Richtlinien für Call Center

Allgemeine Bestimmungen

(A) Vorliegende Bestimmungen stehen in Zusammenhang mit der Umsetzungsmatrix im Anhang 1 dieses Dokuments, in dem Einzelheiten zu Verhaltensweisen und Ergebnissen genannt werden, die seitens BT in der Regel bei der Feststellung der Einhaltung der Vorgaben akzeptiert werden.

(B) BT kann jederzeit, vor oder während der Leistung, Risikobewertungen für das Kontaktzentrum nach den Bestimmungen in Kapitel 3.10 der Sicherheitsanforderungen für BT-Lieferanten durchführen ("Sicherheitsauflagen"). Unbeschadet weiterer zulässiger Rechtsmittel ist BT berechtigt, Abhilfemaßnahmen festzulegen, ausgleichende Kontrollen und Gegenmaßnahmen bei festgestellten Risiken und/oder unzureichender Einhaltung oder Nichteinhaltung vorliegender Bestimmungen durchzuführen. Der Lieferant hat diese Maßnahmen umzusetzen und schriftlich als Anlage zu diesen Bedingungen festzuhalten. Über die Kosten für die Umsetzung neuer Sicherheitsauflagen haben sich beide Parteien zu einigen.

(C) BT hat auf Anfrage das Recht, die Richtlinien und Verfahren des Lieferanten im Hinblick auf eine Entlastung von Anforderungen an vorliegende Standards als Teil der Risikobewertung für das Kontaktzentrum zu überprüfen. Die Richtlinien beziehen sich unter anderem auf: Richtlinien zur Nutzung von Computern, IT-Entsorgung, Kundenauthentifizierung, Voreinstellungsprüfungen, Risikoanalyse und Management-Prozess usw.

1. Sicherheit

1.1 Der Lieferant hat dafür zu sorgen, dass die Bereiche des Kontaktzentrums (siehe Glossar), die für den Betrieb des BT/EE-Kontos genutzt werden, räumlich von den übrigen Geschäftsbereichen getrennt werden und durch besondere Eingangskontrollen gesichert sind.

1.2 Der Lieferant hat ein prüfbares Verfahren einzurichten, das die Bedingungen für Erteilung und Entzug von Zugangsberechtigungen in den Bereich des Kontaktzentrums aufstellt. [1]

1.3 Der Lieferant hat dafür zu sorgen, dass zur Feststellung von Zugangsberechtigungen zu bestimmten Bereichen des Kontaktzentrums (einschließlich interner Verlegungen und Veränderungen) und im Fall, dass Mitarbeiter des Lieferanten ausscheiden, ein prüfbares Zugangsverfahren eingerichtet wird, das im Abstand von drei (3) Monaten überprüft wird, wobei die Daten der Überprüfungen aufzuzeichnen sind.

1.4 Der Lieferant hat dafür zu sorgen, dass im Bereich des Kontaktzentrums keine unbeaufsichtigten Arbeiten durchgeführt werden. Dies bezieht sich auf Reinigungskräfte und sonstige Beschäftigte von Dritten.

1.5 Der Lieferant hat ein prüfbares Verfahren einzurichten, das Drängeln an kontrollierten Eingängen wie Türen und/oder Schranken verhindert. Dieses Verfahren muss gegebenenfalls zwangsweise durchsetzbar sein und wiederholte Verstöße sind disziplinarisch zu ahnen.

2. Sicherheitsausweise und Besucher

2.1 Der Lieferant hat dafür zu sorgen, dass Mitarbeiter, die dazu berechtigt sind, Mobiltelefone, Laptops, iPads und/oder Tablets in das Kontaktzentrum mitzubringen und zu benutzten (in

[1] Siehe Umsetzungsmatrix mit Beispielen zum prüfbaren Zugangsverfahren.

Ausübung ihrer Aufgaben), leicht von anderen Mitarbeitern und Vorgesetzten zu unterscheiden sind.[2]

2.2 Der Lieferant muss ein prüfbares Verfahren zur Ausgabe und Handhabung von Sicherheitsausweisen für Mitarbeiter des Kontaktzentrums und vorläufigen Sicherheitsausweisen für bestimmte Fälle einrichten. In diesem Verfahren ist die automatische Sperrung von Zugangsmöglichkeiten bei Zeitablauf vorzusehen.

2.3 Der Lieferant hat dafür zu sorgen, dass Sicherheitsausweise und Umhängebänder nicht auf den Arbeitsplatz eines Mitarbeiters schließen lassen.

2.4 Der Lieferant hat dafür zu sorgen, dass ein prüfbares Verfahren für Besucher eingeführt wird und alle Mitarbeitern hiervon Kenntnis erhalten. Zu Beweiszwecken ist ein Besucherprotokoll anzufertigen.[3]

2.5 Sicherheitsausweise für Besucher müssen sich von denen der Mitarbeiter unterscheiden und beim Verlassen des Kontaktzentrums zurückgegeben werden. Werden Sicherheitsausweise nicht unverzüglich zurückgegeben, werden sie zum folgenden Arbeitstag deaktiviert.

2.6 Der Lieferant hat dafür zu sorgen, dass Besucher des Kontaktzentrums ständig begleitet werden und erkennbare Besucherbuttons/-ausweise tragen.

3. Beschäftigte

3.1 Der Lieferant hat dafür zu sorgen, dass sämtliche persönlichen Gegenstände (einschließlich mobile Endgeräte) in Schließfächern außerhalb der Räume des Kontaktzentrums aufbewahrt werden.

3.2 Der Lieferant hat Arzneimittel/medizinische Geräte für persönliche Zwecke wie Inhaliergeräte, Insulin oder Hustenmittel in den Räumen des Kontaktzentrums zuzulassen.

