Inhaltsverzeichnis

BTs Sicherheitsanforderungen an Lieferanten

1. Einleitung und Umfang

1.1 Dieses Dokument enthält BTs grundlegende Sicherheitsanforderungen in Bezug auf den von einem Lieferanten übernommenen Arbeitsumfang. Diese Anforderungen gliedern sich in drei Stufen.

Die erste Anforderungsstufe in Abschnitt 2 bezieht sich auf Lieferanten, die Arbeiten mit beschränkten BT-Informationen durchführen und unter Umständen beschränkten Zugang zu BTs administrativen Systemen und BT-Netzwerken haben. Lieferanten, die in diese Kategorie fallen, müssen keine anderen Anforderungen in diesem Dokument erfüllen.

Die Abschnitte 3 bis 6 der zweiten Stufe sind verpflichtend für alle anderen Arten von Arbeiten.

Für die dritte Stufe können je nach Arbeitsumfang eine oder mehrere Anforderungen der Abschnitte 7 bis 18 gelten. Ihr BT-Beschaffungsvertreter kann Ihnen diesbezüglich Auskunft geben.

Einige der Anforderungen verweisen gegebenenfalls auf einen der nachstehend angeführten Anhänge, die zusätzliche Informationen enthalten. :

Anhang 1 Informationsklassifikation
Anhang 2 Verpflichtende Schulung
Anhang 3 Weiterleiten von Fragen/Problemen an eine BT-Sicherheitskontaktperson
Anhang 4 Zugang zu Standorten und Gebäuden von BT durch BT-fremde Organisationen – nur Großbritannien
Anhang 5 Sicherheitsanforderungen für externes Hosting

1.2 Die vorliegenden Sicherheitsanforderungen gelten als Ergänzung und unbeschadet jeglicher sonstigen Verpflichtungen des Lieferanten im Vertrag (unter anderem einschließlich seiner Verpflichtungen unter den Bestimmungen betreffend „Vertraulichkeit", „Schutz persönlicher Daten" und Zuverlässigkeitsprüfungen (PECs)).

2. Sicherheit von Informationen bei beschränktem Zugriff

Die Einhaltung von Abschnitt 2 ist die einzige Anforderung, die gilt, wenn der Lieferant Arbeiten mit beschränktem Zugriff auf BT-Informationen durchführt und unter Umständen beschränkten Zugang zu BTs administrativen Systemen wie iSupplier und BT-Netzwerken hat (darunter fallen unter anderem, jedoch nicht ausschließlich Bürobedarf, Haustechnik, Standortbegutachtungen, Gutscheinprogramme und Personalrabattprodukte, Inhaltsanbieter und Rechteinhaber für BT TV).

Unbeschadet etwaiger Vertraulichkeitsverpflichtungen des Lieferanten hat der Lieferant, wenn der Lieferant oder Fremdpersonal Zugriff auf Informationen von BT oder BTs Kunden (einschließlich persönlicher Daten) hat, die sich auf BT oder BTs Kunden beziehen:
(a) zu gewährleisten, dass bei solchen Informationen (einschließlich persönlicher Daten) keine Preisgabe gegenüber Fremdpersonal und kein Zugriff durch Fremdpersonal erfolgt, das nicht direkt mit BT-Arbeiten beschäftigt ist, und
(b) die Sicherheit und Vertraulichkeit solcher Informationen (einschließlich persönlicher Daten) aufrechtzuerhalten (und die Aufrechterhaltung durch relevantes Fremdpersonal zu gewährleisten) (unter anderem, jedoch nicht ausschließlich durch Systeme und Verfahren, die erforderlich zum Schutz der Sicherheit aller Informationen sind, die BT gehören oder der

Kontrolle von BT unterstehen, soweit sie sich im Besitz oder unter der Kontrolle des Lieferant befinden, gemäß bewährter Branchenpraxis und durch rigorosen Einsatz solcher Systeme und Verfahren).

Die Abschnitte 3 bis einschließlich 6 gelten für alle Lieferantenbeziehungen mit BT (ausgenommen jene Lieferanten, die lediglich Leistungen mit beschränktem Zugriff erbringen).

3. Allgemeine Informationssicherheit

3.1 Der Lieferant hat BT zeitnah die Kontaktangaben der Sicherheitskontaktperson des Lieferanten und jegliche Änderungen daran bekannt zu geben.

3.2 Zu Beginn des Vertrags hat der Lieferant der BT-Sicherheitskontaktperson schriftlich unter Verwendung von Anhang 3 die geografischen Standorte mitzuteilen, wo die Hauptleistungen erbracht werden, wo sich relevantes Fremdpersonal befindet oder wo BT-Informationen verarbeitet oder gespeichert werden. Während der Vertragslaufzeit hat der Lieferant ferner der BT-Sicherheitskontaktperson mittels Anhang 3 jegliche vorgeschlagenen Änderungen an den geografischen Standorten mitzuteilen, damit BT etwaige Risiken für BT oder BT-Kundendaten neu abschätzen kann.

3.3 Der Lieferant hat für alle Verträge mit relevanten Subunternehmern Sorge zu tragen, einschließlich schriftlicher Bedingungen, die Subunternehmer dazu verpflichten, sich an BTs Sicherheitsanforderungen an Lieferanten im zutreffenden Ausmaß zu halten. Diese Bestimmungen müssen zwischen dem Lieferanten und seinem Sublieferanten vereinbart sein, bevor der Sublieferant oder dessen Personal auf BT-Systeme und BT-Informationen zugreifen darf.

3.4 Der Lieferant darf BT-Informationen ausschließlich für den Zweck verwenden, für den ihm die BT-Informationen von BT zur Verfügung gestellt werden, und selbst dann nur in dem Ausmaß, das notwendig ist, damit der Lieferant den Vertrag erfüllen kann. Der Lieferant hat BT-Informationen entsprechend den Anforderungen in Anhang 1 der vorliegenden Sicherheitsanforderungen und entsprechend maßgeblicher Gesetze zu behandeln und zu verwenden.

3.5 Der Lieferant hat die BT-Sicherheitskontaktperson unter Verwendung von Anhang 3 zu verständigen, falls sich beim Lieferanten eine Fusion, eine Akquisition oder eine Veränderung der Besitzverhältnisse anbahnt, damit BT etwaige Risiken für BT und BT- oder BT-Kundendaten neu abschätzen kann.

3.6 Der Lieferant hat zumindest jährlich oder im Fall von Änderungen an den Leistungen oder der Art ihrer Erbringung die vorliegenden Sicherheitsanforderungen erneut zu prüfen, um die unveränderte Einhaltung aller anwendbaren Sicherheitsanforderungen zu gewährleisten.

3.7 Der Lieferant hat für den sicheren Umgang mit etwaigen BT-Sachwerten und/oder BT-Gütern Sorge zu tragen, die dem Lieferanten von BT bereitgestellt werden.

- BT-Sachwerte und BT-Güter sind sicher zu verwahren, wenn sie nicht in Verwendung sind. Beispiele sind unter anderem, jedoch nicht ausschließlich Token für Fernzugriff, BT-Laptops, Netzwerkausrüstung, Server und Dokumentationsmaterial.
- BT-Sachwerte dürfen nicht ohne vorherige Genehmigung vom Arbeitsplatz mitgenommen werden.

3.8 Der Lieferant hat in Bezug auf die Erbringung der Leistungen formelle Managementverfahren für Sicherheitsvorfälle mit definierten Zuständigkeiten zu haben, und jegliche Informationen über einen Sicherheitsvorfall sind „vertraulich" zu behandeln. Der Lieferant hat die BT-Sicherheitskontaktperson unter Verwendung von Anhang 3 innerhalb eines zumutbaren Zeitraums nach Bekanntwerden über jegliche Vorfälle zu informieren:

i) bei denen es zum Verlust oder zur Beschädigung von Material oder zum Missbrauch von BT-Informationen, BT-Sachwerten, BT-Gütern oder zu einem unangemessenen oder nicht autorisierten Zugriff auf BT-Systeme und BT-Informationen oder zu einem Verstoß gegen eine der Verpflichtungen des Lieferanten gemäß den vorliegenden Sicherheitsanforderungen gekommen ist; oder
ii) aus denen die Unfähigkeit folgt, die Leistungen vertragsgemäß zu erbringen,
iii) ferner über jegliche Handlungen, die einen Verstoß gegen die Anforderungen im vorliegenden Sicherheitsdokument darstellen.

Auf entsprechende Anfrage hat der Lieferant BT zeitnah einen schriftlichen Bericht mit einem Behebungsplan einschließlich Zeitplan und Maßnahmen zur Vermeidung einer Wiederholung des Vorfalls vorzulegen.

3.9 Der Lieferant hat zu gewährleisten, dass erkannte Risiken für die Vertraulichkeit, Integrität oder Verfügbarkeit von BT-Informationen im Besitz des Lieferanten oder auf Systemen des Lieferanten umgehend beseitigt werden.

3.10 BT kann Risikobewertungen über jeden relevanten Bestandteil der Leistungen (worunter für die Leistungen relevante Sublieferanten fallen können) durchführen, um etwaige zusätzliche Risiken für BT infolge der Bereitstellung der Leistungen zu identifizieren. Anschließend kann BT zusätzliche Gegenmaßnahmen zur Bewältigung etwaiger Risiken formulieren. Kosten im Zusammenhang mit der Umsetzung von Gegenmaßnahmen sind von beiden Parteien zu vereinbaren.

3.11 Der Lieferant hat über Sicherheitsrichtlinien und -prozesse zu verfügen und Aufzeichnungen zu führen (deren Kopien in englischer Sprache zur Verfügung gestellt werden müssen), um die Einhaltung der vorliegenden Sicherheitsanforderungen zu belegen, und er hat BT gemäß dem nachfolgenden Abschnitt 7 Zugang zu solchen Belegen zu gewähren.

