Deutsche Post DHL Group

DEUTSCHE POST DHL GROUP

VERHALTENSKODEX ZUR INFORMATIONSSICHERHEIT FÜR PARTNER

Dokumenteneigentümer: DPDHL Group CISO

Version: 3.0

Veröffentlichungsdatum: Januar 2022

Inhaltsverzeichnis

HINWEIS: Die englische Fassung des ISCOP enthält die rechtsverbindlichen Bestimmungen, an die sich alle Parteien zu halten haben. Jegliche Übersetzung des ISCOP dient lediglich zu Referenzzwecken. Im Falle eines Widerspruchs zwischen der englischen Fassung und einer anderen Übersetzung ist die englische Fassung des ISCOP maßgebend

Teil 1: DPDHL Group: Einführung in die Sicherheitsanforderungen

1) DPDHL Group verwendet, erstellt und speichert im Rahmen ihrer Geschäftstätigkeit eine erhebliche Menge an Daten und muss sicherstellen, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten geschützt werden. DPDHL Group erwartet und verlangt von allen Lieferanten von DPDHL Group, dass sie angemessene und wirksame Schutzmaßnahmen und Kontrollen umsetzen und aufrechterhalten, um die Sicherheit der DPDHL-Systeme und -Informationen zu gewährleisten.

2) Die im Verhaltenskodex zur Informationssicherheit (englisch: Information Security Code of Practice – ISCOP) verwendeten Begriffe haben die ihnen in den Begriffsbestimmungen in Teil 4 des ISCOP zugewiesene Bedeutung, sofern sich aus dem Kontext heraus nicht etwas anderes ergibt. Wenn der ISCOP Teil einer Vereinbarung zwischen dem Lieferanten und einem Mitglied von DPDHL Group ist, haben die im ISCOP enthaltenen Begriffsbestimmungen Vorrang vor etwaigen widersprüchlichen Begriffsbestimmungen im übrigen Teil einer solchen Vereinbarung, jedoch nur in Bezug auf die Auslegung des ISCOP.

3) Teil 2 des ISCOP enthält verbindliche Mindestsicherheitsanforderungen, deren Einhaltung DPDHL Group vom Lieferanten erwartet. Ist der Lieferant nicht in der Lage, diese Mindestsicherheitsanforderungen einzuhalten, kann er keinen Vertrag mit DPDHL Group schließen.

4) Teil 3 des ISCOP legt die erweiterten Kontrollmechanismen dar, die alle Lieferanten einhalten sollten. Außerdem muss der Lieferant die in Teil 3 des ISCOP dargelegten erweiterten Kontrollmechanismen einhalten, wenn mindestens eines der folgenden Kriterien erfüllt ist:
   a) der Lieferant verarbeitet DPDHL-Daten über Systeme des Lieferanten außerhalb der Räumlichkeiten von DPDHL Group; und/oder
   b) der Lieferant verfügt über einen Zugriff auf DPDHL-Systeme, unabhängig davon, ob es sich um einen Fernzugriff oder eine andere Art Zugriff handelt.

5) Wenn der Lieferant im Auftrag von DPDHL Group personenbezogene Daten verarbeitet und/oder der Lieferant personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums verarbeitet, werden zusätzliche datenschutzrechtliche Anforderungen in die entsprechende Vereinbarung zwischen dem Lieferanten und dem betreffenden Mitglied von DPDHL Group aufgenommen. Soweit sich diese zusätzlichen Maßnahmen mit den Anforderungen des ISCOP überschneiden oder im Widerspruch stehen, gelten für den Lieferanten die strengeren der beiden Anforderungen.

Teil 2: Obligatorische Mindestsicherheitsanforderungen

1) Zusätzlich zu den unten aufgeführten obligatorischen Mindestsicherheitsanforderungen sollte der Lieferant die Informationssicherheit in Übereinstimmung mit den in ISO 27001 beschriebenen Praktiken sicherstellen.

2) Fällt ein Teil der Dienstleistungen nicht in den Geltungsbereich einer aktuellen Zertifizierung nach ISO 27001, sollte der Lieferant jederzeit und auf Anfrage nachweisen können, dass er Kontrollen umgesetzt hat, die den branchenüblichen Kontrollen, beispielsweise ISO/IEC 27002:2013, entsprechen.

3) DPDHL Group kann nach eigenem Ermessen die Einhaltung der Informationssicherheitsanforderungen im Zusammenhang mit der Erbringung von Dienstleistungen durch den Lieferanten überprüfen. Die Einzelheiten dieses Auditrechts durch DPDHL Group sind nachstehend dargelegt.

4) Der Lieferant muss die folgenden verpflichtenden Mindestsicherheitsanforderungen einhalten.

