Westconnect GmbH

Brüsseler Platz

45131 Essen

Anforderungen der Informationssicherheit & Technisch-organisatorische Maßnahmen

Änderungshistorie

Datum	Version	Erstellt durch	Beschreibung der Änderung
1.06.2026	0.9	DWB-G-G/V	initiale Erstellung
01.08.2026	1.0	DSB; CISO; DWB-G-G/V	nach Rücksprache mit Fachabteilung Freigabe und Aktivierung durch GF

Vorbemerkung: Dieses Dokument verwendet überwiegend die männliche Sprachform zur besseren Lesbarkeit. Dies dient lediglich der sprachlichen Vereinfachung und soll keinesfalls diskriminierend wirken. Die gewählte Formulierung schließt alle Geschlechter ein und soll gleichermaßen für alle gelten. Unsere Organisation fördert die Gleichstellung aller Geschlechter und respektiert Vielfalt in jeder Form. Wir sind bestrebt, einen inklusiven und diskriminierungsfreien Sprachgebrauch zu gewährleisten.

Inhaltsverzeichnis

Geltungsbereich

Dieses Dokument beschreibt die grundlegenden Anforderungen an die Informationssicherheit, sowie die technischen und organisatorischen Maßnahmen zum Datenschutz, die vom LIEFERANTEN, der mit WESTCONNECT zusammenarbeitet, einzuhalten sind. Damit soll ein grundlegendes Verständnis der Anforderungen von WESTCONNECT an Informationssicherheit und Datenschutz geschaffen werden. Das Dokument stellt sicher, dass die LIEFERANTEN mit dem Rahmenwerk für Informationssicherheit und dem Datenschutzmanagementsystem von WESTCONNECT im Einklang stehen und alle Daten von WESTCONNECT während der gesamten Dauer ihrer Zusammenarbeit schützen, einschließlich der Wahrung der Vertraulichkeit aller Daten von WESTCONNECT.

Zusätzlich zu diesen Anforderungen können je nach Vertragsgegenstand weitere Kontrollen erforderlich sein, die vom LIEFERANTEN erfüllt und als Anhang vereinbart werden müssen.

1 Anforderungen an die Informationssicherheit

Die folgenden Anforderungen an die Informationssicherheit gelten für die Erbringung von Dienstleistungen durch den LIEFERANTEN und die Organisation des LIEFERANTEN.

1.1 Organisatorische Maßnahmen

1.1.1 Sicherheits-Governance

Der LIEFERANT richtet ein Rahmenwerk für die Informationssicherheit ein und pflegt und überwacht es, welches dem Leitungsgremium des LIEFERANTEN ermöglicht, klare Vorgaben für die Informationssicherheit und das Risikomanagement festzulegen und sein Engagement in diesem Bereich zu demonstrieren.

1.1.2 Informationsrisikomanagement

Der LIEFERANT stellt sicher, dass

- vor der Implementierung neuer Systeme, die WESTCONNECT-Informationen einschließlich personenbezogener Daten (im Folgenden als „WESTCONNECT-Informationen" bezeichnet) erstellen, verarbeiten, speichern, übertragen oder vernichten,
- vor der Implementierung wesentlicher Änderungen an bestehenden Systemen, die sich auf die Erstellung, Verarbeitung, Speicherung, Übertragung oder Vernichtung von WESTCONNECT-Informationen auswirken, und
- vor der Einführung neuer Technologien, die damit verbundenen Informationssicherheitsrisiken identifiziert, bewertet, behandelt, überwacht und in Abstimmung mit WESTCONNECT innerhalb akzeptabler Grenzen gehalten werden. Die Informationen im Zusammenhang mit Risikomanagementaktivitäten werden WESTCONNECT unverzüglich mitgeteilt.

1.1.3 Sicherheitsmanagement

Der LIEFERANT

- hat eine spezielle Funktion für Informationssicherheit eingerichtet, die mit ausreichenden Befugnissen und Ressourcen ausgestattet ist, um sicherzustellen, dass bewährte Verfahren für die Informationssicherheit im gesamten Unternehmen wirksam und einheitlich angewendet werden und dass die Einhaltung der gesetzlichen und vertraglichen Anforderungen in Bezug auf die Informationssicherheit gewährleistet ist.
- unterhält ein umfassendes, kontinuierliches Programm zur Sensibilisierung für Sicherheitsfragen, um das erwartete Sicherheitsverhalten bei allen Personen, die Zugang zu WESTCONNECT-Informationen haben, zu fördern und zu verankern.

1.1.4 Compliance-Management

Der LIEFERANT stellt sicher, dass alle Systeme, die WESTCONNECT-Informationen erstellen, verarbeiten, speichern, übertragen oder vernichten, regelmäßig auf die Einhaltung der eigenen Sicherheitsrichtlinien/-standards des LIEFERANTEN und der Anforderungen von WESTCONNECT

überprüft werden. Die Sicherheitsrichtlinien/-standards des LIEFERANTEN werden WESTCONNECT vor dem Datum des Inkrafttretens, sowie auf Anfrage von WESTCONNECT zur Verfügung gestellt. Abweichungen zwischen den eigenen Sicherheitsrichtlinien/-standards des LIEFERANTEN und den grundlegenden und spezifischen Anforderungen von WESTCONNECT an die Informationssicherheit werden WESTCONNECT vom LIEFERANTEN unverzüglich mitgeteilt.