3.12 Der Lieferant hat dafür Sorge zu tragen, dass Verfahren und Kontrollen vorhanden sind, um die Übertragung von BT-Informationen mittels E-Mail-, Sprach-, Fax- und Videokommunikationseinrichtungen zu schützen. (Zum Beispiel ist bei Telefonkonferenzen sicherzustellen, dass alle teilnehmenden Personen autorisiert sind, über BT-Informationen

zu diskutieren.) Weitere Informationen über den Umgang mit BT-Informationen enthält Anhang 1.

3.13 Der Lieferant hat zum angemessenen Schutz von BT-Informationen Verfahren gegen Sicherheitsbedrohungen zu implementieren, die sich gegen BT oder gegen Dritte richten, die für BT arbeiten.

3.14 Der Lieferant hat zu gewährleisten, dass externe und Heimarbeitsaktivitäten in Bezug auf BT-Informationen und BT-Systeme geeigneten Sicherheitskontrollen innerhalb der Organisation des Lieferanten unterliegen, wozu unter anderem, jedoch nicht ausschließlich die starke Authentifizierung des Fernzugriffs von Benutzern zählt.

3.15 Bei Kündigung oder Ablauf des Vertrags hat der Lieferant dafür Sorge zu tragen, dass er selbst, Fremdpersonal und Subunternehmer jegliche BT-Informationen im Besitz oder unter der Kontrolle des Lieferanten oder seiner Subunternehmer auf sichere Weise gemäß Anhang 1 der vorliegenden Sicherheitsanforderungen vernichten, es sei denn, BT gibt etwas anderes an oder rechtliche oder behördliche Verpflichtungen sprechen dagegen. Archivierte Informationen müssen so verwahrt werden, dass sie nicht für tägliche Geschäftsaktivitäten verwendet werden können.

3.16 Der Lieferant hat BT-Informationen so lange aufzubewahren, wie es für die Erbringung der Leistungen nötig ist, längstens jedoch für zwei Jahre, es sei denn, ein anderer Aufbewahrungszeitraum wird von BT festgelegt oder ist erforderlich, um rechtliche oder behördliche Anforderungen zu erfüllen.

3.17 Der Lieferant hat für die Verfügbarkeit, Qualität, Integrität und angemessene Kapazität zur Bereitstellung der erforderlichen Systemleistung oder der Vertragsleistungen mit unterbrechungsfreier Verfügbarkeit Sorge zu tragen, indem er Folgendes gewährleistet:

- Ein Sicherungsplan ist vorhanden.
- Kritische Systemdaten werden gegebenenfalls geschützt.
- Ein Reservesystem ist implementiert, sofern dies eine vereinbarte Anforderung ist.
- Das System oder der Dienst ist nach einem schwerwiegenden Ausfall oder Unglück wiederherstellbar.
- Der Plan wird mindestens einmal jährlich geprobt.
- Sicherungskopien von Informationen und Software werden gegebenenfalls erstellt, und es wird regelmäßig eine vereinbarte Sicherungsrichtlinie getestet, um die Wiederherstellung von unveränderten Daten zu gewährleisten.

4. Sicherheit in Bezug auf Fremdpersonal

4.1 Relevantem Fremdpersonal darf kein Zugang gewährt werden, bevor BTs Sicherheitsschulung gemäß Anhang 2 der vorliegenden Sicherheitsanforderungen absolviert wurde. BTs Informationssicherheitsschulung kann vom Lieferanten vorbehaltlich der Zustimmung seitens der BT-Sicherheitsabteilung durch dessen eigene

Informationssicherheitsschulung ersetzt werden. Diesbezüglich ist eine verpflichtende Schulung wie in Anhang 2 dargelegt aufzufrischen. Der Lieferant hat Schulungsaufzeichnungen zu führen, die BT zur Prüfung zur Verfügung zu stellen sind.

4.2 Der Lieferant hat dafür Sorge zu tragen, dass jegliches Fremdpersonal eine Vertraulichkeitsvereinbarung des Lieferanten unterzeichnet, bevor mit Arbeiten in BT-Gebäuden oder an BT-Systemen begonnen wird oder bevor Zugriff auf BT-Informationen gewährt wird. Solche Vertraulichkeitsvereinbarungen sind vom Lieferanten aufzubewahren und BT im Rahmen von Kontrollen zur Prüfung zur Verfügung zu stellen.

4.3 Der Lieferant hat Verstöße gegen Sicherheitsrichtlinien und -verfahren mittels formeller Prozesse einschließlich geeigneter Disziplinarmaßnahmen zu ahnden.

4.4 Der Lieferant hat eine vertrauliche Hotline-Einrichtung zu führen, die seinem Personal zur Verfügung steht, um im gesetzlich zulässigen Ausmaß von Fremdpersonal verwendet zu werden, wenn es nicht kohärente Anweisungen erhält, die gegen die vorliegenden Sicherheitsanforderungen verstoßen. Über relevante Meldungen ist die BT-Sicherheitskontaktperson unter Verwendung von Anhang 3 zu informieren.

4.5 Wenn Fremdpersonal nicht mehr mit den zu erbringenden Leistungen befasst ist, hat der Lieferant dafür zu sorgen, dass der Zugriff auf BT-Informationen widerrufen wird und BT-Sachwerte oder BT-Güter oder BT-Informationen im Besitz von Fremdpersonal dem jeweiligen BT-Betriebsteam zurückgegeben oder gemäß Anhang 1 der vorliegenden Sicherheitsanforderungen vernichtet werden. Gegebenenfalls hat der Lieferant ein kontrolliertes Ausstiegsverfahren einzuführen, das den schriftlichen Antrag an die BT-Betriebsleitung beinhaltet, BT-Zugangsberechtigungen und -Identitäten zu entfernen. Fremdpersonal ist darauf aufmerksam zu machen, dass die unterzeichnete Vertraulichkeitsvereinbarung weiterhin in Kraft bleibt und dass BT-Informationen, die im Zuge der Arbeit an den Leistungen erlangt wurden, nicht preisgegeben werden dürfen.

4.6 Im Rahmen der Gewährung von Zugangsberechtigungen hat der Lieferant Aufzeichnungen über jegliches Fremdpersonal zu führen und vorzulegen, das Zugang benötigt oder BT-Leistungen bereitstellt, einschließlich des Namens, des Standorts, an dem gearbeitet wird, Geschäfts-E-Mail-Adresse und (gegebenenfalls) geschäftliche Telefonnummer mit direkter Durchwahl und/oder Mobiltelefonnummer, Datum der Anforderung einer (etwaigen) Benutzeridentifikationsnummer (UIN), Datum der Zuteilung zum BT-Projekt, Datum des Abschlusses der verpflichtenden Schulung, Datum des Ausscheidens aus dem BT-Projekt und einer Bestätigung der Zuverlässigkeitsprüfung. Die Sicherheitskontaktperson des Lieferanten hat jederzeit zu gewährleisten, dass nur relevantes Fremdpersonal eine Autorisierung erhält.

5. Audit und Sicherheitsüberprüfung

5.1 Der Lieferant hat in Bezug auf die Leistungen und unter Wahrung der Vertraulichkeit von Information über seine anderen Kunden auf entsprechende Anfrage BT oder BTs bevollmächtigten Vertretern in solcher Weise Zugang zu den Anlagen, Systemen und Aufzeichnungen des Lieferanten und relevanter Sublieferanten, die BT-Informationen

und BT-Kundendaten enthalten (einschließlich persönlicher Daten), zu gewähren (und für die Gewährung seitens Fremdpersonals Sorge zu tragen), wie es erforderlich ist, um die Einhaltung der vorliegenden Sicherheitsanforderungen durch den Lieferanten zu beurteilen.

Dazu kann die Bewertung aller Elemente physischer und logischer Kontrollen und die Validierung der Systeme des Lieferanten gehören, die BT-Informationen enthalten. Der Lieferant hat diese Beurteilung zu ermöglichen, indem er BT gestattet, Informationen im Zusammenhang mit der Bereitstellung der Leistungen je nach Bedarf zu erheben, zu verwahren und zu analysieren, um potenzielle Sicherheitsrisiken zu identifizieren, und er hat BT in dem zumutbaren Ausmaß Berichte bereitzustellen und an solchen Besprechungen teilzunehmen, wie es BT verlangt.

Falls von BT verlangt hat der Lieferant an einer Online-Befindlichkeitsprüfung teilzunehmen, um die grundlegende Einhaltung der Sicherheitsklauseln der vorliegenden Sicherheitsanforderungen festzustellen.

6. Untersuchung

6.1 Falls BT Grund zu der Annahme hat, dass seitens des Lieferanten oder eines beliebigen Sublieferanten ein Verstoß gegen die Bestimmungen der vorliegenden Sicherheitsanforderungen vorliegt, der sich auf BT-Systeme und/oder BT-Informationen auswirkt, informiert BT darüber die Sicherheitskontaktperson des Lieferanten. Der Lieferant hat in vollem Umfang mit BT und/oder einer Vollzugsbehörde an sich daraus ergebenden Untersuchungen mitzuwirken, wozu der Zugriff zu BT-Informationen in Anlagen des Lieferanten gehören kann, wenn dem Lieferanten hierfür eine angemessene Frist gesetzt wird.