Tabelle A – Mindestsicherheitsanforderungen

Anforderung	Erwartung
Allgemeines	
Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit	Der Lieferant ist für die Wahrung der Integrität der DPDHL-Daten und die Verhinderung der Beschädigung oder des Verlusts von DPDHL-Daten verantwortlich und stellt dabei sicher, dass er (auch bei seinen Beratern, Auftragnehmern oder Unterauftragnehmern) geeignete Kontrollen zum Schutz vor unbefugter und/oder unrechtmäßiger Nutzung von DPDHL-Daten eingerichtet hat.
Systemsicherheit	Der Lieferant stellt sicher, dass jedes System, auf dem er DPDHL-Daten, einschließlich Sicherungsdaten, speichert, ein sicheres System ist, das Teil 3 des ISCOP entspricht, und ermöglicht insbesondere dem Personal des Lieferanten den Zugriff auf DPDHL-Daten in elektronischer Form nur in dem für die Erbringung der Dienstleistungen erforderlichen Umfang.
Anforderung	**Erwartung**
Schutz von Informationen und Cybersicherheit	
Schutz von Informationen	Der Lieferant muss DPDHL-Daten während ihres gesamten Lebenszyklus schützen und ein Inventar der DPDHL-Daten im Besitz des Lieferanten (und auch im Besitz von Unterauftragnehmern) führen. Der Lieferant muss DPDHL Group nachweisen, dass Kontrollen zum Schutz von und zum Umgang mit DPDHL-Daten gemäß ihrer Klassifizierung vorhanden sind.
Informationssicherheitstests	Wenn der Lieferant eine Website oder eine von externen Benutzern verwendete Anwendung hostet, die DPDHL-Daten speichert, verarbeitet oder übermittelt oder Marken von DPDHL Group anzeigt, oder wenn ein DPDHL interner Netzwerkbereich (z.B. IP-Adressraum) auf das Netzwerk des Lieferanten ausgedehnt wird, gelten die folgenden Anforderungen. Soweit der Lieferant der Einhaltung von Anforderungen von DPDHL Group, die sich mit den nachstehenden Anforderungen überschneiden oder damit im Widerspruch stehen, zugestimmt hat, gelten für den Lieferanten die strengeren der beiden Anforderungen: 1) Sicherheitstests, einschließlich Penetrationstests, sind vor der Veröffentlichung der Seiten im Internet von qualifizierten unabhängigen Dienstleistern, die von einer branchenweit anerkannten Sicherheitsteststelle akkreditiert sind, durchzuführen; 2) es besteht ein Zeitplan für regelmäßige, mindestens einmal jährlich durchzuführende Sicherheitstests der Website. Die Zeiten und Termine für die Sicherheitstests sind einvernehmlich zwischen den beiden Vertragsparteien zu vereinbaren; 3) DPDHL Group wird eine Zusammenfassung der Ergebnisse der Penetrationstests sowie eine Liste der Abhilfemaßnahmen für jede Feststellung für Maßnahmen mit Umsetzungsfrist bereitgestellt; und

Anforderung	Erwartung
	4) die Fortschritte von Abhilfemaßnahmen werden DPDHL Group monatlich mitgeteilt.
Anforderung	**Erwartung**
Handhabung von Informationssicherheitsvorfällen	
Maßnahmenplan	Der Lieferant führt einen schriftlichen Maßnahmenplan über Informationssicherheitsvorfälle und stellt DPDHL Group auf Anfrage eine Kopie dieses Plans zur Verfügung. Der Lieferant behebt jeden Informationssicherheitsvorfall zeitnah gemäß seinem Maßnahmenplan für Informationssicherheitsvorfälle in Übereinstimmung mit bewährten Branchenpraktiken („Good Industry Practices“).
Meldepflichten	Der Lieferant ist verpflichtet, DPDHL Group innerhalb von 48 Stunden nach Bekanntwerden eines Informationssicherheitsvorfalls zu benachrichtigen, der DPDHL-Daten oder DPDHL-Systeme betrifft, die vom Lieferanten verarbeitet und/oder betrieben werden oder mit denen über den Lieferanten eine Schnittstelle besteht. Der Lieferant unternimmt angemessene Bemühungen, um einen vollständigen Bericht über den Informationssicherheitsvorfall und die damit verbundenen Maßnahmen zu erstellen und um sicherzustellen, dass er alle verlorenen oder vernichteten Informationen ohne Kosten für DPDHL Group wiederherstellt. Im Falle eines Informationssicherheitsvorfalls oder einer Verletzung des Schutzes personenbezogener Daten (wie im Datenschutzrecht definiert), die DPDHL-Daten betreffen, hat der Lieferant dies an supplier-cybersecurity@dpdhl.com und an den von DPDHL Group definierten Geschäftskontakt zu melden.
Zusammenarbeit mit DPDHL Group bei der Untersuchung von Informationssicherheitsvorfällen	Der Lieferant kooperiert in angemessener Weise mit DPDHL Group bei der Untersuchung von Informationssicherheitsvorfällen, insbesondere in Bezug auf die folgenden Punkte: 1) Abstimmung mit DPDHL Group in Bezug auf den Maßnahmenplan des Lieferanten; 2) Unterstützung der DPDHL Group bei der Untersuchung eines Informationssicherheitsvorfalls; 3) Ermöglichung von Gesprächen mit dem Lieferantenpersonal und anderen Personen, die in den Informationssicherheitsvorfall oder den damit verbundenen Maßnahmen involviert sind; und 4) Bereitstellung aller relevanten Aufzeichnungen, Protokolle, Dateien, Datenberichte, forensischen Berichte, Untersuchungsberichte und anderen Materialien, die DPDHL Group benötigt, um geltende Gesetze, Vorschriften oder Branchenstandards einzuhalten, oder die von DPDHL Group anderweitig verlangt werden.
Benachrichtigungen Dritter	Der Lieferant verpflichtet sich, Dritte (einschließlich Aufsichtsbehörden oder Kunden) nicht ohne die vorherige schriftliche Zustimmung von DPDHL Group über einen