Die eigenen Sicherheitsrichtlinien/-standards des LIEFERANTEN müssen abgebildet werden und mit den in Abschnitt „3 Zertifizierungen und Nachweise zur Informationssicherheit“ dieses Dokuments genannten Zertifikaten übereinstimmen. Die Zuordnung zwischen den digitalen Ressourcen, die zur Erstellung, Verarbeitung, Speicherung, Übertragung oder Vernichtung von WESTCONNECT-Informationen verwendet werden, den entsprechenden Kontrollen gemäß Abschnitt 3 dieses Dokuments und den Sicherheitsrichtlinien/-standards des LIEFERANTEN muss in einem Compliance-Prüfbericht enthalten sein. Der LIEFERANT stellt diesen Bericht WESTCONNECT auf Anfrage zur Verfügung.

1.1.5 Sicherheit in der Lieferkette

Der LIEFERANT stellt sicher, dass er Informationsrisiken in jeder Phase der Beziehungen zu seinen externen Lieferanten entlang der gesamten Lieferkette identifiziert und verwaltet, indem er

- die Informationssicherheitsanforderungen gemäß Abschnitt 1.1.4 dieses Dokuments in formelle Verträge aufnimmt und
- sicherstellt, dass diese erfüllt werden;
- sicherstellt, dass Subunternehmer, die an der Erstellung, Verarbeitung, Speicherung, Übertragung oder Vernichtung von WESTCONNECT-Informationen beteiligt sind, mindestens die in diesem Dokument vereinbarten Anforderungen erfüllen.

Der LIEFERANT gewährleistet eine angemessene Steuerung aller Subunternehmer sowie die Einhaltung ausgelagerter Kontrollen.

1.1.6 Asset Management

Der LIEFERANT richtet einen umfassenden Prozess zum Asset Management ein und pflegt diesen, um alle für die Lieferung von Dienstleistungen und Produkten an WESTCONNECT relevanten Informationswerte zu identifizieren, zu klassifizieren, zu verwalten und zu schützen. Dazu gehören Hardware, Software, virtuelle Infrastruktur, Daten und cloudbasierte Ressourcen, die zur Erstellung, Speicherung, Verarbeitung, Übertragung oder Vernichtung von WESTCONNECT-Informationen verwendet werden. Alle Assets müssen in einem aktuellen Assetverzeichnis erfasst werden, das Angaben zu Eigentumsverhältnissen, Klassifizierung, Standort und Lebenszyklusstatus enthält. Der LIEFERANT weist klare Eigentumsverhältnisse zu und stellt sicher, dass für jedes Asset Verantwortlichkeiten für die Informationssicherheit definiert und durchgesetzt werden. Der Asset Managementprozess muss anerkannten Standards (z. B. ISO/IEC 27001, ISO/IEC 27002) entsprechen und regelmäßig überprüft und aktualisiert werden.

1.1.6.1 Sichere Vernichtung und Wiederverwendung

Aufgrund ihrer Klassifizierung und Kritikalität müssen Assets, die zur Erstellung, Speicherung,

Verarbeitung, Übertragung oder Vernichtung von WESTCONNECT-Informationen verwendet werden, angemessen geschützt und sicher vernichtet oder sicher wiederverwendet werden. Der LIEFERANT muss Verfahren für die sichere Stilllegung, Vernichtung oder Bereinigung von Assets implementieren, um unbefugten Zugriff auf WESTCONNECT-Informationen zu verhindern, indem er modernste Technologien und Verfahren einsetzt. Informationen über eine solche sichere Vernichtung und Löschung werden WESTCONNECT unverzüglich mitgeteilt, Nachweise hierfür werden WESTCONNECT auf Anfrage vorgelegt.

1.1.6.2 Seriöse Quellen

Der LIEFERANT stellt sicher, dass Assets nur aus bekannten, seriösen und überprüfbaren Quellen bezogen werden und dass eine zuverlässige technische Unterstützung, Wartung und eine rückverfolgbare Lieferkette vorhanden sind. Die Verwendung von nicht überprüften oder nicht unterstützten Quellen ist verboten, sofern dies nicht ausdrücklich von WESTCONNECT geprüft und genehmigt wurde.

1.2 Sicherheit im Personalwesen

Der LIEFERANT stellt sicher, dass alle Mitarbeiter, die Zugang zu Systemen, Daten oder Dienstleistungen im Zusammenhang mit WESTCONNECT haben, vor ihrer Einstellung einer angemessenen persönlichen Identitätsprüfung unterzogen werden.

Der LIEFERANT führt Kontrollen durch, um den Missbrauch von Zugriffsrechten oder Berechtigungen durch Personen in seiner Verantwortung zu verhindern. Der Zugriff auf Systeme und Informationen muss streng nach dem Prinzip des minimalen Zugangs und der geschäftlichen Notwendigkeit gewährt werden.

Der LIEFERANT stellt sicher, dass Zugriffsrechte bei Beendigung des Arbeitsverhältnisses, Wechsel der Funktion oder Neuzuweisung von Verantwortlichkeiten unverzüglich widerrufen werden.

Darüber hinaus stellt der LIEFERANT sicher, dass nur Mitarbeiter, die nachweislich für ihre jeweiligen Aufgaben qualifiziert und entsprechend geschult sind, mit der Erbringung von Dienstleistungen im Zusammenhang mit WESTCONNECT beauftragt werden. Die Einhaltung dieser Anforderungen muss durch dokumentierte Prozesse unterstützt werden und regelmäßigen internen Überprüfungen unterliegen.