Während der Untersuchung hat der Lieferant mit BT zusammenzuarbeiten, zumutbare Unterstützung zu leisten und Einrichtungen bereitzustellen, die für die Untersuchung des Verstoßes nötig sind. BT kann verlangen, dass der Lieferant materielle oder immaterielle Anlagen, die dem Lieferanten gehören, für Auswertungszwecke sperrt, und der Lieferant darf eine solche Forderung nicht unbegründet zurückweisen oder hinauszuzögern.

Für die Klauseln der Abschnitte 7 bis 18 gibt die Beschreibung für jeden Abschnitt an, für welche Leistungen die Klauseln gelten.

7. Allgemeine Sicherheitsanforderungen und -richtlinien

Die Einhaltung der Klauseln des Abschnitts 7 ist erforderlich, wenn der Lieferant Zugang zu „sensiblen Informationen" (gemäß Begriffsbestimmung) hat oder wenn er Entwicklungs-, Installations-, Wartungs-, Netzwerkfunktionsunterstützungs- oder professionelle IT-Leistungen bereitstellt.

7.1 Der Lieferant hat ISO27001-zertifiziert zu sein oder die Sicherheitsanforderungen der ISO27001-Zertifizierung oder an ISO27001 angeglichene Sicherheitsrichtlinien zu erfüllen und/oder auf ISO27001 in einem mit BT vereinbarten Zeitrahmen hinzuarbeiten.

7.2 Gegebenenfalls kann BT von Zeit zu Zeit sicherheitsbezogene Richtlinien, Leitlinien, Sicherheitsanforderungen und sonstige Anforderungen aktualisieren. BT baut auf eine Vertragsänderungsanfrage hin, die BT vom Lieferanten schriftlich zu übermitteln ist, relevante Aktualisierungen in eine aktualisierte Version der vorliegenden Sicherheitsanforderungen ein. Kosten im Zusammenhang mit der Umsetzung neuer Sicherheitsanforderungen sind von beiden Parteien zu vereinbaren.

7.3 Der Lieferant hat BT Kopien von Sicherheitsbescheinigungen und Gültigkeitserklärungen in Bezug auf die bereitzustellenden Leistungen zur Verfügung zu stellen, um einen Nachweis der Einhaltung dieses Programms zu erbringen.

8. Physische Sicherheit – BT-Räumlichkeiten

Die Einhaltung der Klauseln von Abschnitt 8 ist erforderlich, wenn der Lieferant Leistungen in BT-Räumlichkeiten erbringt.

8.1 Fremdpersonal, das in BT-Räumlichkeiten arbeitet, muss im Besitz eines vom autorisierten Lieferanten oder von BT bereitgestellten Ausweises sein. Dieser Ausweis ist in BT-Räumlichkeiten jederzeit als Mittel der Identitätsprüfung zu tragen und hat ein auf dem Ausweis sichtbares Foto zu umfassen, das ein klares und unverfälschtes Abbild des Fremdpersonals zeigt. Fremdpersonal kann auch eine elektronische Zugangskarte und/oder zeitlich begrenzte Besucherkarte zur Verfügung gestellt werden, die gemäß örtlichen Anweisungen bei der Ausgabe zu verwenden ist.

8.2 Nur genehmigte BT-Build-Server, BT-Webtop-PCs und vertrauenswürdige Endgeräte dürfen direkt mit BT-Domänen verbunden werden (Anschluss an einen LAN-Port oder drahtlose Verbindung). Der Lieferant darf ohne vorherige schriftliche Genehmigung seitens der BT-Sicherheitskontaktperson (einzuholen unter Verwendung von Anhang 3) keine nicht von BT genehmigte Ausrüstung an eine BT-Domäne anschließen (und er hat gegebenenfalls dafür Sorge zu tragen, dass sich Fremdpersonal ebenfalls daran hält). Die BT-Sicherheitskontaktperson erteilt die schriftliche Genehmigung bei Initiierung des Sicherheitsrichtlinienkonzessionsverfahrens innerhalb von BT.

8.3 BT-Informationen dürfen nicht aus BT-Räumlichkeiten entfernt werden, und ohne vorherige Genehmigung seitens BT darf keinerlei Ausrüstung oder Software aus BT-Räumlichkeiten entfernt oder in BT-Räumlichkeiten installiert werden.

8.4 Physische Schutzmaßnahmen und -richtlinien für die Arbeit in BT-Räumlichkeiten sind zu befolgen, z. B. Begleitung beim Betreten sicherer Bereiche. Zusätzlich gelten Befehle oder Anweisungen, die BT einem Vertreter des Lieferanten erteilt, als dem Lieferanten selbst erteilt.

8.5 Wenn der Lieferant autorisiert ist, seinem Fremdpersonal unbegleiteten Zugang zu Bereichen innerhalb von BT-Anlagen zu gewähren, müssen sich der BT-fremde Zeichnungsberechtigte und Fremdpersonal an jegliche Anweisungen halten, die von BT erteilt werden. Zusätzlich sind für den BT-fremden Zeichnungsberechtigten und Fremdpersonal mindestens Zuverlässigkeitsprüfungen der Stufe L2 erforderlich.

9. Physische Sicherheit – Räumlichkeiten des Lieferanten

Die Einhaltung der Klauseln von Abschnitt 9 ist erforderlich, wenn der Lieferant Leistungen von BT-fremden Räumlichkeiten aus erbringt, und umfasst Fremdpersonal, Subunternehmer sowie Mitarbeiter, Subunternehmer und Bevollmächtigte des Lieferanten.

9.1 Der Zugang zu BT-fremden Räumlichkeiten (Standorten, Gebäuden oder internen Bereichen), in denen Leistungen erbracht werden oder in denen BT-Informationen gespeichert oder verarbeitet werden, hat durch einen von einem autorisierten Lieferanten ausgestellten Ausweis zu erfolgen. Dieser Ausweis ist in den entsprechenden Räumlichkeiten jederzeit als Mittel der Identitätsprüfung zu tragen und hat ein auf dem Ausweis sichtbares Foto zu umfassen, das ein klares und unverfälschtes Abbild der Person zeigt. Personen kann auch eine autorisierte elektronische Zugangskarte für den alleinigen Zwecks des Zugangs zu den entsprechenden Räumlichkeiten zur Verfügung gestellt werden, oder es kann eine Zugangskontrolle mittels Tasteneingabe mit Prozessen zur Kontrolle der Autorisierung, Verbreitung und regelmäßigen Codeänderungen/spontanen Codeänderungen dafür eingesetzt werden.

9.2 Der Lieferant hat dafür Sorge zu tragen, dass der Zugang zu Standorten, Gebäuden oder internen Bereichen, in denen Leistungen erbracht oder BT-Informationen gespeichert oder verarbeitet werden, autorisiert werden muss und dass die Sicherheitsprozesse und -verfahren eingehalten werden, was auch für Sublieferanten mit physischem Zugang zu solchen Bereichen gilt (z. B. Wartung von Umgebungskontrollsystemen, Alarmanlagenunternehmen).

9.3 Auf Verlangen eines BT-Unternehmens oder BT-Projektverantwortlichen hat der Lieferant dafür Sorge zu tragen, dass relevantes Fremdpersonal auf sichere Weise von sonstigem Lieferantenpersonal abgegrenzt wird.

9.4 Sichere Bereiche in Lieferantenräumlichkeiten (z. B. Netzwerkkommunikationsräume) haben durch geeignete Zugangskontrollen abgegrenzt und geschützt zu sein, um zu gewährleisten, dass nur autorisiertes Fremdpersonal Zugang zu solchen sicheren Bereichen gestattet wird. Der Zugang zu solchen Bereichen durch Fremdpersonal ist regelmäßig zu prüfen, und mindestens einmal jährlich ist eine Neuautorisierung der Zugangsrechte zu solchen Bereichen durchzuführen.

9.5 Videoüberwachungssysteme (CCTV) und damit verbundene Aufzeichnungsmedien sind vom Lieferanten als Reaktion auf Sicherheitsstörfälle, als Mittel der Sicherheitsüberwachung, zur Abschreckung oder als Hilfsmittel zur möglichen Ergreifung von Personen beim Begehen eines Verbrechens einzusetzen. Wenn Videoüberwachungsbilder aufgezeichnet werden (entweder auf Band oder digital), müssen sie mindestens 20 Tage lang aufbewahrt werden. Dieser Zeitraum kann in den folgenden Situationen verlängert werden:
i) Wenn Videoüberwachungsbeweismaterial für eine Störfalluntersuchung oder strafrechtliche Ermittlungen aufbewahrt werden muss.
ii) Wenn es eine notwendige Voraussetzung zur Einhaltung von Gesetzen darstellt.

Alle für die Aufzeichnung von Kamerabildern verwendeten Videoüberwachungsbänder müssen in einem versperrten Schrank verwahrt werden, und der Schlüssel dazu ist sicher

und kontrolliert zu verwahren. Der Zugang zu einem solchen Schrank muss ausschließlich auf autorisiertes Personal beschränkt sein.
Alle Videoüberwachungsanlagen/digitalen Videorekorder müssen diskret angeordnet sein, um den nicht autorisierten Zugang dazu und die Möglichkeit „versehentlicher" Einblicke auf einen der angeschlossenen Überwachungsmonitore zu verhindern.

9.6 Das lokale Gebiet im Umfeld der für die Produkte und/oder Leistungen verwendeten Einrichtungen des Lieferanten ist gegebenenfalls vom Lieferanten regelmäßig auf Risiken und Bedrohungen zu überprüfen.

