TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

(FÜR LIEFERANTEN)

Diese technischen und organisatorischen Maßnahmen („**TOMs**“) sind integrierter Bestandteil des zwischen Avaya (einschließlich ihrer weltweiten Konzerngesellschaften) und dem Lieferanten vereinbarten Vertrages/Nachtrags/Anhangs/Anlage/Artikels (oder eines etwaigen anderen gleichwertigen Dokuments) zur Verarbeitung personenbezogener Daten, welcher diese TOMs durch Verweisung einbezieht.

1. Zutrittskontrolle

Der Lieferant gewährleistet durch angemessene Maßnahmen, dass Unbefugten der Zugang zu den Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet oder genutzt werden, verwehrt wird. Dies geschieht jedenfalls durch folgende Maßnahmen:

1.1. Einrichtung einer elektronischen Zugangskontrolle zu Gebäuden, in denen personenbezogene Daten gespeichert sind.

1.2. Einrichtung einer elektronischen Zugangskontrolle für sensible Bereiche innerhalb des Gebäudes, etwa für Datenzentren, Telefonzentralen, LAN-Schränke und Labore.

1.3. Einführung von Richtlinien, um sicherzustellen, dass nur berechtigte Personen Zutritt zu sensiblen Bereichen wie Datenzentren, LAN-Räumen, Telefonschränken und anderen Orten erhalten, an denen personenbezogene Daten verarbeitet werden oder gespeichert sind. Es ist sicherzustellen, dass alle Zutrittsrechte zu diesen Bereichen halbjährlich überprüft werden.

1.4. Erstellung von Zugangsprotokollen, die für mindestens 90 Tage aufbewahrt werden.

1.5. Überwachung und Aufzeichnung von Außenzugangstüren und sensiblen Bereichen und rund um die Uhr durch Überwachungskameras. Aufbewahrung aller Aufnahmen der Überwachungskameras für mindestens 30 Tage.

1.6. Unterhaltung eines aktiv überwachten Alarmsystems, das sensible Bereiche (wie LAN-Räume, Labore und andere Bereiche, in denen personenbezogene Daten verarbeitet werden) physisch sichert.

1.7. Vorhandensein von Sicherheitspersonal an jedem Unternehmensstandort, an dem personenbezogene Daten verarbeitet werden.

1.8. Durchführung eines Prozesses zur Identitätsprüfung vor Erteilung eines Zutrittsausweises.

1.9. Anmeldung von Besuchern und Pflicht zum Tragen eines erkennbaren Besucherausweises. Besucher sind während ihrer Anwesenheit am Standort von Mitarbeitern zu begleiten. Sämtliche Besuchsprotokolle sind mindestens ein Jahr lang aufzubewahren.

1.10. Beschränkung und Kontrolle des Zugangs zu Datenzentren und Medienspeichern, die personenbezogene Daten enthalten, für beauftragte Dritte bzw. freiberuflich tätige Personen wie Sicherheitspersonal oder Hausmeisterdienste.

1.11. Unterhaltung eines dokumentiertes Schlüsselkontrollprogramms mit Hauptschlüsselprotokoll für jeden Standort. Schlüssel zu Schränken in denen personenbezogene Daten verwahrt werden, Geräteräumen und Schaltschränken sind ordnungsgemäß zu verwahren, nur an berechtigte Personen auszugeben und bis zur Rückgabe zu protokollieren.

1.12. Überprüfung von Zugangskontrollaufzeichnungen durch den Administrator auf Alarmaktivitäten, einschließlich durch offen gehaltene oder gewaltsam geöffneten Türen ausgelöste Alarme.

2. Zugangskontrolle

Der Lieferant verhindert durch angemessene Maßnahmen, dass seine Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dies geschieht jedenfalls durch folgende Maßnahmen:

2.1. Vergabe einer eindeutigen Kennung für jeden Nutzer eines Systems (Netzwerk, Server, Datenbank, Anwendung).

2.2. Sicherstellung, dass die Vergabe von Zugangskonten und Privilegien der Zustimmung des Managements bedarf und Überprüfung aller Zugriffsrechte alle sechs Monate.