1.3 Physische Sicherheit

Der LIEFERANT muss geeignete Vorkehrungen für die physische Sicherheit und den Zugangsschutz treffen. Insbesondere müssen Maßnahmen zum

- Schutz vor Feuer und Wasser,
- Schutz vor oder Vermeidung von extremen Temperaturen (Klimatisierung),
- Schutz vor Stromausfall,
- Schutz vor physischen Schäden durch Naturkatastrophen,
- Schutz vor unbefugtem Zutritt.

Der Zugang zu Bereichen mit Informationen oder Systemen, die WESTCONNECT-Informationen erstellen, verarbeiten, speichern, übertragen oder vernichten oder Prozesse unterstützen, die die

Sicherheit von WESTCONNECT-Informationen beeinträchtigen, muss auf eine autorisierte Personengruppe beschränkt sein (Minimaler Zugang). Dazu gehören auch Zugangsschutzmaßnahmen für Rechenzentren, einschließlich der Überwachung kritischer Bereiche, Zugriffsprotokolle, Zugang für externe Mitarbeiter nur in Begleitung und Sicherheitsmaßnahmen gegen Eindringen.

1.4 Technologische Kontrollen

Der LIEFERANT betreibt Systeme auf konsistente Weise, die Informationen von WESTCONNECT erstellen, verarbeiten, speichern, übertragen oder vernichten. Dies dient dem Schutz der Informationen von WESTCONNECT und der betriebenen Systeme von vor Fehlfunktionen, Cyberangriffen, unbefugter Offenlegung, Beschädigung, Diebstahl und Verlust, um die Anforderungen von WESTCONNECT hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen.

1.4.1 Technisches Systemmanagement

Der LIEFERANT verwaltet die Sicherheit der Systeme unter Berücksichtigung der Sicherheitsanforderungen von WESTCONNECT. Dies kann (unter anderem) durch folgende Maßnahmen erreicht werden

- technische Überwachung gemäß vereinbarten Service Level Agreements,
- Anwendung eines (Sicherheits-)Incident- und Changemanagement Prozesses und
- Durchführung von Backups und Wiederherstellungstests für wichtige Informationen und Software.

Der LIEFERANT hat die Verantwortlichkeiten und Verfahren für die Verwaltung und den Betrieb seiner Dienste dokumentiert, um sicherzustellen, dass diese Dokumentation

- den anerkannten Industriestandards und Best Practices entsprechen
- ordnungsgemäß schriftlich dokumentiert und
- während der Laufzeit dieser Vereinbarung jederzeit auf dem neuesten Stand sind. Die Dokumentation der Betriebsverfahren ist WESTCONNECT auf Anfrage unverzüglich zur Verfügung zu stellen.

1.4.2 Lifecycle Management

Der LIEFERANT implementiert und pflegt einen formellen Lifecycle Managementprozess für alle digitalen Dienste, Systeme und Komponenten, die WESTCONNECT bereitgestellt werden. Dazu gehört, dass sichergestellt wird, dass alle Hardware-, Software- und Drittanbieterabhängigkeiten vom Hersteller oder Anbieter unterstützt werden, regelmäßig aktualisiert werden und nicht ohne einen von WESTCONNECT unterzeichneten und genehmigten Risikominderungsplan auslaufen (EOL) oder nicht mehr unterstützt werden (EOS). Lieferanten müssen proaktiv die rechtzeitige Aktualisierung oder den Austausch von Technologien planen, um Betriebs- und Sicherheitsrisiken im Zusammenhang mit veralteten Komponenten zu vermeiden. Alle Änderungen im Lifecycle (einschließlich Veralterung, Aktualisierungen oder wesentliche Änderungen) müssen WESTCONNECT im Voraus mitgeteilt und in Abstimmung mit den Produkt-/Dienstleistungsinhabern von WESTCONNECT verwaltet werden. Altsysteme dürfen nur mit der dokumentierten Genehmigung von WESTCONNECT verwendet werden und müssen gemäß den oben

beschriebenen Anforderungen von WESTCONNECT zur Risikominderung gesichert werden.

1.4.3 Identitäts- und Zugriffsmanagement

1.4.3.1 Verwaltung von Identitäten

Der LIEFERANT implementiert und pflegt robuste Identitätsmanagementpraktiken, um sicherzustellen, dass alle Benutzer- und Systemidentitäten eindeutig identifizierbar, sicher authentifiziert und entsprechend ihren Rollen und Verantwortlichkeiten angemessen autorisiert sind. Identitäts- und Zugriffsmanagementprozesse (IAM) müssen die Grundsätze des minimalen Zugangs und der Aufgabentrennung durchsetzen.

Der LIEFERANT überprüft und aktualisiert regelmäßig die Zugriffsrechte und widerruft den Zugriff sofort bei Rollenänderungen oder Kündigungen. Als bewährte Vorgehensweise wird dem LIEFERANT empfohlen, einen Zero-Trust-Ansatz für das Identitätsmanagement zu verfolgen, bei dem alle Identitäten, ob intern oder extern, als nicht vertrauenswürdig behandelt werden, bis sie ausdrücklich überprüft und kontinuierlich validiert wurden. Für alle privilegierten Zugriffe und Fernzugriffe müssen starke Authentifizierungsmechanismen (z. B. Multi-Faktor-Authentifizierung) verwendet werden. Ereignisse im Identitätslebenszyklus müssen überprüfbar sein und in die allgemeine Sicherheits-Governance des LIEFERANTEN integriert werden.