9.7 Versorgungs- und Telekommunikationskabel, die der Datenübertragung, der Unterstützung von Informationsdiensten oder Funk-/Satellitendiensten dienen, die bei der Bereitstellung der Leistungen verwendet werden, müssen vom Lieferanten auf das nötige Maß an Schutz überprüft werden, um eine Unterbrechung des Geschäftsbetriebs zu verhindern. Physische, der wirtschaftlichen Kritikalität ihres betrieblichen Zwecks angemessene Schutzmaßnahmen müssen wie folgt implementiert sein:
i) Geschäftsentscheidende Trassen, Kabelschirmungen, Schächte oder Gehwege, in denen geschäftsentscheidende Kabel verlaufen, müssen geschützt sein.
ii) Der Zugang zu Kabelschächten oder Steigleitungsschränken innerhalb von Betriebsgebäuden ist entweder durch elektronische Zugangskontrollen oder effektives Schlüsselmanagement zu beschränken.
iii) Computerkommunikationsverbindungen und Kommunikationsausrüstung innerhalb von Computeranlagen müssen physisch und umgebungstechnisch geschützt sein.
iv) Funk- und Satellitenkommunikationsverbindungen und Kommunikationsausrüstung müssen angemessen geschützt sein.

9.8 Bemannte Sicherheitsdienste gelten unter den folgenden Umständen als notwendige Ergänzung von elektronischen und physischen Sicherheitsmaßnahmen an Lieferantenstandorten:

- Standort ist von betrieblicher Bedeutung
- Verarbeitete BT-Informationen können Marke und Ruf beeinträchtigen
- Hohes Aufkommen verarbeiteter BT-Informationen (z. B. Geschäftsprozessauslagerung)
- Vertragliche Kundenanforderungen
- Standortspezifische Risiken/Bedrohungen
- Lieferant ist im Besitz von hochgradig sensiblen BT-Informationen.

9.9 Um BT-Ausrüstung (wie Server oder BT-Switches) in Lieferantenräumlichkeiten vor Umgebungsbedrohungen oder -gefahren und vor der Möglichkeit eines nicht autorisierten Zugriffs zu schützen, ist BT-Ausrüstung in einem geschützten Bereich und abgegrenzt von Anlagen unterzubringen, die für Systeme BT-fremder Organisationen verwendet werden. Das Ausmaß der Abgrenzung muss gewährleisten, dass die Sicherheit von BT-Ausrüstung nicht entweder vorsätzlich oder versehentlich infolge eines Zugriffs, der BT-fremden Organisationen darauf gewährt wird, beeinträchtigt werden kann und kann zum Beispiel die Form von sicheren Trennwänden, versperrbaren Schränken oder Metallkäfigen aufweisen.

9.10 Präventions- und Erkennungsmaßnahmen sind einzusetzen, um durch die Unterbrechung unerlässlicher Dienste oder sonstige Umwelteinflüsse verursachte Anlagenausfälle zu verhindern.

- Feuer

- Gas
- Hochwasser
- Stromausfall

Alarme sind zu installieren und mit einer permanent bemannten Stelle zu verbinden, um die Erkennung folgender Gefahren zu ermöglichen:

- Feuer
- Gas
- Stromausfall
- Ausfall der unterbrechungsfreien Stromversorgung (USV)
- Ausfall der Klimaanlage bzw. Luftfeuchtigkeits-/Temperaturregelung

9.11 Sicherheitsumfriedungen (Barrieren wie Mauern, Zäune, kartengesteuerte Eingangstore oder bemannte Empfangsschalter) sind einzusetzen, um Bereiche zu schützen, die BT-Informationen und Datenverarbeitungseinrichtungen beinhalten.

9.12 Zugangspunkte wie Liefer- und Ladebereiche sowie sonstige Stellen, an denen nicht autorisierte Personen das Gelände betreten könnten, sind zu kontrollieren und nach Möglichkeit von Datenverarbeitungseinrichtungen zu isolieren, um nicht autorisierten Zugang oder vorsätzliche Angriffe zu verhindern.

9.13 Es ist zu gewährleisten, dass der physische Zugang zu Bereichen mit Zugriff auf BT-Informationen ausschließlich mit Chipkarten oder Näherungskarten (oder gleichwertigen Sicherheitssystemen) möglich ist, und der Lieferant hat regelmäßige interne Prüfungen zur Gewährleistung der Einhaltung dieser Bestimmungen durchzuführen.

9.14 Der Lieferant hat dafür Sorge zu tragen, dass das Fotografieren und/oder die Bilderfassung von jeglichen BT-Informationen oder BT-Kundendaten verboten ist. Unter außergewöhnlichen Umständen, wenn eine geschäftliche Notwendigkeit für die Erfassung solcher Bilder vorliegt, muss eine vorübergehende Aussetzung dieser Klausel schriftlich bei der BT-Sicherheitskontaktperson unter Verwendung von Anhang 3 beantragt werden.

9.15 Der Lieferant hat Richtlinien zum Leeren von Schreibtischen und Bildschirmen zum Schutz von BT-Informationen zu unterhalten.

10. Bereitstellung einer Hosting-Umgebung

Die Einhaltung der Klauseln von Abschnitt 10 ist erforderlich, wenn der Lieferant eine Hosting-Umgebung für BT- oder BT-Kundenausrüstung bereitstellt.

10.1 Der Lieferant hat, wenn der Lieferant einen sicheren Zugangsbereich in seinen Räumlichkeiten für das Hosting von BT- oder BT-Kundenausrüstung bereitstellt („Lieferantenstandort"):

(a) zu gewährleisten, dass jegliches Fremdpersonal, das den Lieferantenstandort betritt, im Besitz eines Ausweises oder einer elektronischen Zugangskontrollkarte ist. Dieser Ausweis ist am Lieferantenstandort jederzeit als Mittel der Identitätsprüfung zu tragen und hat ein auf dem Ausweis sichtbares Foto zu umfassen, das ein klares und unverfälschtes Abbild des Fremdpersonals zeigt; und

(b) über Verfahren zum Umgang mit Sicherheitsbedrohungen zu verfügen, die sich gegen BT- oder BT-Kundenausrüstung oder gegen Dritte richten, die für BT arbeiten, um BTs

Informationen und die Informationen von BTs Kunden am Lieferantenstandort zu schützen; und
(c) Videoüberwachungssysteme und damit verbundene Aufzeichnungsmedien als Reaktion auf Sicherheitsstörfälle, als Mittel der Sicherheitsüberwachung, zur Abschreckung oder als Hilfsmittel zur möglichen Ergreifung von Personen beim Begehen eines Verbrechens einzusetzen. Der Lieferant hat zu gewährleisten, dass Videoüberwachungsmaterial im Umfang von 20 Tagen aufgezeichnet wird, um es als wirksames Untersuchungshilfsmittel verwenden zu können; und
(d) BT einen Grundrissplan mit dem im sicheren Bereich des Lieferantenstandorts zugeteilten Platz bereitzustellen; und
(e) zu gewährleisten, dass die Schränke von BT und BTs Kunden am Lieferantenstandort verschlossen gehalten bleiben und nur von autorisiertem BT-Personal, BTs genehmigten Vertretern und relevantem Fremdpersonal darauf zugegriffen werden darf; und
(f) einen sicheren Schlüsselmanagementprozess am Lieferantenstandort zu implementieren; und
(g) regelmäßig das lokale Gebiet im Umfeld des Lieferantenstandorts auf Risiken und Bedrohungen zu überprüfen; und
(h) Betriebsverfahren (in der Sprache des Landes der Herkunft der BT-Arbeiten) zu dokumentieren und zu pflegen, um die in diesem Absatz 12 aufgeführten Sicherheitsanforderungen zu belegen, und BT auf Verlangen Zugang so solchen Unterlagen zu gewähren.

10.2 BT stellt dem Lieferanten Folgendes zur Verfügung:
(a) eine Aufstellung der physischen Sachwerte von BT und/oder BTs Kunden am Lieferantenstandort; und
(b) Details über BTs Mitarbeiter, Subunternehmer und Bevollmächtigte, die (laufend) Zugang zum Lieferantenstandort benötigen.

11. Entwicklung von Leistungen

Die Einhaltungen der Klauseln von Abschnitt 11 ist erforderlich, wenn sich der Lieferant mit der Entwicklung von Leistungen für die Verwendung durch BT und/oder BT-Kunden befasst. (Der Begriff umfasst „vorgefertigte Standardkomponenten", Softwarekonfigurationen und Fertigungskomponenten für die Leistungen.)

11.1 Der Lieferant hat für alle gelieferten Komponenten vereinbarte Sicherheitsmaßnahmen einzubauen, sodass Vertraulichkeit, Verfügbarkeit und Integrität der Leistungen geschützt werden, und zwar durch:

(i) Führen einer entsprechenden Dokumentation (in der Sprache des Landes der Herkunft der BT-Arbeiten) in Bezug auf die Implementierung von Sicherheit und Gewährleistung, dass die Dokumentation und solche Sicherheitsmaßnahmen bewährter Branchenpraxis entsprechen;
(ii) Minimieren der Chancen nicht autorisierter Personen (z. B. Hacker), Zugriff auf BT-Systeme und BT-Informationen, BT-Netzwerke oder BT-Dienste zu erlangen, und
(iii) Minimieren des Risikos eines Missbrauchs von BT-Systemen und BT-Informationen, BT-Netzwerken oder BT-Diensten, der potenziell zu einem Verlust von Einnahmen oder einem Ausfall von Diensten führen könnte.

11.2 Der Lieferant hat auf Verlangen zu belegen, dass gelieferte Software oder BT bereitgestellte Hardware (sowohl Eigenbau als auch vorgefertigter Standard) den mit BT vereinbarten Spezifikationen entspricht. Der Lieferant hat die Integrität von Builds einschließlich Upgrades, Betriebssystemen und Anwendung vom Werk bis zum Schreibtisch zu wahren.