3.3 Mitarbeiter in den Räumen des Kontaktzentrums ist es nicht gestattet, Mobiltelefone oder mobile Endgeräte bei sich zu führen, es sei denn, sie verfügen über eine Genehmigung, die nach vorheriger Risikoanalyse erteilt wurde. Der Lieferant hat regelmäßige Stichproben durch Beobachtung vorzunehmen, um festzustellen, ob Mobiltelefone oder mobile Endgeräte in die Räume des Kontaktzentrums mitgebracht wurden. Das Verbot des Einführens von derartigen Geräten ist durch Hinweisschilder anzuzeigen. Zusätzlich sind Schulungsprogramme zur Bewusstseinsschulung durchzuführen und es ist ein Disziplinarverfahren einzurichten, das bei Verstößen Anwendung findet.

3.4 Der Lieferant hat dafür zu sorgen, dass Verfahren eingerichtet werden, die es ermöglichen, Mitarbeiter durch Dritte zu kontaktieren im Fall von privaten Notfällen.[4]

3.5 Es ist ein prüfbares Verfahren für die Genehmigung und den Gebrauch von Kugelschreibern, Bleistiften und Papier in den Räumen des Kontaktzentrums einzurichten. Kugelschreiber, Bleistifte und Papier dürfen nur von Mitarbeitern benutzt werden, denen hierfür von ihrem Vorgesetzten zur Ausübung ihrer Funktionen eine Genehmigung erteilt wurde.

3.6 Der Lieferant hat dafür zu sorgen, dass Mitarbeiter handschriftliche Notizen, die im Rahmen der Ausübung ihrer Funktionen erstellt werden, nicht unbeaufsichtigt zurückgelassen werden, sondern am Ende eines Arbeitstags sicher aufbewahrt (je nach Art der Information und

[2] Siehe Umsetzungsmatrix mit Beispielen dazu, wie eine leichtere Unterscheidung möglich ist.
[3] Siehe Umsetzungsmatrix zu den Angaben, die in das Besucherprotokoll aufzunehmen sind.
[4] Siehe Umsetzungsmatrix mit Beispielen für das Verfahren bei privaten Notfällen.

Klassifizierung) oder entsorgt werden, um die Vorgaben an einen[5] 'Sauberen Schreibtisch'[6] zu erfüllen.

http://www.selling2bt.bt.com/working/ThirdPartySecuritystandards/index.htm

3.7 Der Lieferant hat Whiteboards & abwischbare Notizblöcke (einschließlich geeigneter Stifte und Tücher) als Alternative zu Kugelschreibern, Bleistiften und Papier und zwecks Aufzeichnung von Notizen bei Telefonaten bereit zu stellen. Der Lieferant hat dafür zu sorgen, dass Notizen sofort nach Abschluss des Kundengesprächs gelöscht werden. Alle Aufzeichnungen auf Whiteboards sind nach der Arbeitsschicht eines jeden Mitarbeiters zu löschen. Geschäftsleiter und Vorgesetzte haben die Räume zu begehen und Stichproben zu nehmen um die Einhaltung dieser Vorgaben festzustellen.

3.8 Der Lieferant hat dafür zu sorgen, dass sämtliche online oder mit elektronischen Geräten aufgezeichnete Notizen (zum Support von Kundengesprächen) automatisch nach der Arbeitsschicht eines jeden Mitarbeiters oder nach Abschluss des Arbeitstags gelöscht werden. Die Löschung ist automatisch vorzunehmen oder in einem Tagesdatensatz zum Nachweis der Einhaltung dieser Vorgabe aufzubewahren.

3.9 Der Lieferant hat dafür zu sorgen, dass ein prüfbares Verfahren für die Benutzung von Whiteboards / Papier eingeführt und angewandt wird, damit:

- Papier nach einem Arbeitstag sicher aufbewahrt, entfernt oder entsorgt wird; und
- Whiteboards nach jeder Arbeitsschicht und nach jedem Arbeitstag gereinigt werden. [7]

3.10 Der Lieferant muss die Aufzeichnung aller Interaktionen mit Kunden auf dem Konto vornehmen (Memo oder Notizblock, je nach System).

3.11 Der Lieferant hat dafür zu sorgen, dass keine Interaktion mit Kunden auf einer Microsoft Office - Applikation aufgezeichnet wird, es sei denn, Mitarbeiter sind dazu in Ausübung ihrer Aufgaben nach Risikoanalyse berechtigt.

3.12 Der Lieferant muss dafür sorgen, dass jede genehmigte Aufgabe zur Durchführung der folgenden Handlungen im Kontaktzentrum einer Risikoanalyse gemäß der in Kapitel 11 genannten Vorgaben unterzogen wird. Unter anderem werden folgende Handlungen erfasst, wobei es sich nicht um eine abschließende Aufstellung handelt:

- Benutzung von Microsoft Office Applikationen
- Benutzung von mobilen Endgeräten des Unternehmens
- Benutzung von Laptops des Unternehmens
- Benutzung privater Gegenstände (siehe Definition im Glossar)
- Möglichkeit zum Drucken oder Kopieren von Kundeninformation
- Möglichkeit, aufgezeichnete Gespräche von dem(n) entsprechenden Server(n) herunterzuladen
- Zugang zu internen oder externen E-Mail-Konten oder sonstigen Kommunikationsinstrumenten, z.B. Chat
- Benutzung von Kugelschreibern/Bleistiften und Papier für Notizen
- Versand mehrfacher Textnachrichten an Kunden

[5] Siehe Umsetzungsmatrix mit Beispielen zur sicheren Aufbewahrung oder Entsorgung.
[6] Siehe Umsetzungsmatrix mit Beispielen zur Umsetzung der Vorgaben an einen sauberen Schreibtisch.
[7] Siehe Umsetzungsmatrix mit Beispielen zum Inhalt von Kontrollen von Whiteboards/Papier.

- Remotezugang zum Gerät des Kunden

3.13 Der Lieferant hat dafür zu sorgen, dass kein Versand mehrfacher Textnachrichten (eine Textnachricht an mehrere Kunden) erfolgt, es sei denn, der Mitarbeiter ist hierzu in Ausübung seiner Aufgabe berechtigt. Werden derartige Textnachrichten versandt, sind hierüber Aufzeichnungen aufzubewahren zum Nachweis von Datum, Empfänger und Grund des Versands.

