echtdaten)] müssen von der Testumgebung gelöscht werden, sobald der Test abgeschlossen ist |

| Implementiert? | Maßnahme | Kommentar |
|---|---|---|
| Ja | 15. Kontrolle und Anpassung von Datenschutz- und Informationssicherheitsvorgaben auf der Grundlage aktueller gesetzlicher Regelungen | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Einhaltung gesetzlicher und vertraglicher Anforderungen<br>Zielsetzung: Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen im Zusammenhang mit Informationssicherheit sowie gegen jegliche Sicherheitsanforderungen.<br>Feststellung anwendbarer Gesetze und vertraglicher Anforderungen, Maßnahmen:<br>1. Alle relevanten gesetzlichen, regulatorischen und vertraglichen Vorschriften sowie die Vorgehensweise der Organisation zur Erfüllung dieser Vorschriften sollten für jedes Informationssystem und die Organisation explizit definiert, dokumentiert und ständig aktualisiert werden.<br>2. In Abhängigkeit vom Geschäftszweck muss der verantwortliche Unternehmensbereich gesetzliche Verpflichtungen, Richtlinien und weitere Auflagen systematisch definieren sowie Vorschriften ableiten, Maßnahmen definieren und diese beispielsweise als Teil des Sicherheitskonzepts und bei Vertragsverhandlungen mit IT-Dienstleistern umsetzen. Die Identifikation anwendbarer Gesetzgebung ist die grundlegende Voraussetzung für IT-Compliance. Eine regelmäßige Überwachung muss durch die Definition und Umsetzung geeigneter technischer und organisatorischer Maßnahmen gewährleistet werden. |
| Ja | 16. Einhaltung der Prinzipien von „Privacy by Design“ und „Privacy by Default“ | DHL GROUP<br>INFORMATION SECURITY DEFAULT IMPLEMENTATION GUIDELINE<br>Personenbezogene Daten und Informationen müssen im Einklang mit den lokalen Datenschutzgesetzen und der Konzern-Datenschutzrichtlinie unter Kontrolle gehalten werden. Die Grundsätze des Datenschutzes durch Technikgestaltung („Privacy by Design“) und des Datenschutzes durch datenschutzfreundliche Voreinstellungen („Privacy by Default“) müssen angewendet werden. |
| Ja | 17. Erstellung und Aktualisierung eines Registers mit Verarbeitungstätigkeiten nach Art. 30 DSGVO | DHL GROUP<br>KONZERNDATENSCHUTZ RICHTLINIE<br>Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person Informationen über die Verarbeitung in prägnanter, transparenter, verständlicher und leicht zugänglicher Form zur Verfügung zu stellen. Die Informationen sind schriftlich oder gegebenenfalls mit anderen Mitteln vorzulegen |

## III. ANHANG – LISTE DER UNTERAUFTRAGSVERARBEITER

**(Unter-)Auftragsverarbeiter**

| Gesellschaft | Adresse | Service Beschreibung / Dauer der Verarbeitung |
|---|---|---|
| Micromata GmbH | Marie-Calm-Straße 1-5, 34131 Kassel | Betrieb System Rapide Postbuch |
| Materna SE | Voßkuhle 37, 44141 Dortmund | Wartung und Betrieb System GK-Portal |
| T-Systems International GmbH | Hahnstraße 43d, 60528 Frankfurt am Main | Betrieb Cloud-Infrastruktur |

**Rechenzentrum / Rechenzentren des Auftragsverarbeiters und / oder Unter-Auftragsverarbeiters):**

| Gesellschaft | Land | Adresse |
|---|---|---|
| Microsoft | Niederlande | Agriport 601<br>1775 TK Middenmeer<br>Netherlands |