11.3 Der Lieferant hat zu gewährleisten, dass die Entwicklung von Systemen für die Verwendung durch BT oder der Bau und die Wartung von Hardware in BT-Eigentum auf BTs IT-Sicherheitsanforderungen abgestimmt ist, wenn diese vom BT-Betriebsteam bereitgestellt werden, oder auf bewährte Branchenpraxis.

11.4 Der Lieferant hat zu gewährleisten, dass Entwicklungs- und Testumgebungen keine Live-Daten enthalten und von der Live-Umgebung abgegrenzt sind. Von BT bereitgestellte Testdaten sind nach einem vom BT-Dateneigentümer festgelegten Zeitraum zu löschen.

11.5 Der Lieferant gewährleistet, dass sämtliche zumutbaren Bemühungen unternommen worden sind, um dafür zu sorgen, dass die Software und/oder Hardware (sowie in elektronischem Format bereitgestellte Dokumentation) frei ist von unter anderem jeder Form von

(i) „elektronischer Besessenheit" und „Logikbomben";
(ii) „Viren" und „Würmern", die unter Verwendung der (zum Zeitpunkt des Versands) neuesten kommerziell erhältlichen Virenerkennungssoftware erkannt hätten werden können; und
(iii) „Spyware", „Adware" und sonstiger Malware.

(Den Begriffen kommt die Bedeutung zu, die man allgemein in der Computerbranche darunter versteht.) Der Lieferant gewährleistet bei und nach der Annahme, dass die Software und/oder Hardware während des Gewährleistungszeitraums gemäß den Funktionsspezifikationen funktionieren, und der Lieferant hat ausschließlich qualitativ gute Materialien, Techniken und Sicherheitsanforderungen bei der Erfüllung des Vertrags einzusetzen und jederzeit die Sicherheitsanforderungen an Sorgfalt, Kompetenz und

Gewissenhaftigkeit anzuwenden, die für gute Computerpraktiken und sichere Codierungsmethodik erforderlich sind.

11.6 Der Lieferant hat mit BT zusammenzuarbeiten, um auf Kosten des Lieferanten zu gewährleisten, dass die Sicherheitsanforderungen den/die entsprechenden Sicherheitsrahmen erfüllen; von Zeit zu Zeit kann es dafür erforderlich sein, dass die Leistungen entsprechenden Sicherheitstests unterzogen werden.

11.7 Etwaige Sicherheitsmängel an den Leistungen, die von BT oder vom Lieferanten erkannt werden, sind auf Kosten des Lieferanten innerhalb eines von BT zumutbar verlangbaren Zeitrahmens zu beheben.

12. Zugriff auf Informationen

Anwendbar, wenn in den Anforderungen aufgeführt.

12.1 Innerhalb von 14 Tagen nach BTs schriftlicher Aufforderung und nach Wahl von BT erfolgt entweder:
(a) dass die Parteien, die dabei jeweils ihre eigenen Kosten tragen, eine Informationszugriffsvereinbarung in der Form der in Anhang 3 dargelegten Informationszugriffsvereinbarung abschließen und der jeweils anderen Partei zustellen; oder
(b) dass der Lieferant auf eigene Kosten eine Hinterlegungsvereinbarung im Wesentlichen in der Form der in Anhang 21 dargelegten Vereinbarung in Bezug auf alle Informationen und Dokumentationsunterlagen im Zusammenhang mit den Leistungen (unter anderem in Hinblick auf Software sämtliche Quellcodes, Kopplungsdaten, Softwarelistings, vollständigen technischen Daten, Anmerkungen der Programmierer, alle Informationen und Dokumentationsunterlagen im Zusammenhang mit der Software, die notwendig für Wartung, Änderung und Korrektur der Software und für die Bereitstellung von Support jeder Stufe für die Software sind) abschließt („die Hinterlegungsinformationen") und bei NCC Escrow International Limited (die „Hinterlegungsstelle") eine aktuelle Kopie der Hinterlegungsinformationen hinterlegt. Der Lieferant hat sicherzustellen, dass es solche Hinterlegungsinformationen BT und/oder einem kompetenten Dritten für BT ermöglichen:

(i) etwaige ausständige Verpflichtungen des Lieferanten unter dem Vertrag fertigzustellen, unter anderem einschließlich Verpflichtungen, die bestanden hätten (einschließlich der Verpflichtung, Aufträge zu erfüllen, die BT andernfalls im Rahmen des Vertrags erteilt hätte), wenn der Vertrag nicht von BT (in anderer Form als gemäß Absatz 4 der Bestimmungen mit dem Titel „Kündigung") vor dem Ablauf seiner natürlichen Laufzeit (worunter jede etwaige Verlängerung der ursprünglichen Laufzeit nach Wahl von BT fällt) gekündigt worden wäre; und
(ii) die Hinterlegungsinformationen problemlos zu verstehen und die Hinterlegungsinformationen und die Leistungen zu warten (einschließlich Upgrades), zu ändern, zu optimieren und zu korrigieren.

12.2 Der Lieferant gewährleistet, dass die entweder bei BT oder bei der Hinterlegungsstelle hinterlegten Hinterlegungsinformationen ausreichend gewartet sind und werden, um es einem hinlänglich kompetenten Programmierer oder Analysten zu ermöglichen, die Software ohne Hilfe einer anderen Person oder zusätzlichen Materials zu warten oder zu optimieren, und der Lieferant verpflichtet sich ferner, die

Hinterlegungsinformationen während der gesamten Laufzeit auf dem neuesten Stand zu halten.

12.3 Im Fall eines Ereignisses, das es BT oder der Hinterlegungsstelle gestattet, die Hinterlegungsinformationen zu verwenden und/oder freizugeben, hat der Lieferant unverzüglich und auf eigene Kosten BT für einen angemessenen Zeitraum Rat, Unterstützung, Hilfe, Daten, Informationen, Zugriff auf entscheidendes Personal des Lieferanten oder dessen Lizenzgeber der Software in der Form bereitzustellen, dass die Hinterlegungsinformationen und/oder die Software verstanden, gewartet (einschließlich Upgrading), optimiert, geändert und korrigiert werden können.

12.4 Unbeschadet etwaiger sonstiger Rechte, die BT unter Umständen hat, fällt BT automatisch das nicht exklusive, unbefristete, unwiderrufliche, weltweite Recht zu, die Hinterlegungsinformationen nach ihrer Freigabe unentgeltlich zu verwenden, um die Leistungen zu warten und zu supporten, und zwar mit dem nicht exklusiven, unbefristeten, unwiderruflichen, weltweiten und unentgeltlichen Recht, die Leistungen und etwaige geänderte, adaptierte, optimierte und/oder korrigierte Leistungen zu verwenden, zu kopieren, zu warten (einschließlich Upgrades), zu ändern, anzupassen, zu optimieren und zu korrigieren und solche Leistungen an Dritte (vorbehaltlich der Beschränkungen etwaiger Lizenzen des Lieferanten) zu lizenzieren, und zwar zusammen mit dem Recht, Dritte zu Vorgenanntem für BT zu autorisieren.

12.5 Diese Bestimmung überdauert den Ablauf oder die Kündigung des Vertrags.

12.6 Falls es zur Gewährleistung der Einhaltung von Sicherheitsbelangen erforderlich ist, hat die BT-Netzwerk-Sicherheitskontaktperson (und/oder von ihr ernannte Personen, die Mitarbeiter von BT sein müssen) ähnliche (sinngemäß anwendbare) Rechte, wenn es im Rahmen der Leistungen, der Einarbeitung und der Validierung (per Definition in der Informationszugriffsvereinbarung) in Bezug auf Quellmaterial (per Definition in der Informationszugriffsvereinbarung) verlangt wird.

13. Zugriff auf BT-Systeme

Die Einhaltung der Klauseln von Abschnitt 13 ist erforderlich, wenn Fremdpersonal des Lieferanten Zugriff auf BT-Systeme benötigt, um Leistungen bereitzustellen.

13.1 BT kann nach alleinigem Ermessen in dem Ausmaß, das BT bestimmt, Zugriff ausschließlich für die Bereitstellung von Leistungen gestatten, solange der Lieferant dazu autorisiert ist, Zugriff zu haben.

13.2 In Bezug auf Zugriff hat der Lieferant dafür Sorge zu tragen (und gegebenenfalls zu gewährleisten, dass jegliches Fremdpersonal dafür Sorge trägt):

a) dass Benutzeridentifikation, Kennwörter, PINs, Token und Konferenzeinrichtungszugang nur für Einzelpersonen von Fremdpersonal gelten und nicht geteilt werden. Solche Angaben müssen sicher und getrennt von dem Gerät verwahrt werden, für dessen Zugriff sie verwendet werden. Wird ein Kennwort einer anderen Person bekannt, muss es umgehend geändert werden.

b) Auf entsprechende Anfrage sind BT Berichte bereitzustellen, die BT betreffend Fremdpersonal benötigt, das autorisiert ist, auf BT-Systeme zuzugreifen.

c) Domänenübergreifendes Verlinken auf BT-Systeme ist nicht zulässig, es sei denn, es wird speziell von der BT-Sicherheitskontaktperson unter Verwendung von Anhang 3 genehmigt und autorisiert.

d) Es sind alle zumutbaren Bemühungen zu unternehmen, um zu gewährleisten, dass keine Viren und kein schädlicher Code (nach allgemeiner Auffassung der Begriffe in der Computerbranche) eingeführt werden, um das Risiko der Beschädigung von BT-Systemen oder BT-Informationen zu minimieren.

e) Es sind zumutbare Bemühungen zu unternehmen, um zu gewährleisten, dass persönlichen Dateien, die Informationen, Daten oder Medien ohne Bezug zu den Leistungen beinhalten, nicht auf BT-Servern, von BT bereitgestellten Laptopcomputern und Desktopcomputern, zentralen BT-Speichereinrichtungen oder BT-Systemen gespeichert werden.

