TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

(FÜR KUNDEN)

1. Zutrittskontrolle

Avaya 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. Avaya unterhält physische Sicherheitsmaßnahmen zur Verhinderung eines unbefugten Zugangs. Dies wird durch die folgenden Maßnahmen erreicht:

1.1.1. ein elektronisches Zugangskontrollsystem mit Protokollen, die 90 Tage lang aufbewahrt werden;

1.1.2. eine Videoüberwachung der Einrichtung rund um die Uhr, mit Protokollen, die 30 Tage lang aufbewahrt werden; sowie

1.1.3. Einbruchsmelde-/Alarmanlagen oder Beauftragung von Sicherheitspersonal vor Ort.

1.2. Avaya beschränkt den Zugang zu verschiedenen Bereichen des Betriebsgeländes basierend auf der Funktion der jeweiligen Person und nimmt eine regelmäßige Überprüfung des Zugangs der jeweiligen Person vor.

1.3. Zur Verhinderung eines unbefugten Zugangs trifft Avaya die folgenden Sicherheitsmaßnahmen für Mitarbeiter und Besucher:

1.3.1. Mitarbeiter müssen Ausweise sichtbar tragen;

1.3.2. Besucher müssen sich anmelden;

1.3.3. Besucher werden angemessen von Mitarbeitern begleitet; und

1.3.4. Besucher müssen Ausweise sichtbar tragen, so dass sie ohne Weiteres als Besucher zu erkennen sind.

2. Zugangskontrolle

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

2.1. Zugang zu Geräten, die personenbezogene Daten verarbeiten, gewährt Avaya nur Personen mit

2.1.1. eindeutigen Benutzerkennung für den Zugang im Rahmen eines Autorisierungsprozesses und

2.1.2. eindeutigem Passwort, das die folgenden Merkmale aufweist:

2.1.2.1. ein komplexes Passwort, bestehend aus acht Zeichen und aus drei von vier Zeichenkategorien;

2.1.2.2. eine Gültigkeitsdauer von höchstens 90 Tagen; und

2.1.2.3. eine Kontosperre nach fehlgeschlagenen Anmeldeversuchen.

2.2. Avaya gewährt den einzelnen Personen Zugang basierend auf ihrer Funktion anhand der folgenden Kriterien:

2.2.1. funktionsbasierter Zugang;

2.2.2. Zugang nach dem Grundsatz der geringstmöglichen Rechteeinräumung; und

2.2.3. Zugang nach dem „need to know“ Prinzip.

2.3. Bildschirme von Endgeräten werden nach 20-minütiger Inaktivität automatisch gesperrt.

2.4. Avaya protokolliert den Zugang zu Datenverarbeitungssystemen.

2.5. Für den Fernzugriff nutzt Avaya eine Mehrfaktor-Authentifizierung für das virtuelle private Netzwerk (VPN) .

2.6. Avaya wird eine zentrale Nutzerverwaltung einrichten und aufrechterhalten.

2.7. Von Avaya selbst bereitgestellte Endgeräte werden verschlüsselt.

3. Zugriffskontrolle

Avaya verhindert den Zugriff auf personenbezogene Daten durch unbefugte Personen. Hierfür trifft Avaya 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. Zugriff auf die personenbezogenen Daten gewährt Avaya nur Personen mit:

3.1.1. eindeutiger Benutzerkennung für den Zugriff im Rahmen eines förmlichen Genehmigungsprozesses und

3.1.2. Eindeutigem Passwort, das die folgenden Merkmale aufweist:

3.1.2.1. ein komplexes Passwort, bestehend aus acht Zeichen und aus drei von vier Zeichenkategorien;

3.1.2.2. eine Gültigkeitsdauer von höchstens 90 Tagen; und

3.1.2.3. eine Kontosperre nach fehlgeschlagenen Anmeldeversuchen.