Anforderung	Erwartung
	Informationssicherheitsvorfall zu informieren, es sei denn, dies verstößt gegen bestehende Gesetze oder Vorschriften. Ferner erklärt sich der Lieferant damit einverstanden, dass DPDHL Group das alleinige Recht hat 1) zu bestimmen, ob die Meldung des Informationssicherheits-vorfalls an einzelne Personen, Aufsichtsbehörden, Strafverfolgungsbehörden oder andere Stellen erfolgen soll; und 2) die Form und den Inhalt einer solchen Meldung festzulegen.
Anforderung	**Erwartung**
Anforderungen an den Lieferanten gemäß Datenschutzrecht	
Einhaltung gesetzlicher Vorschriften	1) Der Lieferant hält sich an die geltenden Datenschutzgesetze, einschließlich der Bestimmungen über die Sicherheit personenbezogener Daten, sowie die einschlägigen Vorschriften, wie die DSGVO; 2) Der Lieferant hält alle genannten Anforderungen ein, wenn personenbezogene Daten, insbesondere solche von Kunden, Verbrauchern, Mitarbeitern und Aktionären, erhoben, gespeichert, gehostet, verarbeitet, übermittelt, verwendet und/oder gelöscht werden; und 3) Der Lieferant hält sämtliche vertraglichen Anforderungen zu Datenschutz und Informationssicherheit ein und legt keine Informationen offen, die der Öffentlichkeit nicht bekannt sind.

5) Wenn der Lieferant Zugriff auf interne Informationen und Systeme von DPDHL Group benötigt, gilt Folgendes:

Tabelle B – Bedingungen für den Zugriff von Lieferanten auf interne Informationen von DPDHL Group sowie auf DPDHL-Systeme

Anforderung	Erwartung
Zugriff nach dem Need-to-Know-Grundsatz (Kenntnis nur, wenn nötig)	Der Zugang zu DPDHL-Daten wird einem Lieferanten nur gestattet, wenn er diese Daten kennen muss und wenn die Offenlegung von einem Vertreter von DPDHL Group ausdrücklich genehmigt wurde.
Berechtigte und dokumentierte Geschäftsanforderung	Der Zugriff auf DPDHL-Systeme wird einem Lieferanten nur gewährt, wenn dieser Lieferant nach Meinung des zuständigen DPDHL-Systemmanagers eine berechtigte und dokumentierte Geschäftsanforderung für diesen Zugriff hat und die Systeme des Lieferanten keine ernstzunehmende Bedrohung für einen beliebigen Teil der Infrastruktur von DPDHL Group darstellen. Der Zugriff des Lieferanten darf nur bestimmten Personen gewährt werden und auch nur für den Zeitraum, der zur Erledigung genehmigter Aufgaben notwendig ist.
Befolgung der DPDHL Group Onboarding-Verfahren für den Netzwerkzugriff	Der Lieferant hat die Onboarding-Verfahren für den Zugriff auf das DPDHL-System einzuhalten, um Zugriff auf DPDHL-Systeme zu erhalten. Zu diesen Verfahren gehört die Bereitstellung der erforderlichen Informationen als Teil der Netzwerkkonfigurationen, insbesondere IP-Adressen, Netzwerkprotokoll und Implementierungsmethode für den Netzwerkzugang (z. B. VPN-Einrichtung).
Nachweis über ein Information Security Management System (ISMS)	Bevor einem Lieferanten eine Benutzerkennung („Account-ID“) ausgestellt werden kann, ist dem Management von DPDHL ein schriftlicher Nachweis über das Vorhandensein eines Information Security Management Systems oder -prozesses vorzulegen und vom Management von DPDHL Group zu genehmigen. Zudem muss sich der Lieferant schriftlich dazu bereit erklären, den unbefugten Zugriff auf die ihm zur Verfügung gestellten DPDHL-Systeme und deren missbräuchliche Nutzung zu verhindern.
Sofortige Trennung der Netzwerkverbindung	DPDHL Group behält sich außerdem das Recht vor, Netzwerkverbindungen mit allen Systemen des Lieferanten sofort zu trennen, wenn DPDHL Group der Meinung ist, dass der Lieferant diese Anforderungen nicht erfüllt oder wenn der Lieferant eine Möglichkeit für einen Angriff auf die DPDHL-Systeme bietet.
Dokumentierte Sicherheitsarchitektur	Der Lieferant ist zur Pflege der dokumentierten Sicherheitsarchitektur, der von ihm für die Erbringung der Dienstleistungen an DPDHL Group betriebenen Netzwerke, verpflichtet. Der Lieferant überprüft regelmäßig (d. h. mindestens einmal im Jahr) die Netzwerkarchitektur, einschließlich der Maßnahmen zur Verhinderung unbefugter Netzwerkverbindungen zu allen Systemen, Anwendungen und Netzwerkgeräten.
Trennung von DPDHL-Systemen und den Systemen und der Infrastruktur des Lieferanten	Die DPDHL-Systeme sind von den internen Systemen und der Infrastruktur des Lieferanten strikt zu trennen.