2.3. Führung und regelmäßige Überprüfung einer Zugangskontrollliste für alle Systeme, die personenbezogene Daten enthalten.

2.4. Verwirklichung des Grundsatzes der geringstmöglichen Rechteeinräumung und des „need to know“ Prinzips bei der Gewährung von Zugangsrechten für Nutzer.

2.5. Durchführung einer Funktionstrennung.

2.6. Festlegung von Prozessen, wonach die Zugangsberechtigung von Nutzern, deren Beschäftigungsverhältnis beim Lieferanten endet (Kündigung, Versetzung etc.), innerhalb von 24 Stunden gesperrt wird.

2.7. Deaktivierung von Benutzerkonten nach 90 Tagen Inaktivität sowie Löschung nach 120 Tagen Inaktivität.

2.8. Sicherstellung der Identitätsprüfung jedes Nutzers bei Logins mittels Passwörtern, Mehrfaktor-Authentifizierung oder biometrischen Daten. Erfolgreiche und fehlgeschlagene Anmeldeversuche sind zu protokollieren und ein Jahr lang aufzubewahren.

2.9. Einrichtung von passwortgeschützten Bildschirmsperre nach mehr als 20-minütiger Inaktivität.

2.10. Sicherstellung, dass Benutzerpasswörter aus mindestens acht Zeichen bestehen und mindestens jeweils ein Zeichen aus drei der vier nachfolgenden Kategorien aufweisen: Großbuchstabe, Kleinbuchstabe, Ziffer und Sonderzeichen.

2.11. Sicherstellung, dass Administrator- und Service-Account-Passwörter sowie Passwörter auf Systemebene aus mindestens 15 Zeichen bestehen und mindestens jeweils ein Zeichen aus allen der nachfolgenden Kategorien aufweisen: Großbuchstabe, Kleinbuchstabe, Ziffer und Sonderzeichen.

2.12. Ablauf von Passwörtern nach jeweils 90 Tagen.

2.13. Sicherstellung, dass sich neue Passwörter von den letzten zehn verwendeten Passwörtern unterscheiden.

2.14. Automatische Sperrung eines Kontos nach fünf fehlgeschlagenen Anmeldeversuchen.

2.15. Zurücksetzung aller voreingestellten Installationspasswörter sowie vom Verkäufer eingestellter Standardpasswörter in sämtlicher neuer Hardware, Systemsoftware und neuen Anwendungen nach der Installation.

2.16. Ausschließliche Speicherung und Übermittlung von Passwörtern in verschlüsseltem Format.

2.17. Durchführung einer sicheren Übermittlung von erstmaligen temporären Passwörtern und Nutzerkennungen. Klartext-Passwörter und Nutzerkennungen dürfen niemals in derselben E-Mail versandt werden.

2.18. Überprüfung der Identität des Nutzers vor Zurücksetzung oder Zuweisung eines Passworts.

2.19. Standardisierung von Server- und Betriebssystem-Builds sowie Einrichtung im Einklang mit Branchenstandards, so dass Widerstandsfähigkeit gegen Angriffe gewährleistet ist.

2.20. Sicherstellen, dass sich Systeme, auf denen personenbezogene Daten gespeichert oder verarbeitet werden, je nach Label- bzw. Klassifikationsebene der auf den Servern gespeicherten Daten auf einem oder mehreren getrennten Netzwerksegmenten befinden, um sicherzustellen, dass nur berechtigte Personen in der Lage sind, mit Systemen, die sie zur Erfüllung ihrer spezifischen Aufgaben benötigen, zu kommunizieren.