13.3 Wenn BT dem Lieferanten Zugang zu Internet/Intranet bereitgestellt hat, dann hat der Lieferant selbst zu gewährleisten und dafür Sorge zu tragen, dass auch Fremdpersonal gewährleistet, dass der Zugriff auf Internet/Intranet ordnungsgemäß erfolgt, um die Bereitstellung der Leistungen zu ermöglichen. Es obliegt der Verantwortung des Lieferanten, zu gewährleisten, dass die folgenden Hinweise zum Missbrauch von Internet und E-Mail relevantem Fremdpersonal mindestens einmal jährlich zur Kenntnis gebracht werden.
Es darf auf keinerlei Material zugegriffen werden, das als Folgendes betrachtet werten könnte: -

a. Anstößig, sexueller Natur, sexistisch, rassistisch, politisch anrüchig;
b. Ein Akt, der BT oder Einzelpersonen in Verruf bringen könnte;
c. Der Betrieb eines Privatunternehmens;
d. Eine Urheberrechtsverletzung;
e. Internettelefonie oder -nachrichtendienste wie Skype
f. Umgehung oder Untertunnelung von BTs Firewall oder anderen Sicherheitsmechanismen;
g. Es dürfen keine Beiträge auf Websites oder Online-Aussagen veröffentlicht werden, die man nach billigem Ermessen als Ansichten von BT werden könnte.
h. Inakzeptable oder gefährliche Websites sind für Benutzer zu sperren.

13.4 Der Lieferant hat BT umgehend zu verständigen, wenn relevantes Fremdpersonal keine Zugriffsrechte auf BT-Systeme mehr benötigt oder sich die Rolle aus beliebigen Gründen von der in der Vereinbarung definierten Rolle ändert, um es BT zu ermöglichen, die Zugriffsrechte auf BT-Systeme zu deaktivieren oder anzupassen.

14. Zugriff auf BT-Informationen auf Lieferantensystemen

Die Einhaltung der Klauseln von Abschnitt 14 ist erforderlich, wenn BT-Informationen auf Lieferantensystemen gespeichert oder verarbeitet werden.

14.1 Wenn Fremdpersonal der Zugriff auf Lieferantensysteme gewährt wird, die mit der Bereitstellung des Lieferanten von Produkten und/oder Diensten für BT in Verbindung stehen, hat der Lieferant:

a) zu gewährleisten, dass jede Person eine eindeutige Benutzerkennung und ein eindeutiges Kennwort hat (das bewährter Branchenpraxis entspricht), das nur der

Person für die ausschließliche Verwendung im Rahmen des sicheren Anmeldevorgangs bekannt ist.

b) Zugriff auf Systeme in Lieferantenbesitz, die BT-Informationen enthalten oder auf BT-Informationen zugreifen, oder auf BT-Systeme nur im mindestens erforderlichen Ausmaß zu gewähren, das erforderlich ist, um es dem Fremdpersonal zu ermöglichen, seine Pflichten im Rahmen der Vereinbarung zu erfüllen.

c) formelle Verfahren zu unterhalten, um die Zuteilung, die Prüfung und die Widerrufung und/oder Beendigung von Zugriffsrechten zu kontrollieren.

d) zu gewährleisten, dass die Zuteilung und die Verwendung erweiterter Rechte und der Zugriff auf sensible Tools und Einrichtungen auf Lieferantensystemen kontrolliert und ausschließlich auf jene Benutzer beschränkt werden, für die eine geschäftliche Notwendigkeit dafür besteht. Der Zugriff und die Bedienung von Systemkonsolen müssen in einer sicheren Umgebung erfolgen, die den Assets, für deren Verwaltung sie verwendet werden, angemessen ist. Es müssen geeignete physische Sicherheitsvorkehrungen eingebaut werden, um zu gewährleisten, dass kein nicht autorisierter Zugriff erfolgen kann.

e) zu gewährleisten, dass die Vergabe von Benutzerkennwörtern für Systeme, die dem Lieferanten gehören und die BT-Informationen enthalten oder auf BT-Informationen zugreifen, durch einen formellen, überprüfbaren Verwaltungsprozess erfolgt.

f) regelmäßige Überprüfungen von Benutzerzugriffsrechten vorzunehmen.

g) zu gewährleisten, dass der physische Zugang zu Rechenausrüstung mit Zugriff auf BT-Informationen oder zur Speicherung von BT-Informationen ausschließlich mit Chipkarten oder Näherungskarten (oder gleichwertigen Sicherheitssystemen) möglich ist, und der Lieferant hat regelmäßige interne Prüfungen zur Gewährleistung der Einhaltung dieser Bestimmungen durchzuführen.

h) zu belegen, dass sich Benutzer bei der Verwaltung ihrer Kennwörter an optimale Sicherheitspraktiken halten.

i) ein Kennwortverwaltungssystem einzuführen, das eine sichere und effektive, interaktive Einrichtung zur Gewährleistung der Qualität von Kennwörtern bietet.

j) zu gewährleisten, dass Benutzersitzungen nach einem vordefinierten Inaktivitätszeitraum beendet werden.

k) zu gewährleisten, dass Prüfprotokolle generiert werden, um Benutzeraktivitäten und sicherheitsrelevante Ereignisse aufzuzeichnen, und dass diese sicher verwaltet werden. Protokolle sind für einen angemessenen Zeitraum aufzubewahren, um etwaige Untersuchungen zu ermöglichen, und es darf keinerlei Möglichkeit seitens des Lieferanten bestehen, den nicht autorisierten Zugriff auf die Prüfprotokolle oder Änderungen an den Prüfprotokollen zu gestatten.

l) zu gewährleisten, dass die Überwachung von Prüf- und Ereignisprotokollen und Analyseberichten für anomales Verhalten und/oder versuchte, nicht autorisierte Zugriffe von Personal des Lieferanten unabhängig von jenen Benutzern erfolgt, die überwacht werden.

14.2 Der Lieferant hat Systeme zu unterhalten, die versuchte Beschädigungen, Änderungen oder nicht autorisierte Zugriffe auf BT-Informationen auf Lieferantensystemen erkennen und aufzeichnen. Beispiele sind unter anderem, jedoch nicht ausschließlich Systemprotokollierung und Prüfprozesse, IDS, IPS usw.

14.3 Der Lieferant hat Kontrollen aufrechtzuerhalten, um Schadsoftware zu erkennen und gegen Schadsoftware zu schützen, ferner ist zu gewährleisten, dass geeignete Benutzerbewusstseinsverfahren implementiert sind.

14.4 Der Lieferant hat zu gewährleisten, dass mindestens einmal monatlich nicht autorisierte Software erkannt und von Lieferantensystemen entfernt wird, die BT-Informationen enthalten, verarbeiten oder auf BT-Informationen zugreifen.

14.5 Der Lieferant hat zu gewährleisten, dass der Zugriff auf Diagnose- und Verwaltungsanschlüsse sowie auf Diagnose-Tools streng kontrolliert wird.

14.6 Der Lieferant hat zu gewährleisten, dass der Zugriff auf die Prüf-Tools des Lieferanten auf relevantes Fremdpersonal beschränkt ist und dass ihre Nutzung überwacht wird.

14.7 Der Lieferant hat zu gewährleisten, dass Codeprüfungen und Penetrationstests an jeglicher hausintern produzierten Software, die zur Verarbeitung von BT-Informationen verwendet wird, von einem von den Entwicklern unabhängigen Team durchgeführt werden.

14.8 Server, die zur Bereitstellung der Leistungen verwendet werden, dürfen ohne geeignete Sicherheitskontrollen nicht in unvertrauenswürdigen Netzwerken eingesetzt werden (Netzwerke außerhalb des eigenen Sicherheitsumfelds, die außerhalb der eigenen administrativen Kontrolle liegen, z. B. mit dem Internet verbunden).

14.9 Änderungen an einzelnen Lieferantensystemen, die BT-Informationen beinhalten und verarbeiten und/oder die verwendet werden, um die Produkte und/oder Dienste für BT bereitzustellen, müssen kontrolliert werden und formellen Änderungskontrollverfahren unterliegen.

14.10 Die internen Uhren aller Systeme müssen mit einer vertrauenswürdigen Quelle synchronisiert werden.

15. Hosting von BT-Informationen durch den Lieferanten

Die Einhaltung der Klauseln von Abschnitt 15 ist erforderlich, wenn der Lieferant als vertraulich oder höher eingestufte BT-Informationen extern in einer Umgebung mit Cloud-Diensten oder in einer Umgebung mit Lieferanten- oder Subunternehmerservern hostet.

15.1 Der Lieferant hat in Zusammenhang mit den Leistungen dafür Sorge zu tragen, dass Umgebungen, in denen BT-Informationen gehostet werden, die Anforderungen in Anhang 5 erfüllen.

16. Netzwerksicherheit

Die Einhaltung der Klauseln von Abschnitt 16 ist erforderlich, wenn der Lieferant BT-Netzwerke oder -Netzwerkkomponenten herstellt, entwickelt oder supportet.