1.4.3.2 Zugriffskontrolle

Der LIEFERANT beschränkt den Zugriff auf Assets, auf denen WESTCONNECT-Informationen erstellt, verarbeitet, gespeichert oder übertragen werden, auf autorisierte Personen, die diese für bestimmte geschäftliche Zwecke benötigen.

Dies umfasst mindestens, dass

- Zugriffsrechte auf genehmigte Systemfunktionen und autorisierte Benutzer beschränkt (Minimaler Zugang) sind mit angemessener Aufgabentrennung, und auf eine minimale Anzahl von Benutzern beschränkt.
- Zugriffsrechte nicht kollektiv (gemeinsam genutzte Funktions-IDs) oder zwischen Benutzern geteilt werden.

Der LIEFERANT stellt sicher, dass der administrative Zugriff auf Systeme, die WESTCONNECT-Informationen erstellen, verarbeiten, speichern oder übertragen,

- immer protokolliert wird, um die Erkennung und Untersuchung von unbefugtem Zugriff und unbefugter Manipulation zu ermöglichen.
- durch ein Multi-Faktor-Authentifizierungsverfahren geschützt sind oder, wenn eine Multi-Faktor-Authentifizierung technisch nicht möglich ist, durch gleichwertige Sicherheitsmaßnahmen.

Der LIEFERANT überprüft regelmäßig (mindestens einmal jährlich), ob die zugewiesenen Zugriffsrechte noch erforderlich sind, und dokumentiert die Überprüfung.

1.4.4 Netzwerk und Kommunikation

Der LIEFERANT, der Zugriff auf die Systeme, Daten oder Netzwerke von WESTCONNECT hat oder WESTCONNECT-Informationen erstellt, verarbeitet, speichert oder überträgt, muss robuste Netzwerksicherheitskontrollen implementieren und aufrechterhalten, um vor unbefugtem Zugriff, Datenverletzungen und Dienstunterbrechungen zu schützen. Der LIEFERANT ist mindestens verpflichtet, Firewalls, Funktionen zur Erkennung und Abwehr von Eindringlingen, eine sichere Netzwerksegmentierung und verschlüsselte Kommunikation (z. B. TLS 1.3 oder höher) zu verwenden. Die Netzwerkinfrastruktur muss kontinuierlich überwacht, regelmäßig aktualisiert und getestet werden, um Schwachstellen zu erkennen und zu beheben. Der Fernzugriff muss durch Multi-Faktor-Authentifizierung (MFA) und VPNs oder gleichwertige sichere Kanäle gesichert werden. Alle Sicherheitsvorfälle oder -verletzungen müssen WESTCONNECT unverzüglich gemeldet werden.

1.4.4.1 Fernzugriff und mobiles Arbeiten

Mobiles Arbeiten von Mitarbeitern des LIEFERANTEN mit Zugriff auf WESTCONNECT-Informationen muss WESTCONNECT im Voraus gemeldet werden (allgemein, nicht für einzelne Mitarbeiter) und darf nur unter der Voraussetzung erfolgen, dass die Mitarbeiter geschult wurden und sich schriftlich zur Einhaltung der Datenschutz- und Betriebsvorschriften verpflichtet haben. Der LIEFERANT stellt seinen Mitarbeitern hierfür Software und Hardware zur Verfügung, die nur für geschäftliche Zwecke genutzt werden darf oder eine wirksame Trennung von geschäftlichen und privaten Daten unterstützt (z. B. Containerlösungen). Vertrauliche Informationen sind vor dem Zugriff durch Dritte zu schützen und dürfen nur in den Räumlichkeiten des LIEFERANTEN entsprechend ihrer Vertraulichkeitsstufe entsorgt werden. Bei der Vernichtung vertraulicher Informationen ist das gleiche Sicherheitsniveau zu gewährleisten. Das gleiche Sicherheitsniveau ist bei der Erbringung der Dienstleistung im mobilen Einsatz sicherzustellen. Das Mithören und Mitlesen durch Unbefugte muss ausgeschlossen sein. Der LIEFERANT stellt WESTCONNECT auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Vorgaben für den mobilen Einsatz erforderlich sind.

1.4.4.2 Trennung von Entwicklungs-, Test- und Produktionssystemen

Produktionsdaten sind in Entwicklungs- und Testumgebungen nicht zulässig. Personenbezogene Daten (PII) müssen in Entwicklungs- und Testumgebungen anonymisiert werden.

Der LIEFERANT stellt sicher, dass Entwicklungs-, Test- und Produktionssysteme zumindest logisch voneinander getrennt sind, um das Risiko eines unbefugten Zugriffs oder einer unbefugten Änderung an produktiven Systemen zu verringern. Entwicklungs-, Test- und Produktionssysteme müssen getrennte Benutzer-IDs verwenden.

1.4.5 Sicherheitsmaßnahmen

Der LIEFERANT setzt Endpoint Protection- und Eventmanagementlösungen auf Systemen und für diese ein, auf denen WESTCONNECT-Informationen Bedrohungen ausgesetzt sein können. Dazu gehören Server, Endbenutzer- Geräte und Bürogeräte (sofern zutreffend).

Endpoint Protectionsoftware sollte vor allen Formen von Malware schützen und automatisch verteilt und aktualisiert werden.

Der LIEFERANT stellt sicher und überwacht kontinuierlich, dass

- die Malware-Schutzsoftware nicht deaktiviert oder in ihrer Funktionalität eingeschränkt wurde,
- die Konfiguration der Malware-Schutzsoftware korrekt ist,
- Updates innerhalb festgelegter Zeiträume korrekt durchgeführt werden,
- Scans zu festgelegten Zeiten durchgeführt werden und identifizierte Malware-Vorfälle angemessen gemeldet werden.