2.21. Festlegung eines dokumentierten Patch-Management-Prozesses und Durchführung von Aktualisierungen auf Systemen mit kritischen und risikoreichen Schwachstellen innerhalb von zwei Wochen nach dem Patch-Release sowie innerhalb eines Monats auf allen anderen Systemen. Darüber hinaus ist ein Patch auf Verlangen von Avaya unverzüglich zu korrigieren.

2.22. Installation und Einsatzbereitschaft von Antivirus-Software auf allen Servern und PCs, auf denen personenbezogene Daten verarbeitet werden. Soweit möglich, haben Lieferanten weitergehende Techniken zur Erkennung von Malware zu nutzen (z.B. Scannen von E-Mails und Dateisystemen sowie des Internetverkehrs etc.).

2.23. Mindestens tägliche Aktualisierung von Antivirus-Software. Sie muss in der Lage sein, dringende, außerplanmäßige Signatur-Updates zu unterstützen.

2.24. Konfiguration von Antivirus-Software, so dass Nutzer die Software nicht deaktivieren können.

3. Zugriffskontrolle

Der Lieferant verhindert den Zugriff auf personenbezogene Daten durch unbefugte Personen. Hierfür trifft er dauerhaft angemessene Maßnahmen, die das unbefugte Lesen, Kopieren, Ändern oder Entfernen von Speichermedien, die personenbezogene Daten enthalten, sowie unbefugte Speichereingaben, Lesen, Ändern oder Löschen der gespeicherten personenbezogenen Daten verhindern. Dies geschieht jedenfalls durch folgende Maßnahmen:

3.1. Erstellung einer schriftlichen Richtlinie zur Klassifizierung und Handhabung von Daten sowie eines Verzeichnisses der Datensätze mit Angaben zur Klassifizierung sowie des physischen und elektronischen Speicherorts.

3.2. Der Lieferant hat sicherzustellen, dass personenbezogene Daten bei der Übermittlung nicht mittels veralteter Protokolle verschlüsselt werden (z.B. SSH/SCP/SFTPV2, TLSv1.2 oder höher).

3.3. Der Lieferant stellt eine risikoadequate Verschlüsselung gespeicherter personenbezogener Daten nach dem Stand der Technik sicher. Sämtliche Sicherungskopien von personenbezogenen Daten auf Sicherungsmedien sind zu verschlüsseln.

3.4. Personenbezogene Daten dürfen nur auf PCs, Laptops, Mobilgeräten oder Wechseldatenträgern des Lieferanten gespeichert werden, wenn auf dem betreffenden Gerät eine Festplattenverschlüsselung aktiviert ist.

3.5. Regelmäßige Rotation und Verwaltung von Kodierungsschlüsseln.

3.6. Personenbezogene Daten dürfen nur dann in Entwicklungs-, Test- und / oder Staging-Umgebungen verwendet werden, wenn sie pseudonymisiert sind und Avaya die schriftliche Einwilligung erteilt hat.

3.7. Werden Daten von Kreditkarteninhabern gehandhabt, gespeichert oder auf andere Weise verarbeitet, müssen die Systeme des Lieferanten PCI DSS zertifiziert sein.

4. Weitergabekontrolle

Der Lieferant gewährleistet durch angemessene Maßnahmen, insb. durch sichere Kommunikationskanäle, dass personenbezogene Daten während der Übertragung bzw. des Transports nicht unbefugt gelesen oder modifiziert werden können, und dass sämtliche Übertragungen und Transporte protokolliert werden. Dies geschieht jedenfalls durch folgende Maßnahmen::

4.1. Perimeternetzwerke sind physisch oder logisch von internen Netzwerken, die personenbezogene Daten enthalten, zu trennen.

4.2. Einrichtung von Firewalls zwischen: Internet- und webbasierten Systemen; webbasierten Systemen und Anwendungssystemen; Anwendungssystemen und internen Netzwerken. Bei diesen Firewalls muss es sich um physisch getrennte Geräte handeln.