16.1 Der Lieferant hat in Bezug auf die Leistungen auf allen gelieferten Komponenten Sicherheitsmaßnahmen so einzubauen, dass sie die Vertraulichkeit, Verfügbarkeit und Integrität der BT-Netzwerke und/oder 21CN-Assets schützen. Der Lieferant hat BT umfassende Dokumentation in Bezug auf die Umsetzung der Netzwerksicherheit in Zusammenhang mit den Leistungen bereitzustellen und zu gewährleisten, dass sie und solche Sicherheitsvorkehrungen:

(a) alle rechtlichen und behördlichen Anforderungen zu erfüllen; und
(b) bestmöglich nicht autorisierte Personen (z. B. Hacker) davon abhalten, Zugang zu den Netzwerkverwaltungselementen und anderen Elementen zu erlangen, auf die über die BT-Netzwerke und/oder 21CN zugegriffen wird; und
(c) bestmöglich das Risiko eines Missbrauchs der BT-Netzwerke und/oder 21CN, der potenziell zu einem Verlust von Einnahmen oder einem Ausfall von Diensten führen könnte, durch jene Personen verringern, die autorisiert sind, darauf zuzugreifen; und
(d) bestmöglich auftretende Sicherheitsverstöße erkennen, um eine rasche Beseitigung sich daraus ergebender Probleme und die Identifizierung der Personen, die Zugang erlangt haben, und die Ermittlung, wie sie Zugang erlangt haben, zu ermöglichen; und
(e) das Risiko einer Fehlkonfiguration von BT-Netzwerken minimieren, was z. B. erreicht werden kann, indem nur die mindestens zur Erfüllung der vertraglichen Rolle erforderlichen Berechtigungen erteilt werden.

16.2 Der Lieferant muss alle zumutbaren Schritte zur Sicherung aller Schnittstellen gelieferter Komponenten ergreifen und darf nicht davon ausgehen, dass die gelieferten Komponenten in einer sicheren Umgebung betrieben werden.

16.3 Der Lieferant hat der BT-Netzwerk-Sicherheitskontaktperson die Namen und Anschriften (und weitere Angaben, die BT benötigt) aller Personen des Fremdpersonals bereitzustellen, die von Zeit zu Zeit direkt mit der Bereitstellung, Wartung und/oder Verwaltung der Leistungen befasst sind, und zwar bevor sie mit jeweiligen Bereitstellungs-, Wartungs- und/oder Verwaltungsaufgaben betraut werden.

16.4 In Bezug auf Support-Aktivitäten in Großbritannien hat der Lieferant ein kompetentes Sicherheitsteam zu unterhalten, das zumindest einen britischen Staatsbürger umfasst, der für den Kontakt mit der BT-Netzwerk-Sicherheitskontaktperson (oder von ihr ernannten Personen) zur Verfügung steht und an Besprechungen teilnimmt, die von der BT-Netzwerk-Sicherheitskontaktperson von Zeit zu Zeit begründet verlangt werden.

16.5 Der Lieferant hat der BT-Netzwerk-Sicherheitskontaktperson einen (nach Bedarf von Zeit zu Zeit aktualisierten) Übersichtsplan aller aktiven, in den Leistungen enthaltenen Komponenten und ihrer jeweiligen Quellen bereitzustellen.

16.6 Der Lieferant hat Details seiner einzelnen Mitarbeiter bereitzustellen, die Kontakt mit dem BT-Schwachstellen-Managementteam (CERT) in Bezug auf Schwachstellen in den Leistungen halten werden, die von BT und vom Lieferanten erkannt werden. Der Lieferant hat BT zeitgerecht Informationen über Schwachstellen bereitzustellen und auf eigene Kosten zumutbare Anforderungen in Bezug auf Schwachstellen zu erfüllen, die von der BT-Netzwerk-Sicherheitskontaktperson von Zeit zu Zeit gestellt werden können. Der Lieferant hat BT frühzeitig genug über Schwachstellen zu informieren, um die Einführung von

Entschärfungskontrollen zu ermöglichen, bevor der Lieferant die Schwachstellen öffentlich freigibt.

16.7 Der Lieferant hat der BT-Netzwerk-Sicherheitskontaktperson und von ihr ernannten Personen von Zeit zu Zeit vollen und uneingeschränkten Zugang zu Räumlichkeiten zu gewähren, wo die Leistungen entwickelt, hergestellt oder produziert werden, um Sicherheitserfüllungstests und/oder -beurteilungen durchzuführen, und der Lieferant hat an solchen Erfüllungstests mitzuwirken (und dafür Sorge zu tragen, dass relevantes Fremdpersonal daran mitwirkt).

16.8 Der Lieferant hat dafür Sorge zu tragen, dass in den Leistungen enthaltene, sicherheitsbezogene Komponenten, die durch oder für BT identifiziert werden, von Zeit zu Zeit auf Kosten des Lieferanten extern zu BTs angemessener Zufriedenheit evaluiert werden.

16.9 In Bezug auf Informationen, die von BT bereitgestellt oder erhalten werden und die als „STRENG VERTRAULICH" gekennzeichnet oder einfach als vertraulich interpretierbar sind, hat der Lieferant dafür Sorge zu tragen, dass:

(a) der Zugriff darauf nur solchem Fremdpersonal gewährt wird, das eigens von BT dafür autorisiert wurde, sie zu sehen und zu verarbeiten, und dass Aufzeichnungen über solche Zugriffe geführt werden;
(b) der Umgang damit, die Verwendung und die Speicherung mit großer Sorgfalt und Verschlüsselung mittels PGP oder WinZip 9 vor der Speicherung und unter solchen Bedingungen erfolgen, die ein hohes Maß an Widerstand gegen vorsätzliche Gefährdung (d. h. durch Verwendung des stärksten verfügbaren Verschlüsselungsalgorithmus/Verwendung eines starken Kennworts) bieten und mit hoher Wahrscheinlichkeit eine tatsächliche oder versuchte Gefährdung erkennen;
(c) bei der Übertragung angemessene Sicherheit durch Verschlüsselung mit Secure Email, PGP oder WinZip 9 zur Anwendung gelangt; und
(d) sie nicht ohne BTs schriftliche Erlaubnis außerhalb des Europäischen Wirtschaftsraums exportiert werden.

16.10 Der Lieferant hat der BT-Netzwerk-Sicherheitskontaktperson prompt und jedenfalls innerhalb von sieben Werktagen vollständige Angaben über Merkmale und/oder Funktionalität in den Leistungen (oder in der Roadmap für Leistungen geplante Merkmale und/oder Funktionalität) bereitzustellen, von denen:

(a) der Lieferant weiß; oder
(b) die BT-Netzwerk-Sicherheitskontaktperson begründet glaubt und dies dem Lieferanten mitteilt, dass sie für das legale oder sonstige Abfangen von Telekommunikationsverkehr gedacht sind oder verwendet werden könnten. Solche Angaben haben alle Informationen zu enthalten, die billigerweise erforderlich sind, um es der BT-Netzwerk-Sicherheitskontaktperson zu ermöglichen, das Wesen, die Zusammensetzung und den Umfang solcher Merkmale und/oder Funktionalität vollständig zu verstehen.

16.11 Um den Zugriff auf BT-Netzwerke und/oder -Systeme zu bewahren, hat der Lieferant BT umgehend über etwaige Änderungen seiner Zugriffsmethode durch die Firewalls zu informieren, einschließlich der Bereitstellung von Netzwerkadressübersetzung.

16.12 Netzwerküberwachungs-Tools, die Anwendungsinformationen einsehen können, dürfen nicht verwendet werden.

16.13 IPv6-Funktionalität in Betriebssystemen ist auf Hosts (Endnutzergeräte, Server), die Verbindungen mit BT-Netzwerkdomänen herstellen, und dort zu deaktivieren, wo sie nicht erforderlich ist.

16.14 Der Lieferant hat bereitgestellte BT-Richtlinien und Sicherheitsanforderungen zu erfüllen und dafür Sorge zu tragen, dass sie von jeglichen Leistungen erfüllt werden, wobei Ausnahmen bei Vertragsunterzeichnung oder im Rahmen der Änderungskontrolle zu vereinbaren sind.

16.15 Der Lieferant hat zu gewährleisten, dass für jegliches Fremdpersonal Zuverlässigkeitsprüfungen entsprechend der Zugangsstufe vorliegen.
http://www.selling2bt.bt.com/Downloads/3rdPartyPECsPolicy-v1.1.pdf

Lieferanten, die BT-Netzwerke oder -Netzwerkkomponenten herstellen, entwickeln oder supporten, müssen gewährleisten, dass für jegliches Fremdpersonal mindestens Zuverlässigkeitsprüfungen der Stufe L2 vorliegen. L3-Zuverlässigkeitsprüfungen sind für von der BT-Netzwerk-Sicherheitskontaktperson genannte Rollen erforderlich. Hat der Lieferant nicht die Möglichkeit, die Sicherheitsunbedenklichkeit von Fremdpersonal im Rahmen von L3-Prüfungen direkt zu ermitteln, unterstützt BT auf Kosten des Lieferanten beim Erlangen der Unbedenklichkeitsbescheinigung.

17. Lieferantennetzwerksicherheit

Die Einhaltung der Klauseln von Abschnitt 17 ist erforderlich, wenn das Netzwerk des Lieferanten genutzt wird, um die Leistungen bereitzustellen. (Darunter fallen LAN, WAN, Internet, Drahtlos- und Funknetze.)

17.1 Der Lieferant hat in Bezug auf die Leistungen auf seinen Netzwerken Sicherheitsmaßnahmen so einzubauen, dass sie die Vertraulichkeit, Verfügbarkeit und Integrität von BT-Informationen schützen. Die Maßnahmen haben:

(a) alle rechtlichen und behördlichen Anforderungen zu erfüllen; und
(b) bestmöglich nicht autorisierte Personen (z. B. Hacker) davon abzuhalten, Zugang zu den Netzwerken zu erlangen, und
(c) bestmöglich das Risiko eines Missbrauchs der Netzwerke, der potenziell zu einem Verlust von Einnahmen oder einem Ausfall von Diensten führen könnte, durch jene Personen, die autorisiert sind, darauf zuzugreifen, zu verringern; und
(d) bestmöglich auftretende Sicherheitsverstöße zu erkennen, um eine rasche Beseitigung sich daraus ergebender Probleme und die Identifizierung der Personen, die Zugang erlangt haben, und die Ermittlung, wie sie Zugang erlangt haben, zu ermöglichen.