1.4.5.1 Schwachstellen Management

Der LIEFERANT richtet ein umfassendes technisches Schwachstellen Managementprogramm für alle von ihm betriebenen Systeme und Anwendungen ein und pflegt dieses, um eine zeitnahe Identifizierung, Bewertung und Behebung von Sicherheitslücken zu gewährleisten. Dazu gehören das regelmäßige Scannen, Überwachen und Patchen der eigenen Infrastruktur in Übereinstimmung mit den Best Practices der Branche und den relevanten Bedrohungsinformationen.

Darüber hinaus ist der LIEFERANT verpflichtet, sich gegebenenfalls aktiv am technischen Schwachstellenmanagementprozess von WESTCONNECT zu beteiligen. Für Systeme und Dienste, die ausschließlich für WESTCONNECT betrieben werden, werden Schwachstellenscans durch interne Prozesse von WESTCONNECT durchgeführt. Der LIEFERANT stellt sicher, dass diese Systeme für Scans vollständig zugänglich sind, und behebt identifizierte Schwachstellen umgehend gemäß den von WESTCONNECT definierten Kriterien, wie in der Cybersicherheitsrichtlinie „Technisches Schwachstellenmanagement" festgelegt.

1.4.5.2 Aktuelle Patch-Level

Der LIEFERANT betreibt in Abstimmung mit dem jeweiligen Ansprechpartner bei WESTCONNECT einen Patch-Management-Prozess, der sicherstellt,

- Patches aus autorisierten Quellen zu identifizieren und zu beschaffen, sobald sie verfügbar sind,
- Patches in einem Testsystem zu testen,
- dass Patches zeitnah bereitgestellt werden,
- die Anwendung von Patches zu dokumentieren.

1.4.5.3 Härtung

Der LIEFERANT stellt sicher, dass alle Systeme, in denen Informationen von WESTCONNECT erstellt, verarbeitet, gespeichert oder übertragen werden, gemäß den bewährten Verfahren der Branche gehärtet sind.
Dazu gehört

- die Deaktivierung unnötiger Anwendungen, Dienste, Tools, Protokolle und Schnittstellen,
- das Löschen oder zumindest Ändern der vom Hersteller bereitgestellten Standardbenutzerkonten und -kennwörter,
- die Aktivierung von Optionen zur Verbesserung der Sicherheit und
- die Verhinderung der Übertragung technischer Informationen an externe Stellen.

1.4.5.4 Protokollierung von Sicherheitsereignissen, Überwachung und Event Management

Der LIEFERANT implementiert und unterhält geeignete Protokollierungs- und Überwachungsmechanismen, um sicherheitsrelevante Ereignisse in allen Systemen, Anwendungen und Diensten, die zur Erstellung, Verarbeitung, Speicherung, Übertragung oder Weitergabe von WESTCONNECT-Informationen verwendet werden, jederzeit zu erfassen. Die Protokolle müssen mindestens Authentifizierungsversuche, Berechtigungserweiterungen, Konfigurationsänderungen, Statusänderungen und den Zugriff auf sensible Daten enthalten. Diese Protokolle müssen zeitlich synchronisiert, vor unbefugtem Zugriff und unbefugten Änderungen geschützt und mindestens 180 Tage lang aufbewahrt werden, sofern nicht durch geltendes Recht oder vertragliche Verpflichtungen etwas anderes vorgeschrieben ist. Der LIEFERANT überwacht die Protokolle aktiv auf ungewöhnliche Aktivitäten und Anzeichen für Kompromittierungen und stellt sicher, dass Sicherheitsvorfälle gemäß einem dokumentierten Incident-Management-Prozess rechtzeitig identifiziert, priorisiert, eskaliert und behoben werden. Hochriskante Vorfälle, die die Vertraulichkeit, Integrität oder Verfügbarkeit von WESTCONNECT-Informationen oder -Diensten beeinträchtigen, müssen WESTCONNECT unverzüglich, spätestens jedoch 24 Stunden nach ihrer Entdeckung, gemeldet werden. Darüber hinaus stellt der LIEFERANT sicher, dass jede Art von forensischer Analyse/Aktivität, die Systeme betrifft, die WESTCONNECT-Informationen erstellen, speichern, verarbeiten oder übertragen, auf Wunsch gemeinsam mit einem Mitarbeiter der WESTCONNECT-Cybersicherheit durchgeführt wird, um das Vier-Augen-Prinzip zu erfüllen.

1.4.5.5 Verschlüsselung

Der LIEFERANT muss starke Verschlüsselungsmechanismen implementieren, um die Vertraulichkeit und Integrität von WESTCONNECT-Informationen sowohl im gespeicherten Zustand als auch während der Übertragung zu schützen. Daten während der Übertragung müssen mit branchenüblichen Protokollen wie TLS 1.3 verschlüsselt werden. Daten im Ruhezustand müssen mit Algorithmen und Schlüssellängen verschlüsselt werden, die anerkannten Standards (z. B. AES-256) entsprechen und den aktuellen Best Practices der Branche entsprechen. Kryptografische Schlüssel müssen gemäß einem dokumentierten Schlüsselverwaltungsprozess sicher generiert, gespeichert, verwaltet und rotiert werden. Schlüssel müssen vor unbefugtem Zugriff geschützt und ihr Lebenszyklus durch sichere Schlüsselverwaltungssysteme verwaltet werden. Der Lieferant darf keine veralteten oder unsicheren kryptografischen Algorithmen, Protokolle oder Konfigurationen verwenden. Ausnahmen von den Verschlüsselungsanforderungen müssen, sofern vorhanden, formell dokumentiert, einer Risikobewertung unterzogen und schriftlich von WESTCONNECT genehmigt werden.