3.14 Der Lieferant hat dafür zu sorgen, dass kein Herunterladen von aufgezeichneten Gesprächen von dem(n) entsprechenden Server(n) auf Desktops/Laptops erfolgt oder ermöglicht wird, es sei denn, der Mitarbeiter ist hierzu in Ausübung seiner Aufgabe berechtigt. Bei Vorliegen einer Berechtigung hat der Berechtigte eine Aufzeichnung anzufertigen. Werden aufgezeichnete Gespräche heruntergeladen, sind die Aufzeichnungen aufzubewahren zum Nachweis für den Grund der Berechtigung, des heruntergeladenen Gesprächs und der Gründe für das Herunterladen. Berechtigte Mitarbeiter und sämtliche Fälle von Nichterfüllung sind regelmäßig zu überprüfen.

4. Arbeitsgeräte

4.1 Der Lieferant hat dafür zu sorgen, dass sämtliche Mitarbeiter über geschützte Bildschirme verfügen, die von außerhalb der abgegrenzten Räume des Kontaktzentrums nicht eingesehen werden können.[8]

4.2 Der Lieferant hat dafür zu sorgen, dass Drucker und Faxgeräte in Sicherheitsbereichen aufgestellt werden, zu denen lediglich berechtigte Personen Zugang haben und nur zu den erforderlichen Zwecken. Die Liste berechtigter Nutzer und die Nutzung der Geräte ist regelmäßig auf ihre Gültigkeit zu überprüfen. Ausdrucke sind sicher aufzubewahren je nach Art der Klassifizierung der Information und Handhabungsvorschriften und dürfen nur mit Genehmigung von BT aus dem Kontaktzentrum entfernt werden.

4.3 Der Lieferant hat dafür zu sorgen, dass Ausdrucke und Kopien nur mit einer Nutzer-ID und einem Sicherheitscode angefertigt werden, damit eine Überprüfung und Protokollierung zu Kontrollzwecken möglich ist.

4.4 Der Lieferant hat dafür zu sorgen, dass Aktenvernichter mit Partikelschnitt und plombierbare Abfallbehälter dort bereit gestellt werden, wo Drucker und Faxgeräte aufgestellt werden. Aktenvernichter und Abfallbehälter sind regelmäßig zu leeren und ihr Inhalt ist sicher zu entsorgen.

4.5 Der Lieferant hat dafür zu sorgen, dass sämtliche Informationen auf Ausdrucken sicher entsorgt werden, durch Zerkleinern oder Einlegen in plombierbare Abfallbehälter nach den Bestimmungen in Kapitel 4.4.

4.6 Der Lieferant hat dafür zu sorgen, dass sämtliche Gegenstände, die Mitarbeiter zu Beginn ihres Arbeitsverhältnisses erhalten, bei ihrem Ausscheiden aus dem Kontaktzentrum oder bei Ende des BT/EE-Vertrags zurückgegeben / entfernt werden. Eine Bestandsliste über die Gegenstände ist anzulegen.[9]

4.7 Der Lieferant hat dafür zu sorgen, dass zurückgegebene oder entfernte Gegenstände im Sinne der einschlägigen Bestimmungen hierzu sicher entsorgt werden.[10]

[8] Siehe Umsetzungsmatrix mit Beispielen zu 'Bildschirmschutz'.
[9] Siehe Umsetzungsmatrix mit Beispielen zum Inhalt der Bestandsliste über Gegenstände.
[10] Siehe Umsetzungsmatrix mit Beispielen zu den Anforderungen an eine sichere Entsorgung.

5. Systemzugang

5.1 Zum Schutz von Kundendaten müssen Mitarbeiter bei Zugriff auf Kundenkonten / Kundendaten ihre Nutzer-ID aufzeichnen und den Grund den Zugriff angeben. Ein Zugriff darf nur nach Genehmigung des Systembesitzers oder des Vorgesetzten möglich sein. Darüber hinaus ist ein Zugriff auf Kundenkonten nur zu gestatten, wenn dies für die Funktion des Mitarbeiters erforderlich ist. Ferner muss der Zugriff auf das für die Ausübung der Aufgaben erforderliche Maß beschränkt werden. Mitarbeiter, die keinen Zugang in die BT- und/oder EE-Systeme zum Einblick in Aufzeichnungen von Kundendaten benötigen, dürfen keine Erlaubnis hierzu erhalten.

5.2 Zugriffe 'nur zur Ansicht' sind zu unterbinden, es sei denn, sie sind aus betrieblichen Gründen erforderlich. Genehmigte Zugriffe 'nur zur Ansicht' sind zu protokollieren und zu überwachen, um unsachgemäße Nutzung zu verhindern.

5.3 Der Lieferant hat dafür zu sorgen, dass Mitarbeiter keine Zugangsberechtigung zum Internet, zu privaten oder außerbetrieblichen E-Mail-Konten, sozialen Netzwerken (wie z.B. Facebook) oder sonstigen Kommunikationsinstrumenten wie Messenger oder Communicator haben, es sei denn, dies wird von BT genehmigt und ist zur Ausübung der Funktionen des Mitarbeiters erforderlich.

5.4 Der Lieferant hat dafür zu sorgen, dass sämtliche Textnachrichten, die aus seinen Systemen gesendet werden, protokolliert und überwacht werden. Bei Textübertragungen sind Aufzeichnungen zum Nachweis über den Zeitpunkt, des(r) Empfänger und den Grund des Versands aufzubewahren.