Anforderung	Erwartung
Datenprotokollierung	Der Lieferant ist verpflichtet, alle Protokollierungsdaten, die sich auf DPDHL Group beziehen (als Beleg/Nachweis für Handlungen), zu erheben und hat diese Daten DPDHL Group unaufgefordert vorzulegen oder DPDHL Group den ständigen Zugang zu diesen Daten zu ermöglichen.

6) DPDHL Group hat die folgenden Auditrechte gegenüber dem Lieferanten. Soweit der Lieferant DPDHL Group Auditrechte eingeräumt hat, die sich mit den nachstehenden Rechten überschneiden oder damit im Widerspruch stehen, kann DPDHL Group die jeweils umfassenderen Auditrechte ausüben:

Tabelle C – Auditrecht für DPDHL Group

Anforderung	Erwartung
Auditzugriff	Die vom Lieferanten erbrachten Dienstleistungen und bereitgestellten IT-Systeme unterliegen Audits durch DPDHL Group (oder durch von DPDHL Group beauftragte externe Auditoren), die mit schriftlicher Mitteilung mit einer angemessenen Frist anzukündigen sind (insbesondere bei vom Lieferanten abgeschlossenen Datenverarbeitungsverträgen, die dem Datenschutzrecht entsprechen).
Auditfeststellungen	Der Lieferant hat sämtliche im Rahmen des Audits identifizierte Feststellungen innerhalb einer gemeinsam vereinbarten Frist zu beheben und DPDHL Group Nachweise über die erfolgreiche Behebung vorzulegen.
Compliance-Nachweis	Auf Verlangen von DPDHL Group (nicht häufiger als einmal alle zwölf Monate) muss der Lieferant einen Nachweis der Konformität der erbrachten Dienstleistungen und IT-Systeme in Form einer unabhängigen Prüfung durch externe Auditoren oder branchenweit anerkannter Sicherheitsstandards zu erbringen. Der Nachweis muss Folgendes umfassen: 1) eine Kopie seiner jährlichen Zertifizierung gemäß ISO 27001 und/oder von SSAE SOC2- oder gleichwertigen Berichten und 2) eine Kopie der Berichte über die Bewertung von Schwachstellen und/oder zu Penetrationstests im Zusammenhang mit Systemen und Prozessen, die zur Erbringung dieser Dienstleistung eingesetzt werden (einschließlich Angabe der Produkte und der Anwendungsversion, die für konform befunden wurden). Zum Schutz der Vertraulichkeit der Systeme des Lieferanten können vertrauliche und/oder sensible Daten aus dem Bericht bzw. den Berichten entfernt werden. Die Anzahl und der Schweregrad der erkannten Probleme sind jedoch ebenso anzugeben wie die Maßnahmen zur Risikominderung und der Zeitrahmen zur Durchführung dieser Maßnahmen.
Informationsanfragen zur Informationssicherheit	Auf Verlangen von DPDHL Group muss der Lieferant DPDHL Group Antworten und Nachweise im Wege der Selbsteinschätzung im Rahmen eines „Request for Information“ (RfI) bezüglich der Informationssicherheit und des Datenschutz-risikos sowie der Einhaltung der Vorschriften durch den Lieferanten vorlegen.

Teil 3: Erweiterte Sicherheitsanforderungen

1) Diese erweiterten Sicherheitsanforderungen enthalten eine Zusammenfassung der technischen und organisatorischen Anforderungen an die Informationssicherheitskontrollen, die der Lieferant einhalten muss, wenn:
   a) der Lieferant DPDHL-Daten mithilfe von Systemen außerhalb der Räumlichkeiten von DPDHL Group verarbeitet oder
   b) der Lieferant über einen Zugriff (Fernzugriff oder eine andere Art Zugriff) auf DPDHL-Systeme verfügt.