4.3. Einsatz von Network Intrusion Detection Systemen (IDS) im Rahmen der Netzwerksicherheitsstrategie in Ergänzung der Firewalls. Sämtliche IDS-Protokolle sind regelmäßig zu überwachen, um mutmaßliche Versuche unbefugter Zugriffe auf personenbezogene Daten aufzudecken.

4.4. Firewalls sind mit zustandsorientierter Paketüberprüfung zu verwenden und Firewall-Regeln sind jährlich zu überprüfen.

4.5. Beschränkung und Kontrolle des Zugriffs auf drahtlose Netzwerke durch Wireless-Sicherheitsprotokolle nach dem Stand der Technik, mindestens so sicher wie WPA2.

4.6. Beschränkung und Kontrolle des Netzwerk-Fernzugriffs sowie obligatorische Nutzung von VPN mit Zwei-Faktor-Authentifizierung.

5. Eingabekontrolle

Der Lieferant gewährleistet durch angemessene Maßnahmen, dass er prüfen und feststellen kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht jedenfalls durch folgende Maßnahmen:

5.1. Jede Konfigurationsänderung von Servern, Netzwerken, Datenbanken oder Geschäftsanwendungen, die personenbezogene Daten verarbeiten, sowie Änderungen von personenbezogenen Daten selbst muss protokolliert werden. Durch Prüfprotokolle ist sicherzustellen, dass alle Änderungen einer bestimmten Person zugeordnet werden können. Sie müssen mindestens den Zeitpunkt, das Datum und die Art der Änderung enthalten und sind ein Jahr lang aufzubewahren.

5.2. Prüf-, Änderungs-, Ereignis- und Zugriffskontrollprotokolle sind bei allen Systemen, auf denen personenbezogene Daten verarbeitet werden oder die Verarbeitung gesteuert wird, mittels eines Erhebungsmechanismus nach dem Stand der Technik wie z.B. SIEM aktiv zu überwachen, überprüfen sowie zentral zu aggregieren. Für unbefugten Zugriff und Anomalien sind Alarme einzurichten. Auf Anfrage sind Protokollierungsprüfungen und Anomaliemeldungen vorzulegen.

5.3. Durchführung von Konfigurationsmanagement einschließlich sicherer Baseline-Konfigurationen.

5.4. Überwachung zur Erkennung von unbefugten Änderungen sowie Alarmierung in diesem Fall.

5.5. Es ist sicherzustellen, dass für Notfalländerungen vor der Implementierung die Zustimmung von Führungskräften der entsprechenden Ebene erforderlich ist.

5.6. Die Folgen von Richtlinienverstößen sind klar festzulegen, bekanntzumachen und umzusetzen.

6. Organisationskontrolle

Der Lieferant gewährleistet durch angemessene Maßnahmen, dass seine interne Organisation so eingerichtet ist, dass die spezifischen Anforderungen des Datenschutzes erfüllt werden. Dies geschieht jedenfalls durch folgende Maßnahmen:

6.1. Festlegung einer schriftlichen Datensicherheitsrichtlinie, die jährlich von der Geschäftsleitung des Lieferanten genehmigt wird und allen Beschäftigten des Lieferanten sowie relevanten Dritten bekanntgegeben wird.

6.2. Einrichtung einer dedizierten Sicherheits- und Compliance-Funktion für die Konzeption, die Pflege und den Betrieb von Sicherheitsmaßnahmen zur Unterstützung seiner „Vertrauensplattform“ nach dem Stand der Technik. Diese Funktion bezieht sich auf Systemintegrität, Risikoakzeptanz, Risikoanalyse und -abschätzung, Risikobewertung, Risikomanagement, Risikoumgangserklärungen und Lieferantenmanagement.

6.3. Durchführung regelmäßiger Sicherheitsprüfungen durch unabhängige Dritte und Vorlage von Prüfberichten wie SSAE16 oder ISAE3402.