5.5 Der Lieferant hat dafür zu sorgen, dass nur vorab genehmigte Instrumente für den Remotezugang zu Kundengeräten zu Supportzwecken und nur von Mitarbeitern, zu deren Aufgaben der Remotezugang gehört, verwendet werden. Die Zugangsberechtigungen sind im Abstand von 3 Monaten zu überprüfen und zu widerrufen, wenn diese Aufgabe für die Funktionen des Mitarbeiters nicht mehr erforderlich ist. Es sind Konzepte vorzusehen, um unzulässige Instrumente für den Remotezugang zu erkennen.[11]

5.6 Der Lieferant darf Remotezugänge auf betriebliche E-Mail-Konten von Mitarbeitern des Kontaktzentrums oder sonstiger Systeme für den Zugriff auf Aufzeichnungen zu Kundendaten nicht gestatten.

5.7 Der Lieferant hat dafür zu sorgen, dass Mitarbeiter einen 'schreibgeschützten' Zugang nur zu freigegebenen Laufwerken, die von BT und/oder EE geliefert und geführt werden, haben. Andere freigegebene Laufwerke dürfen im Kontaktzentrum nicht benutzt werden. Das Herunterladen, Kopieren, Löschen oder Verändern von Kundeninformationen von sämtlichen BT und/oder EE-Systemen, Applikationen oder Datenbanken ist untersagt.

6. Aufzeichnung von Telefonaten

6.1 Der Lieferant hat dafür zu sorgen, dass sämtliche Telefonate mit Kunden aufgezeichnet werden. Der Lieferant hat dafür zu sorgen, dass die Aufzeichnungen von Telefonaten (Sprache

[11] Siehe Umsetzungsmatrix mit Beispielen zur Erkennung von Instrumenten für Remotezugang.

und Bildschirm) während der Übertragung vom PC Desktop auf Server für Gesprächsaufzeichnungen geschützt sind.[12]

6.2 Der Lieferant hat dafür zu sorgen, dass Gesprächsaufzeichnungen sicher gespeichert werden, insbesondere, wenn Informationen zu Geldkarten (PCI) enthalten sind, um dem Verlust oder unbefugten Gebrauch dieser Daten vorzubeugen. Daten zu Geldkarten müssen verschlüsselt werden und zum Schutz ist ein Schlüsselverwaltungsverfahren einzurichten, das die hierfür geltenden besten Praktiken berücksichtigt. BT und/oder EE dürfen die Verfahren und Vorgänge zur Verschlüsselung und geschützten Speicherung in zeitlichen Abständen überprüfen um deren Angemessenheit und Geeignetheit festzustellen.

7. Kundenauthentifizierung

7.1 Der Lieferant muss für ein genehmigtes Verfahren zur Kundenauthentifizierung bei eingehenden und ausgehenden Telefonaten sorgen. [13]

7.2 Der Lieferant muss garantieren, dass PIN oder Passwörter, die Kunden zum Nachweis ihrer Identität angeben nicht für andere Mitarbeiter des Kontaktzentrums sichtbar sind, zum Beispiel durch Schutzvorrichtungen für Bildschirme oder räumliche Trennung.

7.3 Der Lieferant hat dafür zu sorgen, dass die Kundenauthentifizierung automatisiert stattfindet, ohne Bekanntgabe der vollständigen PIN oder des vollständigen Passworts gegenüber dem Mitarbeiter, z.B. mittels eines Systems, bei dem nach dem Zufallsprinzip Ziffern / Buchstaben des Passworts abgefragt werden, wie 1., 3. und 5. Stelle. BT und/oder EE können das Kundenauthentifizierungsverfahren in zeitlichen Abständen im Hinblick auf die Einhaltung der vorliegenden Bestimmungen überprüfen.

7.4 Der Lieferant hat dafür zu sorgen, dass ein Zurücksetzen von PIN oder Passwörtern bei Kunden, die diese vergessen haben, erst nach Prüfung von zusätzlichen Authentifizierungsmerkmalen erfolgt.[14]

7.5 Der Lieferant hat dafür zu sorgen, dass die Systeme zum Zurücksetzen von PIN oder Passwörtern von Kundenkonten automatisch arbeiten und keine Beteiligung eines Mitarbeiters des Kontaktzentrums erfordern.

7.6 Der Lieferant muss dafür sorgen, dass neue PIN oder Passwörter mit Hilfe eines automatisierten Systems erstellt werden und direkt an den Kunden geschickt werden, als Text oder E-Mail ohne die Beteiligung eines Mitarbeiters.

7.7 Der Lieferant muss dafür sorgen, dass das Zurücksetzen von Passwörtern oder PIN durch den Kunden selbst durchgeführt werden kann, entweder online oder mittels interaktiver Sprachantwort (IVR).

7.8 Der Lieferant hat auch dafür zu sorgen, dass ein Verfahren zur Zurücksetzung von Einstellungen mit Hilfe eines Mitarbeiters verfügbar ist, das es Kunden ermöglicht, ihre PIN oder ihr Passwort mit Hilfe eines Mitarbeiters des Kontaktzentrums zurückzusetzen. Es darf nur eine beschränkte Anzahl von Mitarbeitern geben, die das Zurücksetzen von PIN oder Passwörtern durchführen.[15]

---

[12] Siehe Umsetzungsmatrix mit Beispielen zum Schutz bei Übertragungen von Gesprächsaufzeichnungen.
[13] Siehe Umsetzungsmatrix mit Beispielen zum Inhalt von Kundenauthentifizierungsverfahren.
[14] Siehe Umsetzungsmatrix mit Beispielen zum Inhalt von zusätzlichen Merkmalen zur Kundenauthentifizierung.
[15] Siehe Umsetzungsmatrix mit Beispielen zum Verfahren beim Zurücksetzen von Einstellungen mit Hilfe von Mitarbeitern.

7.9 Der Lieferant hat auf Anforderung ein Prüfprotokoll über Fälle vorzulegen, in denen PIN und Passwörter von Kunden zurückgesetzt wurden, sowie das dazu eingesetzte System (online, IVR oder Hilfe durch Mitarbeiter) und welcher Mitarbeiter den jeweiligen Fall bearbeitet hat.