18. Cloud-Sicherheit

Die Einhaltung der Klauseln von Abschnitt 18 ist ebenfalls erforderlich, wenn der Lieferant für BT Cloud-bezogene Dienste bereitstellt. (**Eine Definition des Begriffs „Cloud" ist der folgenden NIST-Veröffentlichung zu finden: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-143.pdf**)

18.1 Der Lieferanten hat den entsprechenden Nachweis zu erbringen, dass bereitgestellte Cloud-Dienste die Kontrollanforderungen der Cloud Security Alliance Cloud Controls Matrix (CCM) in der letztgültigen, unter https://cloudsecurityalliance.org verfügbaren Fassung zusätzlich zu Anhang 5 der vorliegenden Sicherheitsanforderungen erfüllen.

18.2 BT-Informationen, die im elektronischen Geschäftsverkehr genutzt werden und über öffentliche Netzwerke gelangen, sind bei der Übertragung und im Ruhezustand (einschließlich Sicherungen) gemäß Anhang 1 vor betrügerischen Aktivitäten sowie vor nicht autorisierter Preisgabe, nicht autorisiertem Zugriff und nicht autorisierten Änderungen zu schützen.

18.3 Netzwerk- und Infrastruktur-Service-Level-Vereinbarungen (intern oder extern) haben klar Sicherheitskontrollen, Umfang und Service-Level sowie Unternehmens- oder Kundenanforderungen zu dokumentieren.

18.4 Der Lieferant hat Penetrationstests und/oder Zugriff auf bestehende Lieferantenpenetrationstestberichte zu gestatten, die relevant für die Leistungen sind, die bereitgestellt werden, wobei Umfang und Zeitpunkt der Tests einvernehmlich mit BT zu vereinbaren sind.

18.5 Der Lieferant hat vereinbarte Sicherheitsmaßnahmen für alle gelieferten Komponenten so zu implementieren, dass Vertraulichkeit, Verfügbarkeit, Qualität und Integrität der Leistungen geschützt werden, indem die Chance minimiert wird, dass nicht autorisierte Personen (z. B. andere Cloud-Kunden) Zugriff auf BT-Informationen und BT-Dienste erlangen.

Glossar

In den vorliegenden Sicherheitsanforderungen gelten die folgenden Definitionen, andernfalls gelten die Begriffe des Vertrags für die vorliegenden Sicherheitsanforderungen, und alle Wörter und Ausdrücke, die in den vorliegenden Sicherheitsanforderungen verwendet werden, haben dieselbe Bedeutung, die ihnen im Vertrag beigemessen wird:
„**Zugriff**" – Verarbeitung, Handhabung oder Speicherung von BT-Informationen durch eine oder mehrere der folgenden Methoden:

- Durch wechselseitige Verbindung mit BT-Systemen
- Bereitgestellt in gedrucktem oder sonstigem nicht elektronischem Format
- BT-Informationen auf Lieferantensystemen
- Durch mobile Medien

und/oder Zugang zu BT-Gebäuden für die Bereitstellung von Leistungen (ausgenommen die Lieferung von Hardware und die Teilnahme an Besprechungen).]
[**Autorisiert**" – BT hat Zugriff entweder im Rahmen von BTs System-Interconnect-Prozess erteilt, oder es liegt eine schriftliche Autorisierung seitens des BT-Unternehmens oder BT-Projektverantwortlichen vor; „**Autorisierung**" ist dementsprechend auszulegen. Die Zugriffsebene hat relevant und auf das zur Bereitstellung der Leistungen erforderliche Ausmaß beschränkt zu sein.]
„**BT-Güter**" – All Güter, die dem Lieferanten von BT zur Verfügung gestellt werden, und alle Güter im Besitz des Lieferanten, die BT gehören. (Beispiele: Schlüssel für Schränke, Laptops, Token, Ausweiskarten, Pläne, Verfahrensdokumentation.)
„**BT-Netzwerk-Sicherheitskontaktperson**" – Informationssicherungsexperte der BT-Sicherheitsabteilung, zu kontaktieren durch Ausfüllen und Senden des Anfrageformulars in Anhang 3, oder eine andere Person, deren Identität und Kontaktangaben dem kaufmännischen Ansprechpartner des Lieferanten von Zeit zu Zeit bekannt gegeben werden können.
„**BT-Sachwerte**" – Alle Sachwerte im Besitz des Lieferanten, die BT gehören. (Beispiele: Router, Switches, Server oder Dokumentation.)
„**BT-Sicherheitsabteilung**" – Die für Sicherheit zuständige Organisation innerhalb von BT.
„**BT-Sicherheitskontaktperson**" – Informationssicherungsexperte der BT-Sicherheitsabteilung, zu kontaktieren durch Ausfüllen und Absenden des Anfrageformulars in Anhang 3.
„**BT-Sicherheitsrichtlinien**" steht für relevante BT-Netzwerksicherheitsrichtlinien, die von BT bereitgestellt werden.
„**BT-Systeme**" – Die Dienste und Dienstkomponenten, Produkte, Netzwerke, Server, Prozesse, papiergestützten Systeme oder IT-Systeme, die (gänzlich oder teilweise) BT gehören und/oder von oder für BT, BT Group plc oder eine beliebige juristische Person von BT Group plc betrieben werden; oder andere Systeme, die gegebenenfalls in BT-Räumlichkeiten untergebracht sind (einschließlich iSupplier (gemäß der Definition von „iSupplier" im Vereinbarungsabschnitt mit dem Titel „Zahlung und Rechnungslegung")) und im Kontext von „Zugriff" (nach obiger Definition) verwendet werden.
„**CCTV**" – steht für Close Circuit Television, d. h. Videoüberwachung.

„Beginndatum" – Entsprechend vertraglicher Definition.
„**Fremdpersonal**", „**Relevantes Fremdpersonal"** – Entsprechend vertraglicher Definition.
„**Informationen**" – bedeutet Informationen in konkreter oder jeder sonstigen Form, unter anderem einschließlich Spezifikationen, Berichte, Daten, Notizen, Dokumentationen, Zeichnungen, Software, Richtlinien, Verfahren, Prozesse, Standards, Computerausgaben, Entwürfe, Schaltpläne, Modelle, Muster, Proben, Erfindungen, (unabhängig davon, ob patentiert oder nicht) und Know-how sowie (gegebenenfalls) die Medien, auf denen solche Informationen geliefert werden.
„**ISO 27001**" – ein internationaler Sicherheitsmanagementsystemstandard von der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission.
„**Bestellung(en**)" – Eine Bestellung seitens BT beim Lieferanten über Leistungen gemäß Vertrag.
„**Netzwerksicherheit**" – steht für die Sicherheit der untereinander verbundenen Kommunikationswege und -knoten, die Endnutzertechnologien miteinander und damit verbundene Verwaltungssysteme logisch verbinden.
„**Persönliche Daten**" – hat die Bedeutungen, die dem Begriff in Richtlinie 95/46/EG oder nachfolgenden Gesetzen in Bezug darauf zugeschrieben werden („Die Richtlinie").
„**Prozess," „Verarbeitet" oder „Verarbeitung**" steht für jede Operation oder Abfolge von Operationen, die an BT-Informationen durchgeführt werden, sei es automatisch oder nicht, beispielsweise Erhebung, Aufzeichnung, Organisation, Speicherung, Anpassung oder Änderung, Abfrage, Einsicht, Verwendung, Preisgabe durch Übertragung, Verteilung oder sonstige Bereitstellung, Ausrichtung oder Kombination, Sperre, Löschung, Rückgabe oder Vernichtung.
„**Sensible Informationen**" – Jegliche als „vertraulich" oder höher eingestuften oder gekennzeichneten BT-Informationen, einschließlich persönlicher Daten.
„**Sublieferant**" – Entsprechend vertraglicher Definition.
„**Lieferantensysteme**" – Jegliche Computer-, Anwendungs- oder Netzwerksysteme, die dem Lieferanten gehören und verwendet werden, um auf BT-Informationen zuzugreifen, BT-Informationen zu speichern oder zu verarbeiten oder die an der Bereitstellung der Leistungen beteiligt sind.
„**Sicherheitskontaktperson des Lieferanten**" – Person, die BT vom Lieferanten von Zeit zu Zeit zu nennen ist und als einheitlicher Ansprechpartner für sicherheitsbezogene Themen agiert.
„**Leistungen**" – Gesamtheit aller Komponenten, Materialien, Werke, Werkzeuge, Testausrüstung, Dokumentation, Firmware, Software, Ersatzteile und Teile und sonstigen Dingen, die BT gemäß Vertrag bereitzustellen sind, zusammen mit allen Informationen und Arbeiten, deren Lieferung oder Erbringung für BT der Vertrag erfordert.
„**Übertragung" oder „Übertragen**" bedeutet
(a) das Verschieben von BT-Informationen im Besitz von Fremdpersonal (unter anderem einschließlich persönlicher Daten) von einem Standort zu einem anderen oder von einer Person zu einer anderen, sei es in physischer, mündlicher oder elektronischer Form; und
(b) das Gewähren von Zugriff auf BT-Informationen im Besitz von Fremdpersonal (unter anderem einschließlich persönlicher Daten) von einem Standort zu einem anderen oder von einer Person zu einer anderen, sei es in physischer, mündlicher oder elektronischer Form.