2) Diese erweiterten Sicherheitsanforderungen gelten zusätzlich zu den Anforderungen in Bezug auf Informationssicherheitsverfahren und Datenschutzstandards, die in einer Vereinbarung zwischen dem Lieferanten und DPDHL Group festgelegt sind.

Tabelle D – Erweiterte Sicherheitsanforderungen

ISO-Kapitel/Kontrolle	Voraussetzungen
Organisation der Informationssicherheit	Der Lieferant muss über einen koordinierten Ansatz zur Informationssicherheit verfügen. Das Information Security Management System (ISMS) des Lieferanten muss insbesondere Folgendes umfassen: 1) Verschiedene regelmäßig überprüfte Informationssicherheits-richtlinien, die definiert und umgesetzt werden müssen; 2) Alle Verantwortlichen für die Informationssicherheit müssen definiert und zugewiesen werden; 3) Sich widersprechende Aufgaben und Verantwortungsbereiche müssen getrennt werden, um die Möglichkeiten einer unbefugten und unbeabsichtigten Änderung oder einer missbräuchlichen Nutzung der Vermögenswerte von DPDHL Group zu verringern; 4) Geeignete Kontakte zu zuständigen Behörden, speziellen Interessengruppen oder anderen speziellen Sicherheitsforen und Berufsverbänden, die gepflegt werden müssen; 5) Maßnahmen zur Informationssicherheit müssen unabhängig von der Art des Projekts im Projektmanagement berücksichtigt werden; 6) Definierte Sicherheitsmaßnahmen/Kontrollen zur Bewältigung der Risiken, die durch den Einsatz mobiler Geräte und durch mobiles Arbeiten entstehen; und 7) Die Informationssicherheitsrichtlinien müssen in geplanten Abständen oder bei wesentlichen Änderungen überprüft werden, um ihre fortdauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen.
Personalsicherheit	Der Lieferant muss Maßnahmen eingeleitet haben, um die Sicherheitsrisiken durch Personen vor und während der Beschäftigung sowie nach der Beendigung des Beschäftigungsverhältnisses zu verringern. Insbesondere muss der Lieferant: 1) alle Bewerber für eine Beschäftigung beim Lieferanten einer Hintergrundprüfung sowie einem Screening unterziehen;

ISO-Kapitel/Kontrolle	Voraussetzungen
	2) die Verantwortung für Informationssicherheit des Lieferantenpersonals in vertragliche Vereinbarungen, Richtlinien und Verfahren einbeziehen; 3) in regelmäßigen und festgelegten Abständen Aufklärungs- und Schulungsmaßnahmen zum Thema Informationssicherheit durchführen; und 4) über formale Disziplinarmaßnahmen für Lieferantenpersonal verfügen, das gegen die Informationssicherheitsrichtlinien verstößt.
Management von organisationseigenen Werten (Asset Management)	Der Lieferant muss Maßnahmen zum Management von Informationssicherheitswerten während ihres gesamten Lebenszyklus ergreifen. Insbesondere muss der Lieferant: 1) Vermögenswerte in Verbindung mit Informationen und informationsverarbeitenden Einrichtungen identifizieren und ein Inventar dieser Vermögenswerte erstellen und pflegen; 2) sicherstellen, dass die im Inventar geführten Vermögenswerte einen namentlich genannten Verantwortlichen haben; 3) sicherstellen, dass Regeln für den zulässigen Gebrauch von Informationen und von Vermögenswerten im Zusammenhang mit Informationen und informationsverarbeitenden Einrichtungen identifiziert, dokumentiert und umgesetzt werden; 4) sicherstellen, dass das gesamte Lieferantenpersonal und externe Nutzer bei Beendigung ihres Beschäftigungsverhältnisses, ihres Vertrags oder ihrer Vereinbarung alle in ihrem Besitz befindlichen Vermögenswerte von DPDHL Group und/oder des Lieferanten (wie jeweils zutreffend) zurückgeben; und 5) sicherstellen, dass Klassifizierung, Kennzeichnung und Handhabung von Informationswerten im Hinblick auf gesetzliche Anforderungen, Wert, Kritikalität und Sensibilität umgesetzt werden.
Zugangskontrolle (access control)	Der Lieferant muss Maßnahmen zur Zugangssteuerung ergreifen, um Informationswerte und Ressourcen zu schützen. Insbesondere muss der Lieferant: 1) Richtlinien und Verfahren für die Zugangssteuerung (einschließlich Onboarding, Offboarding und Crossboarding von Benutzern) festlegen und umsetzen und privilegierte Zugangsrechte verwalten; 2) Zugang nach dem Prinzip der geringsten Berechtigung und der Aufgabentrennung gewähren; 3) die Verantwortlichkeiten der Benutzer bei der Verwendung von geheimen Authentisierungsinformationen festlegen und mitteilen; 4) die Zugangsrechte der Benutzer in regelmäßigen Abständen überprüfen; 5) den Einsatz von Hilfsprogrammen, die in der Lage sind, System- und Anwendungskontrollen zu umgehen, einschränken; und