8. Datenschutz

Neben obligatorischen Schulungen von BT zu Sicherheit und Datenschutz (siehe Anhang 2), die jeder Mitarbeiter des Lieferanten zu absolvieren hat und deren Verständnis er zu erklären hat, sind folgende Bestimmungen zu beachten:

8.1 Der Lieferant hat dafür zu sorgen, dass Mitarbeiter im Kontaktzentrum auf einfache Weise Zugang zu relevanten und anzuwendenden Sicherheits- und Datenschutzinformationen erhalten, auf der Startseite der Intranet-Home-Page (oder, falls kein Intranet besteht, durch E-Mails zu Aktualisierungen und Schulungen).

8.2 Der Lieferant muss alle Mitarbeiter im Kontaktzentrum durch regelmäßige Erinnerungsmitteilungen mindestens zwei Mal im Jahr auf positive Verhaltensweisen und unterstützende gute Praktiken zur Sicherheit unterrichten.

9. Überwachung

9.1 Der Lieferant muss die wöchentliche Überwachung von Telefonaten (eingehende und ausgehende) im Hinblick auf die ‘Qualitätskontrolle’ durch Vorgesetzte / Führungskräfte veranlassen, um neben der Einhaltung weiterer Vorgaben zu garantieren, dass die Kundenauthentifizierung korrekt durchgeführt wird.[16]

9.2 Der Lieferant hat dafür zu sorgen, dass Telefonate als ‘fehlgeschlagene Telefonate’ qualifiziert werden wenn das korrekte Kundenauthentifizierungsverfahren nicht eingehalten wird. Im Anschluss an jedes fehlgeschlagene Telefonat muss der Lieferant ein Nachbereitungsverfahren bereithalten, das die Mitarbeiter des Kontaktzentrums an ihre Pflicht zur korrekten Authentifizierung und/oder sicheren Aufbewahrung von Passwörtern (falls erforderlich) erinnert.

9.3 Der Lieferant muss ein prüfbares Verfahren bereit halten für den Fall, dass ein Mitarbeiter des Kontaktzentrums wiederholt ‘fehlgeschlagene Telefonate’ vorweist und bei Durchführung der korrekten Kundenauthentifizierung Fehler auftreten. Dabei sind auch die Folgen für den Mitarbeiter zu bestimmen, der wiederholt bei der korrekten Kundenauthentifizierung oder bei korrekten Aufzeichnungen Fehler macht. Diese können zum Nachweis bei der Leistungsbewertung oder in Disziplinarverfahren des Mitarbeiters herangezogen werden.

10. Compliance

10.1 Der Lieferant hat dafür zu sorgen, dass ein prüfbares schriftliches Verfahren eingerichtet wird zur Durchführung und Handhabung regelmäßiger Sicherheitskontrollen in den Betriebseinrichtungen und/oder Stichproben genommen werden, um die Einhaltung der vorliegenden Normen und der Sicherheitsbestimmungen von BT zu überwachen, wie z.B. Rundgänge, sauberer Schreibtisch usw.[17]

[16] Siehe Umsetzungsmatrix mit Beispielen zu den Mindestanforderungen an sämtliche Qualitätskontrollen.
[17] Siehe Umsetzungsmatrix mit Beispielen, was alles zu den Stichproben gehört.

10.2 Der Lieferant hat ein Verfahren einzuführen, bei dem vierteljährliche Überprüfungen auf der Grundlage von Nachweisen (10% der Eingaben) an Mitarbeiter des Kontaktzentrums oder Mitarbeiter von BT und/oder EE weitergeleitet werden um zu gewährleisten, dass Vorauswahlverfahren für Einstellungen und Sicherheitsschulung (als Teil der Einarbeitungsphase) tatsächlich durchgeführt und betrieben werden. So soll dafür gesorgt werden, dass Mitarbeiter im Kontaktzentrum angemessen geprüft werden (im Sinne der Bestimmungen von BT zur Vorauswahl bei Einstellungen) und eine entsprechende Sicherheitsschulung erhalten, damit auf den angemessenen Schutz von sensiblen Kundeninformationen vertraut werden kann.

10.3 Der Lieferant hat ein Verfahren einzuführen, bei dem vierteljährliche Überprüfungen auf der Grundlage von Nachweisen (100% der Eingaben) an Mitarbeiter des Kontaktzentrums oder Mitarbeiter von BT und/oder EE weitergeleitet werden, um zu gewährleisten, dass die jährlichen Pflichtschulungen zu Sicherheit und Datenschutz durchgeführt werden.

10.4 Der Lieferant hat dafür zu sorgen, dass vierteljährliche Anweisungen zur Auffrischung in Bezug auf die Pflichten zu Sicherheit und Datenschutz ergehen. Es sind schriftliche Nachweise zur Teilnahme und zum Verständnis der Mitarbeiter anzufertigen.

10.5 Der Lieferant hat dafür zu sorgen, dass den Mitarbeitern des Kontaktzentrums die wichtigen Bestimmungen, Normen, Leitfäden und Verfahren zugänglich sind, um die Erfüllung vorliegender Bestimmungen und der Sicherheitsanforderungen von BT zu garantieren.

11. Risikoanalyse

Der Lieferant hat dafür zu sorgen, dass eine Risikoanalyse bei Nichterfüllung, Genehmigungen oder besonderen Ausnahmen von den vorliegenden Bestimmungen durchgeführt und schriftlich festgehalten wird, nach den Vorgaben für Risikomanagementverfahren. Die Risikoanalyse muss folgende Angaben enthalten:

- Grund für die Handlung / das Vorgehen und Begründung für die Nichterfüllung der vorgegebenen Bestimmungen;
- Status der Nichterfüllung: dauerhafte oder vorübergehende Nichterfüllung;
- Bei vorübergehender Nichterfüllung ist das Datum anzugeben, an dem Kontrollen eingerichtet werden und das Datum, an dem die Handlung / das Vorgehen abgeschlossen sein wird;
- Die Funktion/Aufgabe des Mitarbeiters ist anzugeben sowie der Grund für die Angemessenheit der Handlung/des Vorgehens (und für den Ausschluss des Kontrollerfordernisses);
- Einsatz von Kontrollen zur Risikominderung aus der Handlung/dem Vorgehen;
- Begründung für die Einführung bestimmter Kontrollen und/oder für das Absehen von erforderlichen Kontrollen; und
- Nachweis der Genehmigung durch die Geschäftsleitung.