6.4. Inanspruchnahme der Leistungen branchenweit anerkannter unabhängiger Dritter zur Durchführung von Schwachstellenanalysen und Penetrationstests bei Netzwerken, Systemen, Anwendungen und Datenbanken, auf denen sich gespeicherte, in Übertragung befindliche sowie verwendete personenbezogene Daten befinden. Der Lieferant hat identifizierte Schwachstellen zu prüfen und kritische Schwachstellen innerhalb von vier Wochen nach Patch-Release sowie wesentliche Schwachstellen im Einklang mit üblichen Branchenstandards zu beheben.

6.5. Unterhaltung von Datenschutz-, Sicherheitsbewusstseins- und Compliance-Programmen sowie von Verfahren und Tools zur Datensicherheit und Best Practices. Darüber hinaus müssen Datensicherheitsrichtlinien, Verfahren und Kontrollen zum Schutz personenbezogener Daten bestehen.

6.6. Unterhaltung von Reporting-Richtlinien, Verfahren und Tools, welche die entsprechende Dokumentation sowie Berichte zur Implementierung, Effektivität und, falls nötig, Wiederherstellung geeigneter Sicherheitsvorkehrungen im Zusammenhang mit der Verarbeitung personenbezogener Daten gewähren. Avaya ist auf Anfrage Zugriff darauf zu gewähren.

7. Verfügbarkeitskontrolle

Der Lieferant gewährleistet durch angemessene Maßnahmen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies geschieht jedenfalls durch folgende Maßnahmen:

7.1. Überwachung sicherheitsrelevanter Ereignisse sowie Einrichtung von Melde- und Alarmprozessen auf allen Servern, Netzwerken und in allen Datenbanken, die personenbezogene Daten enthalten.

7.2. Unterhaltung eines Prozesses zur Reaktion auf sicherheitsrelevante Zwischenfälle.

7.3. Unterhaltung von Richtlinien, Verfahren und Tools zur Notfallplanung, die Funktionen und Zuständigkeiten definieren sowie klare Vorgaben und Schulungsmaßnahmen für den ordnungsgemäßen Umgang mit Notfällen bieten. Zu solchen Notfällen zählen insbesondere Naturkatastrophen wie Überschwemmungen, Tornados, Erdbeben, Hurrikane und Schneestürme; Unfälle wie Auslaufen von Chemikalien und mechanische oder elektrische Störungen sowie vorsätzliche Handlungen wie Datenschutz- und Sicherheitsverstöße, Bombendrohungen, Überfälle und Diebstahl.

7.4. Unterhaltung eines Business Continuity/Disaster Recovery-Plans zur Wiederherstellung der für die Leistungen des Lieferanten kritischen Prozesse und Abläufe an den Standorten, von denen aus Leistungen des Lieferanten erbracht werden. Der Lieferant hat außerdem einen jährlich zu testenden Plan vorzuhalten, der dabei hilft, auf eine Katastrophe in geplanter und erprobter Art und Weise zu reagieren.

7.5. Unterhaltung einer redundanten Stromversorgung sowie von Brand- und Rauchmeldern, Feuerlöschanlagen, Generatoren, Kühlsystemen und erhöhten Fußböden in Datenzentren, in denen personenbezogene Daten verarbeitet werden nach dem Stand der Technik.

7.6. Sichere Erstellung vollständiger Backups aller Datenbanken, in denen personenbezogenen Daten gespeichert sind, zur Gewährleistung der Verfügbarkeit entsprechend der der Kritikalität der Daten.

8. Assetkontrolle

Der Lieferant gewährleistet durch angemessene Maßnahmen den Schutz aller Ausrüstung und Anwendungen, die personenbezogene Daten verarbeiten. Dies geschieht jedenfalls durch folgende Maßnahmen:

8.1. Festlegung von Verfahren und Tools zur Identifizierung und Nachverfolgung sämtlicher zur Verarbeitung personenbezogener Daten genutzten Geräte und Medien.