1.4.5.6 Sicherer Softwareentwicklungs-Lebenszyklus

Für alle Software, die WESTCONNECT-Informationen erstellt, verarbeitet, speichert, überträgt oder vernichtet, richtet der LIEFERANT einen sicheren Softwareentwicklungs-Lebenszyklus (SSDLC) ein und pflegt diesen, der Sicherheitsprinzipien und -kontrollen in allen Phasen der Softwareentwicklung integriert, einschließlich Design, Entwicklung, Test, Bereitstellung und Wartung. Der SSDLC muss mit anerkannten Industriestandards und -rahmenwerken (z. B. OWASP, ISO/IEC 27034, NIST SP 800-218) übereinstimmen und muss risikobasierte Bedrohungsmodellierung, sichere Codierungspraktiken, Codeüberprüfungen und Sicherheitstests (z. B. statische und dynamische Analyse, Penetrationstests) umfassen. Entwickler müssen regelmäßig in sicheren Codierungstechniken, einschließlich aktueller Sicherheitsbedrohungen, geschult werden. Alle identifizierten Schwachstellen müssen nachverfolgt, anhand des Risikos priorisiert und innerhalb festgelegter Fristen behoben werden. Der LIEFERANT stellt sicher, dass Komponenten und Bibliotheken von Drittanbietern regelmäßig auf Schwachstellen überprüft und auf dem neuesten Stand gehalten werden. Die Verwendung unsicherer oder nicht unterstützter Komponenten ist untersagt, sofern dies nicht ausdrücklich von WESTCONNECT nach einem dokumentierten Risikoakzeptanzprozess genehmigt wurde. Gleiches gilt für erworbene Software.

1.5 Künstliche Intelligenz

Die Verwendung von Technologien der künstlichen Intelligenz muss vor ihrer Nutzung durch WESTCONNECT genehmigt werden. Dies umfasst unter anderem

- den Einsatz von KI-Technologien in Produkten und Dienstleistungen,
- die Verwendung von WESTCONNECT-Daten zu Schulungszwecken.

Der LIEFERANT muss WESTCONNECT vor der Verwendung von KI-Technologien informieren.

2 Datenschutzanforderungen

2.1 Verpflichtung zur Vertraulichkeit

Der LIEFERANT verpflichtet alle Mitarbeiter, die personenbezogene Daten von WESTCONNECT verarbeiten oder Zugriff hierauf haben, schriftlich zur Vertraulichkeit beim Umgang mit personenbezogenen Daten.

Sofern auftragsbezogen oder gesetzlich erforderlich, verpflichtet der LIEFERANT die Mitarbeiter darüber hinaus schriftlich auf das Fernmeldegeheimnis (gemäß ePrivacy-Richtlinie oder -Verordnung in ihrer jeweils gültigen Fassung in Verbindung mit nationalen Vorschriften zum Fernmeldegeheimnis, z.B. § 3 TDDDG für Deutschland).

Der LIEFERANT schult alle Mitarbeiter, die personenbezogene Daten von WESTCONNECT verarbeiten oder Zugriff hierauf haben, in Bezug auf Datensicherheit und Datenschutz. Die Teilnahme wird namensscharf dokumentiert.

2.2 Datenschutz durch Technikgestaltung

Der LIEFERANT trifft Regelungen zum „Datenschutz durch Technikgestaltung“, um das Recht auf Datenschutz bei der Entwicklung und Gestaltung von Produkten, Diensten und Anwendungen zu berücksichtigen (z. B. durch Maßnahmen wie Datenminimierung, Pseudonymisierung, datenschutzfreundliche Voreinstellungen).

2.3 Datenschutzbeauftragter

Gemäß den gesetzlichen Anforderungen (Artikel 37 bis 39 EU-DSGVO und nationales Recht) wird ein Datenschutzbeauftragter benannt.

Es bestehen für den Datenschutzbeauftragten keine Interessenkonflikte. Der Datenschutzbeauftragte verfügt über die für das Unternehmen erforderliche Qualifikationen und Zuverlässigkeit.

Die Geschäftsleitung unterstützt den Datenschutzbeauftragten. Der Datenschutzbeauftragte ist der Geschäftsleitung direkt unterstellt und berichtet direkt an diese. Der Datenschutzbeauftragte wird bei der Planung neuer Verfahren oder der Änderung bestehender Verfahren rechtzeitig informiert und einbezogen. Der Datenschutzbeauftragte gestaltet die Verfahrenskonzeption aktiv mit.

2.4 Datenschutz-Managementsystem

Der LIEFERANT hat ein Datenschutz-Managementsystem eingerichtet, das den Anforderungen der DSGVO entspricht und einem kontinuierlichen Prüf- und Verbesserungsprozess unterliegt.

Im Hinblick auf die Verarbeitung personenbezogener Daten wird eine Risikoanalyse nach festgelegten und nachvollziehbaren Kriterien durchgeführt und darauf aufbauend Informationssicherheits- und Datenschutzrisiken in einem verbindlich festgelegten und kontinuierlichen Prozess identifiziert, bewertet, angemessen behandelt und die Wirksamkeit der Maßnahmen im Rahmen regelmäßiger interner Audits überprüft.