12. Glossar

Begriff	Erklärung
Kundenkontaktzentrum	Ein Kontaktzentrum (auch Kundeninteraktionszentrum oder E-Kontaktzentrum) ist eine zentrale Stelle in einem Unternehmen, von dem aus sämtliche Kundenkontakte geführt werden. Das Kontaktzentrum umfasst typischerweise ein oder mehrere Online Call Center, kann aber ebenso

	andere Arten von Kundenkontakt einschließen, wie E-Mail-Newsletter, Postversand für Kataloge, Umfragen auf Webseiten und Chats sowie die gesamten Informationen über Kunden zu deren Online-Einkäufen. Ein Kontaktzentrum ist in der Regel Teil einer umfassenden Kundenpflege, dem sogenannten Kundenbeziehungsmanagement (CRM).
Schließfächer	Das Personal in den Räumen des Kontaktzentrums darf an den jeweiligen Arbeitsplätzen keine persönlichen Gegenstände bei sich führen, die geeignet sind, Kundeninformationen aufzuzeichnen, wie zum Beispiel Mobiltelefone. Solche Geräte sind in Schließfächern (entsprechend gekennzeichnet) außerhalb der Räume des Kontaktzentrums aufzubewahren.
Beschäftigte(r)	Beschäftigter ist eine Person, die im räumlichen Bereich des Kontaktzentrums arbeitet, einschließlich fest angestellter Beschäftigter des Lieferanten, vorübergehend Beschäftigte, Mitarbeiter der Agentur, Auftragsnehmer und Arbeiter.
Begleitung	Im Rahmen eines formellen Besucherverfahrens ist sicher zu stellen, dass Besucher von Kontaktzentren ständig begleitet werden, damit diese sich nicht verirren oder in Bereiche gelangen, zu denen ihnen der Zutritt verwehrt ist.
Umsetzungsmatrix	Anliegende Matrix legt die Mindestanforderungen an die Ergebnisse und Bestimmungen für den Lieferanten fest, die bei der Umsetzung bestimmter Verfahren, Vorgaben oder Vorgehensweisen nach den Anforderungen zu beachten sind.
Unbeaufsichtigte Arbeiten	Es ist festzulegen, dass unbeaufsichtigtes Arbeiten im Kontaktzentrum außerhalb der üblichen Arbeitszeiten nur mit Genehmigung der Leitung zulässig ist. Davon sind auch Reinigungskräfte und sonstige Personen wie Wartungspersonal erfasst.
Microsoft Office Applikationen	Microsoft Office Applikationen beinhalten Word, PowerPoint, Excel, Outlook und OneNote, sind aber nicht auf diese beschränkt. Um die Datenausschleusung zu verhindern dürfen Kundenkontakte über Onlinesysteme nicht auf diesen Applikationen gespeichert werden (ausgenommen bei Genehmigung), da Informationen hieraus leicht kopiert und extrahiert werden können.
Persönliche Gegenstände	Jeder persönliche Gegenstand, der geeignet ist, Kundeninformation zu erfassen / aufzuzeichnen - einschließlich, aber nicht beschränkt auf: Mobiltelefone, Smartwatches, iPods, iPads, Kameras, USB-Sticks, Stifte und Papier.
Zugangskontrollen	Zugangskontrollen hängen davon ab, wo sich die Räume des Kontaktzentrums befinden. Die Zugangskontrollen können technischer Art sein (z.B. Magnetkarte, Tastenfeld, biometrische Identifikation) oder ein bestimmtes Verfahren erfordern (z.B. Schlüssel mit einem prüfbaren Abmeldeverfahren oder ein Anmeldeverfahren, bei dem am Eingang eine Personenkontrolle durchgeführt wird). Die Art der Zugangskontrolle ist auf die jeweiligen Bereiche abzustimmen.
Objekt	Objekt im Sinne des vorliegenden Dokuments ist jedes Objekt, das geeignet ist, Kundendaten oder Informationen zu verarbeiten oder zu speichern.

Abgrenzung	Abgrenzung im Sinne des vorliegenden Dokuments bedeutet, dass andere Geschäftsbereiche Unterhaltungen nicht mithören und Informationen nicht erkennen können. Es ist eine räumliche Trennung einzurichten (Wände, separate Gebäude usw.) mit Zugangskontrollen zu den jeweiligen Bereichen.
Sicherheitsvorfall	Ein Sicherheitsvorfall liegt vor bei einer Änderung des gewöhnlichen Geschäftsbetriebs, durch die die Vertraulichkeit, Vollständigkeit oder Verfügbarkeit von Daten betroffen wird unter der Vermutung eines möglichen Verstoßes gegen Sicherheitsvorgaben, -regeln /-anforderungen oder eines Ausfalls von Schutzmaßnahmen. Einige Beispiele: Systemmissbrauch, unbefugter Zugang, Verlust / Diebstahl von Geräten und Infizierung durch Schadsoftware.
Genehmigung der Geschäftsleitung	Werden Ausnahmen für bestimmte Anforderungen erforderlich, sind die Risiken der Umstände zu bewerten und durch eine Person zu genehmigen, die in dem betroffenen Arbeitsbereich die verantwortliche Leitung innehat.
Systembesitzer	Der offizielle Verantwortliche für die gesamte Beschaffung, Entwicklung, Integration, Modifizierung, Betrieb und Wartung eines Informationssystems.
Drängeln	Drängeln liegt vor, wenn eine Person einer anderen so dicht folgt, dass sie eine kontrollierte Zugangstür oder -schranke passiert, dabei die eigene Zugangskarte nicht benutzt und so in den genehmigungspflichtigen Bereich der Geschäftsräume des Lieferanten gelangt, in dem Geschäftstätigkeiten von BT/EE ausgeführt werden. Eingeschlossen sind auch unbefugte Personen, denen auf diese Weise Zugang ermöglicht wird.
Vorläufige Sicherheitsausweise	Vorläufige Sicherheitsausweise sind im Rahmen eines prüfbaren Verfahrens (wie Buch, Protokoll oder Arbeitsblatt) auszustellen. Alle ausgestellten vorläufigen Sicherheitsausweise sind aufzuzeichnen unter Angabe von Ausstellungsdatum, Name, Abteilung, Telefonnummer und Ausstellungsgrund, Name des Gastgebers und Datum der Rückgabe. Für Ausweise, die nicht zurückgegeben werden, ist ein eigenes Verfahren vorzusehen.
Nutzer-ID	Zur Nutzung von Druckern und Faxgeräten in den Räumen des Kontaktzentrums ist die Eingabe einer ID und Sicherheits-Code-Nr. erforderlich, so dass die Nutzung für den jeweiligen Nutzer überprüft werden kann. Beschäftigte müssen die Nutzer-ID bei Zugang zu Kundenkonten / Aufzeichnungen nach Kapitel 5.1 eingeben.