ISO-Kapitel/Kontrolle	Voraussetzungen
	6) Passwortrichtlinien umsetzen und Technologien für eine Multi-Faktor-Authentifizierung gemäß Risikovorgaben und Best Practice einsetzen.
Kryptographie	Der Lieferant muss kryptographische Kontrollen umsetzen, die den anerkannten Industriestandards entsprechen. Insbesondere muss der Lieferant: 1) eine Richtlinie zur Festlegung obligatorischer Verschlüsselungsmaßnahmen in Übereinstimmung mit den Informationsklassifizierungen definieren und umsetzen; und 2) eine Richtlinie für den Einsatz, den Schutz und die Lebensdauer von kryptografischen Schlüsseln definieren und umsetzen.
Physische und umgebungsbezogene Sicherheit	Der Lieferant muss über Maßnahmen verfügen, mit denen die Sicherheit von physischen Räumlichkeiten und Einrichtungen (z. B. Büros, Lager, Rechenzentren) gewahrt wird. Insbesondere muss der Lieferant Sicherheitskontrollen definieren und umsetzen, um Folgendes zu schützen: 1) Physische Sicherheitsperimeter und Zugangspunkte; 2) Büros, Räume, Anlagen, Sicherheitsbereiche sowie Be- und Entladezonen; 3) Ausrüstung (z. B. Betriebstechnik), Versorgungsanlagen, Strom- und Telekommunikationsverkabelung; 4) Verfahren für die Arbeit in Sicherheitsbereichen, die erarbeitet und angewendet werden sollen; und 5) Zugangspunkte, wie Be- und Entladezonen und andere Bereiche, bei denen die Möglichkeit eines Zutritts durch unbefugte Personen besteht. Zugangspunkte sind zu überwachen und nach Möglichkeit von informationsverarbeitenden Einrichtungen zu trennen, um so einen unbefugten Zutritt zu verhindern.
Betriebssicherheit	Der Lieferant muss Kontrollen zum Schutz von Informationswerten und informationsverarbeitenden Einrichtungen umsetzen. Insbesondere muss der Lieferant: 1) Richtlinien und Verfahren für Änderungsmanagement, Kapazitätsmanagement und Betriebsabläufe definieren und umsetzen; 2) Entwicklungs-, Test- und Betriebsumgebungen voneinander trennen; 3) Erkennungs-, Vorbeugungs- und Wiederherstellungs-maßnahmen zum Schutz gegen Schadsoftware umsetzen; 4) Sicherungskopien von Informationen, Software und System-abbildern in regelmäßigen und festgelegten Abständen erstellen und pflegen; 5) Ereignisprotokolle über Benutzeraktivitäten und Aktivitäten von Systemadministratoren/Systembetreibern führen und Protokolle vor unbefugtem Zugriff sichern; 6) alle Uhren von informationsverarbeitenden Systemen mittels einer einzigen Referenzquelle synchronisieren;

ISO-Kapitel/Kontrolle	Voraussetzungen
	7) die Installation von Software auf Produktivsystemen kontrollieren; 8) technische Schwachstellen identifizieren und zeitnah beheben; und 9) Auditanforderungen und -maßnahmen, einschließlich der Verifizierung der Betriebssysteme, sorgfältig planen, und dabei für eine möglichst geringe Störung der Geschäftsprozesse Sorge tragen.
Kommunikationssicherheit	Der Lieferant muss Kontrollen umsetzen, um die Sicherheit von Informationen, die über Netzwerke verarbeitet und übertragen werden, zu gewährleisten. Insbesondere muss der Lieferant Folgendes sicherstellen: 1) Netzwerke sollten zum Schutz von Informationen in Systemen und Anwendungen verwaltet und kontrolliert werden. Sicherheits-mechanismen, die Servicelevels und die Anforderungen an die Verwaltung aller Netzwerkdienste sollten ermittelt und in die Vereinbarungen über Netzwerkdienste aufgenommen werden, unabhängig davon, ob diese Dienste intern erbracht oder ausgelagert werden. Gruppen von Informationsdiensten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt sein. Es sollten formelle Übermittlungsrichtlinien, -verfahren und -kontrollen vorhanden sein, um die Übermittlung von Informationen durch die Nutzung aller Arten von Kommunikationseinrichtungen zu schützen; 2) Die Vereinbarungen sollten die sichere Übertragung von Geschäftsinformationen zwischen dem Lieferanten und externen Parteien regeln; 3) Informationen, die bei der elektronischen Nachrichtenübermittlung gesendet werden, sollten angemessen geschützt werden; und 4) Die Anforderungen an Vertraulichkeitsvereinbarungen, die die Bedürfnisse des Lieferanten zum Schutz von Informationen widerspiegeln, sollten ermittelt, regelmäßig überprüft und dokumentiert werden.
Beschaffung, Entwicklung und Instandhaltung von Systemen	Der Lieferant muss Kontrollen der Informationssicherheit in alle Informationssysteme und in den gesamten Lebenszyklus der Softwareentwicklung integrieren. Insbesondere muss der Lieferant Folgendes sicherstellen: 1) Es sollten Regeln für die Entwicklung von Software und Systemen aufgestellt und auf die Entwicklungen innerhalb des Lieferanten angewandt werden; 2) Bei Änderungen von Betriebsplattformen sollten geschäftskritische Anwendungen überprüft und getestet werden, um sicherzustellen, dass es keine negativen Auswirkungen auf die Betriebsabläufe oder die Sicherheit des Lieferanten und/oder von DPDHL Group (wie jeweils zutreffend) gibt;