Mindestens einmal jährlich wird ein Datenschutzbericht über den aktuellen Stand der Wirksamkeit des Datenschutz-Managementsystems sowie etwaige Störungen oder datenschutz-/sicherheitsrelevante Ereignisse erstellt und auf Anfrage zur Verfügung gestellt.

Die Geschäftsleitung ist in eine Informationssicherheits- und Datenschutz-Organisation sowie entsprechende Kommunikations-, Eskalataions- und Entscheidungsprozesse ausreichend informiert eingebunden und stellt sicher, dass die Aufgaben und Verpflichtungen im erforderlichen Umfang und ausreichender Qualität durchgeführt werden können.

Für die Einrichtung, Implementierung, Durchführung, Überwachung, Überprüfung, Aufrechterhaltung und Verbesserung des Datenschutz-Managementsystems werden nachweislich ausreichende Ressourcen zur Verfügung gestellt.

Es wird sichergestellt, dass beim Betrieb des Datenschutz-Managementsystems nur Personal zum Einsatz kommt, dass über ausreichende Fähigkeiten zur Wahrnehmung der zugewiesenen Aufgaben verfügt. Dies wird durch Schulungen und andere Fortbildungsmaßnahmen sichergestellt.

Unabhängig von IT-Sicherheits- und Risikobewertungen werden regelmäßig interne Audits zum in Bezug auf den Stand des Datenschutzes durchgeführt. Diese lassen Abweichungen zwischen dem vertraglich festgelegten Datenschutzniveau (Gesamtheit aller vereinbarten technischen und organisatorischen Maßnahmen) und dem Ist-Zustand des Datenschutzes erkennen, die dann im Hinblick auf das daraus resultierende Risiko bewertet und auf Anfrage zur Verfügung gestellt werden können.

Nach Datenschutzmanagement-Audits wird ein Maßnahmenplan erstellt, der erkennen lässt, mit welchen Maßnahmen und in welcher angemessenen Frist die festgestellten Deltas beseitigt werden. Dieser kann auf Anfrage zur Verfügung gestellt werden.

Die kontinuierliche Verbesserung des Datenschutz-Managementsystems basiert auf dem Plan-Do-Check-Act-Zyklus. Sind dedizierte Ressourcen von WESTCONNECT oder Mehrmandanten-Ressourcen von Verbesserungsmaßnahmen betroffen, informiert der LIEFERANT WESTCONNECT vor der Umsetzung dieser Maßnahmen. Das Datenschutz-Managementsystem wird durch interne und externe (Revisions-)Prüfungen auf seine Wirksamkeit getestet.

3 Zertifizierungen und Nachweise zur Informationssicherheit

Der LIEFERANT hält die relevanten, international anerkannten Informationssicherheitsstandards ein, die der Art und Kritikalität der angebotenen Dienstleistungen und Produkte angemessen sind, und weist deren Einhaltung nach.

Vom LIEFERANTEN wird mindestens erwartet, dass er die gleichwertige Umsetzung von Informationssicherheitsmanagementprozessen nachweist, vorzugsweise durch eine gültige ISO/IEC 27001-Zertifizierung oder einen aktuellen AICPA SOC2 Typ II-Bericht. Der LIEFERANT legt auf Anfrage aktuelle Nachweise für solche Zertifizierungen vor, einschließlich Auditberichten, Zertifizierungsumfängen und Plans zur Behebung von Nichtkonformitäten. Der LIEFERANT stellt sicher, dass die „Anwendbarkeitserklärung" alle Hosting- und Betriebsanlagen, Anwendungen und Prozesse abdeckt, in denen WESTCONNECT-Informationen erstellt, verarbeitet, gespeichert, übertragen oder entsorgt werden. Gegebenenfalls können zusätzliche Zertifizierungen vereinbart werden, wie z. B. ISO/IEC 27017/27018 oder die Einhaltung von Rahmenwerken wie dem NIST Cyber Security Framework. (CSF)

Liegt keine formelle Zertifizierung vor, muss der Lieferant eine alternative Bewertung der Sicherheit durch Dritte, unabhängige Audits oder detaillierte Selbstbewertungen bieten, die einer Überprüfung und Genehmigung durch WESTCONNECT unterliegen. WESTCONNECT stellt eine Cybersicherheits-Sicherheitsplattform zur Verfügung, die zur Durchführung einer solchen detaillierten Selbstbewertung genutzt werden kann. Der Lieferant muss WESTCONNECT unverzüglich über den Verlust oder die Aussetzung relevanter Zertifizierungen oder wichtige Auditergebnisse informieren.

4 Informations- und Cybersicherheits-Prozessschnittstellen

Der LIEFERANT benennt eine bestimmte Person als zentralen Ansprechpartner für alle Fragen im Zusammenhang mit Informations- und Cybersicherheit. Dieser Sicherheitskontakt muss über die entsprechenden Qualifikationen und Befugnisse verfügen, um Sicherheitsthemen zu koordinieren, Sicherheitsanfragen zu beantworten und Prozesse zur Bearbeitung von Vorfällen zu unterstützen. Der LIEFERANT stellt eine zeitnahe und zuverlässige Kommunikation über diesen Ansprechpartner sicher, auch bei Sicherheitsvorfällen oder Eskalationen. Je nach Art, Kritikalität und Risikograd der bereitgestellten Dienstleistungen oder Produkte können die Parteien vereinbaren, regelmäßige Sicherheits-Compliance-Meetings einzurichten, um relevante Sicherheitskontrollen, Auditergebnisse, offene Befunde, die Historie von Vorfällen und geplante Verbesserungen zu überprüfen. Die Häufigkeit und der Umfang solcher Meetings werden gemeinsam festgelegt und als Teil des Lieferantenmanagement- oder Governance-Prozesses dokumentiert.