KITE-PROJEKT: Umsetzungsmatrix für Lieferanten im Hinblick auf Anforderungen an Kontaktzentren.

Aufstellung Referenz	**Allgemeine Angaben**	**Mindestergebnisse, die als Erfüllung anerkannt werden.**
1.2	Prüfbares Zugangsverfahren	Ein Arbeitsblatt oder ein Datenblatt mit Namen und detaillierten Angaben zum Zeitpunkt der Erteilung der Zugangsberechtigung, Grund für die Berechtigung, Datum des Entzugs der Berechtigung, Grund für den Entzug etc.
2.1	Leichte Erkennung	Mitarbeiter, denen aufgrund ihrer Funktionen der Gebrauch von Mobiltelefonen, Laptops, iPads, Tablets gestattet ist, sollen leicht erkennbar sein und haben zu diesem Zweck Umhängebänder in anderen Farben oder sonstige Objekte zur Unterscheidung zu tragen.
2.4	Besucherprotokolle	Folgende Angaben sind aufzuzeichnen: i) Name des Besuchers, ii) Organisation, iii) Datum und Uhrzeit des Ein- und Ausgangs, iv) Zweck des Besuchs, v) Name der besuchten Person, vi) Kennzeichen des Fahrzeugs, das auf das Firmengelände gelangt, vii) Mobiltelefonnummer, viii) Nummer des Besucherausweises.
3.5	Private Notfälle	Es ist ein System einzurichten, das den Kontakt von Angehörigen oder Freunden mit dem Mitarbeiter ermöglicht bei privaten Notfällen. Das Kontaktsystem kann in der Nutzung einer bestimmten Nummer der Telefonzentrale oder der Nummer eines Vorgesetzten, die als zentrale Kontaktstelle dient, bestehen.
3.7	Sichere Aufbewahrung oder Entsorgung	Macht ein Mitarbeiter im Rahmen seiner Funktionen Aufzeichnungen, sind diese sicher aufzubewahren bzw. zu entsorgen. Dies kann beispielsweise durch Aktenvernichter, besondere (eventuell plombierbare) Abfallbehälter und/oder Aufbewahrung in eigens dafür vorgesehenen Räumen, die die Mitarbeiter abschließen können, erfolgen.
3.7	Saubere Schreibtische	Sämtliches Material ist sofort nach Gebrauch sicher aufzubewahren oder zu entsorgen und am Ende des Arbeitstags darf kein Material auf dem Schreibtisch zurückgelassen werden. Mitarbeiter werden regelmäßig überprüft. Es ist ein Disziplinarverfahren vorzusehen bei Verstößen gegen diese Bestimmungen.

3.10	Prüfung von Whiteboards/Papier	Im Hinblick auf das Verfahren in Kapitel 3 sind Aufzeichnungen anzufertigen (z.B. Arbeitsblatt) zum Nachweis der Durchführung der Überprüfungen und zur Sicherstellung der Erfüllung der Anforderungen.
4.1	Bildschirmschutz	Es ist dafür zu sorgen, dass Personen, die sich im Kontaktzentrum aufhalten und nicht entsprechend berechtigt sind, nicht die Bildschirme der Mitarbeiter im Kontaktzentrum einsehen und Informationen lesen (wie Reinigungskräfte und Wartungspersonal). Kundendaten auf Computerbildschirmen müssen durch entsprechende Ausrichtung des Monitors oder durch Sichtschutz vor Einblick geschützt werden.
4.6	Bestandsverzeichnis	Alle Gegenstände, die Mitarbeiter im Rahmen ihrer Aufgaben besitzen, wie Sicherheitsausweise, Schließfachschlüssel, Laptops, Desktops und Remotezugriffsinstrumente sind in ein Bestandsverzeichnis aufzunehmen, das für Kontrollzwecke zu führen ist. Verlässt ein Mitarbeiter seine Arbeitsstelle oder das Kontaktzentrum, ist ein Verfahren vorzusehen, um unverzüglich Maßnahmen einzuleiten, um alle Zugangseinrichtungen zu entfernen und sonstige Gegenstände, Schlüssel und Sicherheitsausweise zurück zu erhalten. Das Bestandsverzeichnis ist Teil der Checkliste für „ausscheidende Mitarbeiter“ zum Ende ihres Arbeitsverhältnisses.
4.7	Sichere Entsorgung	Werden Gegenstände zum Ende ihrer Nutzung entsorgt, ist eine geeignete Software wie ‘Tabernus’ oder ‘Blanco’ einzusetzen, um die endgültige (soweit erheblich) Löschung vertraulicher Kundeninformationen nach den von BT und/oder EE vorgegebenen Standards zu garantieren. Ist die sichere Löschung von Daten durch die genannte Software nicht möglich, ist das Gerät zu zerstören in einem von BT und/oder EE genehmigten Verfahren. Zu diesem Zweck kann eine Sicherheitsperson von BT und/oder EE herangezogen werden. Nach Löschung sämtlicher vertraulicher Kundeninformationen kann das Gerät anderweitig eingesetzt oder entsorgt werden.
5.5	Instrumente für den Remotezugriff	Zur Vermeidung unbefugter Zugriffe auf Kundendaten ist ein Verfahren einzurichten, das den Remotezugriff nur mit zuvor von BT und/oder EE genehmigten Instrumenten für den Zugriff auf Kundengeräte garantiert. Zur Identifizierung nicht genehmigter Remotezugriffsinstrumente ist ein Verfahren einzurichten, das regelmäßig überprüft wird um sicher zu stellen, dass solche Instrumente nicht eingesetzt werden können und/oder eingesetzt wurden. Außerdem ist der Einsatz von genehmigten Remotezugriffsinstrumenten nur von hierzu entsprechend befugten Personen zulässig und die Genehmigung hierzu in einem formellen Verfahren