ISO-Kapitel/Kontrolle	Voraussetzungen
	3) Von Änderungen an Softwarepaketen ist abzuraten; diese sollten auf notwendige Änderungen beschränkt sein und alle Änderungen sollten streng kontrolliert werden; und ~~4)~~ Der Lieferant sollte die Tätigkeit der ausgelagerten System-entwicklung beaufsichtigen und überwachen.
Lieferantenbeziehungen	Der Lieferant muss die Risiken steuern, die mit der Beauftragung von Drittanbietern (d. h. vierten Parteien von DPDHL Group) verbunden sind, welche auf die Informationswerte des Lieferanten zugreifen, diese verarbeiten oder speichern können. Insbesondere muss der Lieferant: 1) über eine Richtlinie für das Risikomanagement von Drittanbietern verfügen, mit der die Anforderungen an die Informationssicherheit festgelegt werden, um die Risiken von Drittanbietern zu mindern; 2) Anforderungen an die Informationssicherheit mit jedem Drittanbieter festlegen und förmlich vereinbaren (z. B. im Rahmen rechtsverbindlicher Verträge); 3) die Erbringung der Dienstleistungen durch Drittlieferanten regelmäßig überwachen, überprüfen und auditieren; und 4) Änderungen bezüglich der Erbringung von Dienstleistungen durch Drittanbieter durch Pflege von Informationssicherheitsrichtlinien, -verfahren und -kontrollen steuern.
Umgang mit Informationssicherheitsvorfällen	Der Lieferant muss über einen etablierten und dokumentierten Prozess zur Identifizierung, Bewertung und Reaktion auf Informations-sicherheitsvorfälle verfügen. Insbesondere muss der Lieferant: 1) Rollen und Zuständigkeiten im Zusammenhang mit der Handhabung von Informationssicherheitsvorfällen, einschließlich der Ermittlung der wichtigsten Abhängigkeiten und Eskalationspunkte, definieren; 2) Kanäle für die Meldung von Informationssicherheitsvorfällen (unabhängig davon, ob es sich um definierte Informations-sicherheitsvorfälle handelt oder nicht) oder festgestellten Sicherheitslücken/Schwachstellen einrichten und kommunizieren; 3) eine Methodik zur Einstufung und Klassifizierung von Informationssicherheitsvorfällen umsetzen; 4) im Anschluss an Informationssicherheitsvorfällen Analysen zur kontinuierlichen Verbesserung des Prozesses für die Handhabung von Informationssicherheitsvorfällen durchführen; und 5) Beweise bezogen auf einen Informationssicherheitsvorfall dokumentieren und aufbewahren.
Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs	Der Lieferant muss Maßnahmen zur Aufrechterhaltung der Informationssicherheit und deren Widerstandsfähigkeit in sein Business Continuity Management einbetten. Insbesondere muss der Lieferant: 1) Richtlinien, Verfahren und Pläne entwickeln, um die Aufrechterhaltung der Informationssicherheit und die Aufrecht-erhaltung des Informationssicherheitsmanagements unter widrigen Umständen sicherzustellen;

ISO-Kapitel/Kontrolle	Voraussetzungen
	2) Tests von Business Continuity-Plänen in regelmäßigen und vordefinierten Abständen durchführen und deren Ergebnisse dokumentieren, um sicherzustellen, dass die Kontrollen zwecks Aufrechterhaltung der Informationssicherheit wie erforderlich wirksam sind; und 3) Maßnahmen für einen redundanten Betrieb umsetzen, um die Verfügbarkeit der informationsverarbeitenden Einrichtungen zu gewährleisten.
Einhaltung von Vorgaben (Compliance)	Der Lieferant muss sicherstellen, dass er die gesetzlichen und vertraglichen Verpflichtungen und die selbst auferlegten Richtlinien und Verfahren zur Informationssicherheit einhält. Insbesondere muss der Lieferant: 1) ein Governance-Intervall (z.B. die erforderliche Häufigkeit von Überprüfungen) bezogen auf den Ansatz der Organisation zur Steuerung und Umsetzung der Good Industry Practice im Bereich der Informationssicherheit festlegen; und 2) Überprüfungen in regelmäßigen und geplanten Abständen durchführen, um die Einhaltung von Informationssicherheits-richtlinien, -prozessen und -standards zu bewerten.