Darüber hinaus kann der LIEFERANT zusätzliche Ansprechpartner benennen, die mindestens die folgenden Sicherheitsthemen abdecken:

- IT-Security Incident Management und Verletzungen des Schutzes personenbezogener Daten
- Verwaltung von Schwachstellen
- Patch-Management
- Identitäts- und Zugriffsmanagement

Wenn kein spezifischer WESTCONNECT-Sicherheitskontakt definiert ist, ist WESTCONNECT CERT der primäre Ansprechpartner (cert@westconnect.com). Beide Parteien vereinbaren, im Rahmen der oben genannten Sicherheitsprozesse zusammenzuarbeiten und Informationen auszutauschen.

5 Auditrechte

WESTCONNECT und jede Regulierungsbehörde sowie andere Stellen, die zur Auditierung und Inspektion von WESTCONNECT selbst berechtigt sind, sind berechtigt, jährlich (nicht beschränkt auf ereignisbezogene Audits) Audits beim Lieferanten durchzuführen, um die Einhaltung der Bedingungen dieser Vereinbarung und des geltenden Rechts durch den Lieferanten und die Dienstleistungen zu überprüfen. Dies umfasst das Recht, zu überprüfen und zu kontrollieren, ob

- die beauftragte Datenverarbeitung in Übereinstimmung mit den geltenden Datenschutzgesetzen, den Bestimmungen dieser Vereinbarung und den vereinbarten WESTCONNECT-Vertrags- und Leistungsbeschreibungen durchgeführt wird,
- die Dienstleistungen in Übereinstimmung mit den Anforderungen an die Informationssicherheit, den Lizenzanforderungen und dem dienstleistungsbezogenen internen Überwachungssystem erbracht werden.

WESTCONNECT ist berechtigt, die vorgenannten Audits auch unter Einsatz von Audit-Software und anderen Reporting-Tools und/oder unter Beauftragung Dritter durchzuführen.

6 Besondere Verpflichtungen für Callcenter

Sofern der LIEFERANT Callcenter-Dienstleistungen erbringt, hat er zusätzlich die folgenden technischen und organisatorischen Maßnahmen umzusetzen.

6.1 Der Zutritt zu den Räumlichkeiten des LIEFERANTEN, die zur Leistungserbringung gegenüber WESTCONNECT verwendet werden, ist auf die zur Leistungserbringung erforderlichen Personen beschränkt.

6.2 Originaldokumente, die WESTCONNECT-Informationen enthalten, werden durch die den Prozess verantwortlich leitenden Personen an die zur Leistungserbringung eingesetzten Personen herausgegeben und von diesen nach Arbeitsschluss wieder entgegengenommen.

6.3 Die Client-Systeme der für den LIEFERANTEN bei der Leistungserbringung beschäftigten Personen sind so gestaltet, dass der Zugang zum Internet auf das zur Leistungserbringung erforderliche Maß beschränkt ist. Insbesondere ist der Zugang zu über das Internet angebotenen Diensten Dritter, insbesondere Übersetzungsdienste, Speicherdienste oder Web-Mailer technisch unterbunden.

6.4 Die den bei der Leistungserbringung beim LIEFERANTEN beschäftigten Personen auf den Client-Systemen bereitgestellten Applikationen sind auf das erforderliche Maß beschränkt. Es ist, neben der ggf. vom LIEFERANTEN in Absprache mit WESTCONNECT zur Leistungserbringung eingesetzten Software, keine Applikation verfügbar, über welche, WESTCONNECT-Informationen aus den Systemen von WESTCONNECT übernommen und unbefugt weitergeben werden können (z.B. Snipping Tool).

6.5 Auf den vom LIEFERANTEN zur Leistungserbringung eingesetzten Clients ist durch technische Maßnahmen, wie beispielsweise den Einsatz einer Software zur Schnittstellen-kontrolle oder eine vollständige Deaktivierung der Schnittstellen (insbesondere USB-Ports, Card Reader) die Übertragung von WESTCONNECT-Informationen auf externe Medien technisch grundsätzlich unterbunden. Soweit die Nutzung solcher Schnittstellen und Speichermedien im Einzelfall und nach Absprache mit WESTCONNECT erforderlich ist, werden WESTCONNECT-Informationen lediglich zu den im Einzelfall mit WESTCONNECT abgestimmten Zweck lediglich in gem. Ziffer 1.4.5.5 verschlüsselter Form auf diese Medien und dort gespeichert.

6.6 In den zur Leistungserbringung verwendeten Räumlichkeiten des LIEFERANTEN ist der Zugang zu technischen Einrichtungen, die zur Anfertigung von Kopien geeignet sind (insbesondere Fotokopierer) sowie zu Druckern lediglich nach Maßgabe eines restriktiven und technisch implementierten Zugangskonzepts, z.B. mit einem Zugangscode, und so realisiert, dass der Zugang zu diesen Geräten auf besonders instruierte Mitarbeiter (z.B. Projekt- oder Teamleiter, Führungskräfte) und auf die Erfüllung von deren Aufgaben beschränkt ist.