		zu erteilen, in dem auch eine Risikoanalyse nach den Anforderungen an Remotezugriffen vorzunehmen ist.
6.1	Übertragung von Gesprächsaufzeichnungen	Aufzeichnungen von Kundengesprächen müssen verschlüsselt vom PC auf die Server für Gesprächsaufzeichnungen übertragen werden. Die Verschlüsselung muss sowohl die Sprachaufzeichnung als auch Bildschirmdetails enthalten.
7.1	Kundenauthentifizierung	Alle Mitarbeiter haben das von BT/EE vorgegebene Verfahren zur Kundenauthentifizierung durchzuführen, um sicher zu stellen, dass es sich um den gewünschten Kunden handelt. Dieses Verfahren wird Lieferanten und Mitarbeitern gesondert erläutert und kann je nach Aufgabe(n)und Leistung(en) des Kontaktzentrums variieren.
7.4	Zusätzliche Authentifizierungskontrollen	Mitarbeiter haben vor einer Änderung von PIN oder Passwort eines Kunden immer dafür zu sorgen, dass der Gesprächspartner ausreichende Angaben macht, um sich zu vergewissern, dass es sich tatsächlich um den Kunden handelt, indem sie bestimmte Sicherheitsfragen stellen zur Identität, durch Fragen nach dem Namen und der Anschrift, welche Kontoaktivitäten zuletzt durchgeführt wurden, den Betrag der letzten Rechnung oder seit wann die Person Kunde von BT oder EE ist. Diese Angaben sind lediglich Beispiele, die Aufstellung ist nicht abschließend.
7.8	Zurücksetzen von Einstellungen mit Hilfe von Mitarbeitern	Wenn Kunden nicht in der Lage sind, ihre PIN oder das Passwort online oder mittels interaktiver Sprachantwort (IVR) zurückzusetzen, muss es möglich sein, dies mit Unterstützung eines Mitarbeiters des Callcenters durchzuführen. Es ist ein formelles Verfahren vorzusehen um sicher zu stellen, dass das Zurücksetzen von Einstellungen nur von einer begrenzten Anzahl von Mitarbeitern durchgeführt wird und Sicherheitsvorkehrungen getroffen werden, um Mitarbeiter, die Kunden PIN oder Passwörter zurücksetzen dürfen, von anderen Mitarbeitern im Kontaktzentrum räumlich zu trennen und entsprechenden Kontrollen zu unterziehen. Die Aufstellung der Genehmigung erteilenden Mitarbeiter ist regelmäßig zu überprüfen, um festzustellen, ob eine Genehmigung noch erforderlich ist und ist mit der erforderlichen Diskretion zu benutzen.
9.1	Qualitätskontrolle von Telefonaten	Leitende Mitarbeiter müssen Qualitätskontrollen durchführen, einschließlich der wöchentlichen Prüfung einer zufälligen Auswahl von Kundentelefonaten (Anrufe von Kunden und Anrufe bei Kunden), die von Mitarbeitern geführt wurden, sowie einer monatlichen Kontrolle aller Aufnahmen und der durch den Lieferanten eingeführten Verfahren. Dadurch wird garantiert, dass der Lieferant vorgenannte Anforderungen erfüllt und insbesondere, dass Mitarbeiter das korrekte

		Kundenauthentifizierungsverfahren anwenden und die Aufnahmen entsprechend speichern.
10.1	Stichproben zur Einhaltung von Vorgaben	Es ist ein prüfbares Verfahren einzurichten um die Einhaltung von Sicherheitsnormen in den Geschäftseinrichtungen und Stichproben zu prüfen. Sowohl der Lieferant als auch BT und / oder EE können jederzeit Stichproben zur Prüfung der Einhaltung der Vorgaben nehmen. Stichproben-Prüfungen umfassen folgende Punkte, sind jedoch nicht auf diese beschränkt: • Sicherheits-ID / Sicherheitsausweis • Sauberer Schreibtisch / Sauberer Bildschirm • Nutzung von Schließfächern • Persönliche mobile Endgeräte • Nutzung von Whiteboards • Löschen und Entsorgung von vertraulichen gedruckten Informationen oder als Fax • Kundenauthentifizierung • Qualitätskontrolle von Telefonaten • Prüfprotokolle über das Zurücksetzen von Passwörtern • Nutzung von Textnachrichten • Einhaltung von Vorgaben zu Datenschutz und Sicherheitstraining Sämtliche Prüfungen von Stichproben müssen detailliert beschreiben, wie im Fall von Abweichungen oder Nichterfüllung vorzugehen ist. Sämtliche Pläne zur Mängelbeseitigung, die von BT und/oder EE angefordert werden, sind vollständig durchzuführen.