Teil 4: Begriffsbestimmungen

1) Die in diesem Teil 4 aufgeführten Begriffsbestimmungen gelten für den ISCOP.

„Verbundene Unternehmen“	(i) in Bezug auf DPDHL Group eine juristische Person, die zurzeit oder in Zukunft direkt oder indirekt von Deutsche Post AG kontrolliert wird oder unter gemeinsamer Kontrolle mit Deutsche Post AG steht; und (ii) in Bezug auf den Lieferanten eine juristische Person, die zurzeit oder in Zukunft direkt oder indirekt vom Lieferanten kontrolliert wird oder unter gemeinsamer Kontrolle mit dem Lieferanten steht;
„Kontrolle“ oder „kontrolliert“	das kontrollierende Unternehmen, das direkt oder indirekt oder gemeinsam mit einem oder mehreren Dritten die Möglichkeit hat, die Geschäftsführung und die Politik des beherrschten Unternehmens zu bestimmen;
„Datenschutzrecht“	die DSGVO; die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (aktualisiert durch Richtlinie 2009/136/EG); sowie, soweit anwendbar, sämtliche einschlägigen Gesetze und Verordnungen anderer Länder im Zusammenhang mit der Verarbeitung von personenbezogenen Daten und Datenschutz;
„DPDHL-Daten“	sämtliche Daten oder Aufzeichnungen jeglicher Art und Form, die sich auf das Geschäft, die Mitarbeiter, die Kunden, die Lieferanten oder auf andere Weise auf das Geschäft von DPDHL Group beziehen;
„DPDHL Group“	Deutsche Post AG und jeweils die verbundenen Unternehmen von Deutsche Post AG; Verweise auf DPDHL Group im ISCOP gelten als Verweise auf alle und jede einzelne Gesellschaft. Darin eingeschlossen ist das betreffende Mitglied von DPDHL Group, das Vertragspartei

	einer Vereinbarung mit dem Lieferanten ist, die den ISCOP als Bestandteil umfasst;
„DPDHL-Systeme“	die Informationstechnologie- und Kommunikationssysteme, einschließlich Netzwerke, Hardware, Software, Middleware, virtuelle Plattformen und Schnittstellen, die Eigentum von DPDHL Group oder eines ihrer Vertreter, Kunden oder Auftragnehmer sind oder für diese lizenziert wurden;
„DSGVO“	Verordnung (EU) 2016/679 (die Datenschutz-Grundverordnung), einschließlich etwaiger jeweils geltender Änderungen und Aktualisierungen;
„Good Industry Practice”	in Bezug auf jede Tätigkeit die effektive, zuverlässige und fachkundige Ausübung dieser Tätigkeit mit dem Maß an Sachkunde, Sorgfalt, Umsicht, Weitblick und Urteilskraft, das vernünftigerweise von einem sachkundigen und erfahrenen Unternehmer mit vergleichbarem Renommee erwartet werden kann, der ähnliche Dienstleistungen erbringt;
„Informationssicherheitsvorfall“	1) jede tatsächliche oder vermutete Beeinträchtigung der Vertraulichkeit, Integrität oder Verfügbarkeit von DPDHL-Daten; 2) jede tatsächliche oder vermutete Beeinträchtigung oder jeder unbefugter Zugriff auf DPDHL-Daten verarbeitende Systeme, die die Vertraulichkeit, Integrität oder Verfügbarkeit von DPDHL-Daten gefährden; oder 3) der Eingang einer Beschwerde, eines Berichts oder sonstiger Informationen über die mögliche Beeinträchtigung oder Offenlegung von DPDHL-Daten, die vom Lieferanten verarbeitet werden;
„Internet“	das globale Netzwerk, das eine Vielzahl von Informations- und Kommunikationsmöglichkeiten bietet und aus miteinander verbundenen Netzwerken besteht, die standardisierte Kommunikationsprotokolle verwenden;
„ISCOP“	der von DPDHL Group verfasste „Verhaltenskodex zur Informationssicherheit für Partner“;
„Verarbeitung” oder „**verarbeiten“** oder **„verarbeitet“**	jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit 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.
„Personenbezogene Daten“	personenbezogene Daten (wie im Datenschutzrecht definiert), die dem Datenschutzrecht unterliegen;
„Dienstleistungen“	eine einzelne bzw. alle Dienstleistungen, die vom Lieferanten erbracht werden;
„Lieferant“	die Gegenpartei einer Vereinbarung mit DPDHL Group, die den ISCOP als Bestandteil umfasst;

„Lieferantenpersonal“	die Mitarbeiter, Auftragnehmer und andere Personen, die vom Lieferanten, seinen verbundenen Unternehmen oder deren Subunternehmern von Zeit zu Zeit mit der Erfüllung der Verpflichtungen des Lieferanten beauftragt werden.