8.2. Übertragung der Verantwortung für sämtliche Geräte und Medien auf eine oder mehrere Aufsichtspersonen.

8.3. Jährliche Durchführung einer umfassenden Kontrolle des Anlagenbestands und Freizeichnung im Hinblick auf Genauigkeit sowie zur Identifizierung fehlender Geräte und Medien.

9. Anwendungskontrolle

Der Lieferant gewährleistet durch angemessene Maßnahmen den Schutz von Anwendungen (Applikationen), welche personenbezogene Daten verarbeiten. Dies geschieht jedenfalls durch folgende Maßnahmen:

9.1. Soweit anwendbar, Durchführung von Penetrationstests, Schwachstellentests an Webanwendungen sowie Minderung hoher Sicherheitsrisiken vor der Veröffentlichung von Anwendungen.

9.2. Mindestens jährliche Durchführung von Penetrationstests an der IT-Umgebung des Lieferanten und Übermittlung der Ergebnisse an Avaya binnen 30 Tagen nach Erhalt der Ergebnisse bzw. Berichte über die von ihm oder seinen Unterauftragsverarbeitern durchgeführten Penetrationstests.

9.3. Soweit Anwendungen zur Verarbeitung personenbezogener Daten zur Erbringung der Leistungen des Lieferanten an Avaya entwickelt werden, ist zu gewährleisten, dass die Entwickler in Best Practices zur sicheren Entwicklung geschult sind.

9.4. Sicherstellung, dass Anwendungen zur Verarbeitung personenbezogener Daten in sicherer Art und Weise entwickelt werden und dabei der formale, dokumentierte Prozess des Lieferanten eingehalten wird, welcher belegt, dass die Anwendung keine Sicherheitsschwachstellen besitzt, wenn sie produktiv verwendet wird. Weiterhin sind mindestens vierteljährlich sowie nach jeder erheblichen Änderung Wiederholungstests durchzuführen. Zu den Schwachstellen von Anwendungen zählen jedenfalls die SANS Top 20 und die OWASP Top 10.

9.5. Sicherheitsschwachstellen von Anwendungen, die personenbezogene Daten betreffen, sind nach ihrer Identifizierung innerhalb angemessener Frist zu beseitigen.

9.6. Validierung der vorgenannten Anforderungen durch Tools wie dynamische Anwendungsprüfung und/oder statische Codeanalyse.

10. Änderungs- und Datentrennungskontrolle

Der Lieferant gewährleistet angemessene Änderungskontrollmaßnahmen für die Verarbeitung personenbezogener Daten. Dies geschieht jedenfalls durch folgende Maßnahmen:

10.1. Einrichtung von Change-Management-Prozessen, welche für alle Änderungen an Systemen, die personenbezogene Daten verarbeiten, die Dokumentation ihres Zwecks, eine Analyse der Auswirkungen auf die Sicherheit, einen Prüfplan und die Testergebnisse sowie ihre angemessene Genehmigung des Managements enthalten.

10.2. Die Konfiguration von Systemen, die personenbezogene Daten verarbeiten, ist vor der Einbindung ins produktive Netzwerk zu validieren.

10.3. Änderungen an Produktionsumgebungen, die personenbezogene Daten enthalten, sind durch das Management des Lieferanten zu prüfen und zu genehmigen, wobei die Dokumentation der Prüfung/Genehmigungen im Falle eines Audits verfügbar sein muss.

10.4. Physische und/oder logische Trennung der Entwicklungs-, Test- und Staging-Umgebungen von Produktionsumgebungen, in denen personenbezogene Daten verarbeitet werden.

10.5. Der Lieferant hat zur Verarbeitung personenbezogener Daten für Avaya physisch oder logisch getrennte Datenbanken zu führen.

- ENDE DER TOMs -