3.2. Avaya gewährt den einzelnen Personen Zugriff auf personenbezogene Daten abhängig von ihrer Funktion bzw. Rolle anhand der folgenden Kriterien:

3.2.1. Funktions-/Rollenbasierter Zugang;

3.2.2. Zugang nach dem Grundsatz der geringstmöglichen Rechteeinräumung ; und

3.2.3. Zugang nach dem „need to know“ Prinzip.

3.3. Bildschirme von Endgeräten werden nach 20-minütiger Inaktivität automatisch gesperrt.

3.4. Avaya protokolliert den Zugriff auf Datenverarbeitungssysteme.

3.5. Avaya führt Zugriffskontrolllisten (.

3.6. Avaya führt Datensicherungen und Wiederherstellungen durch und verwahrt alle Backup-Medien und Test-Backups sicher.

3.7. Avaya unterhält ein Zugangskontroll-Change-Management-Programm.

3.8. Avaya unterhält sowohl auf Konzern- als auch auf Geschäftsbereichsebene interne Sicherheitsrichtlinien und -standards.

3.9. Avaya führt regelmäßig Schulungen über den Schutz personenbezogener Daten durch. Die Teilnahme an den Schulungen ist verpflichtend, wird überwacht und durchgesetzt.

3.10. Avaya unterhält zentral überwachte und aktualisierte Virenschutzprogramme. , und führt regelmäßig Antiviren-Scans durch.

3.11. Avaya sorgt für eine sichere Löschung und/oder Entsorgung von Daten.

4. Weitergabekontrolle

Avaya verhindert durch sichere Kommunikationskanäle, dass personenbezogene Daten während der Übertragung bzw. des Transports unbefugt gelesen werden können, und dass sämtliche Übertragungen und Transporte protokolliert werden. Dies geschieht jedenfalls durch folgende Maßnahmen:

4.1. Avaya nutzt für den Fernzugriff ein VPN mit Mehrfaktor-Authentifizierung.

4.2. Avaya setzt Firewalls mit den folgenden Merkmalen und Prozessen ein:

4.2.1. Zustandsorientierte Paketüberprüfung;

4.2.2. sofern es keine ausdrücklich genehmigten Zugangsregeln gibt, wird der Zugang standardmäßig verweigert;

4.2.3. funktions-/ rollenbasierter Zugang nach dem Grundsatz der geringstmöglichen Rechteeinräumung und nach dem „need to know“ Prinzip;

4.2.4. Zugriffsprotokollierung und -alarm; und

4.2.5. jährliche Überprüfung der Firewall-Regeln.

4.3. Falls vom Kunden aktiviert, nutzt Avaya E-Mail-Verschlüsselung der Transport Layer Security (TLS) Methode.

4.4. Avaya implementiert sowohl auf Konzern- als auch auf Geschäftsbereichsebene dauerhaft angelegte interne Sicherheitsrichtlinien und -standards.

5. Eingabekontrolle

Avaya gewährleistet durch angemessene Maßnahmen, dass geprüft und festgestellt kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht jedenfalls durch folgende Maßnahmen:

5.1. Personen, die auf personenbezogene Daten zugreifen, benötigen eine eindeutige Benutzerkennung sowie eine Autorisierung für den Zugriff.

5.2. Avaya implementiert sowohl auf Konzern- als auch auf Geschäftsbereichsebene dauerhaft angelegte interne Sicherheitsrichtlinien und -standards.

5.3. Die Geräte zur Verarbeitung personenbezogener Daten sind mit Protokollfunktionalität ausgestattet.

5.4. Zugriff auf personenbezogene Daten gewährt Avaya Einzelpersonen nur aufgrund ihrer Funktion, anhand der folgenden Kriterien :

5.4.1. Funktions-/ rollenbasierter Zugang;

5.4.2. Zugang nach dem Grundsatz der der geringstmöglichen Rechteeinräumung ; und

5.4.3. Zugang nach dem „need to know" Prinzip.

6. Organisationskontrolle

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

6.1. Avaya stellt im Rahmen von Auftragsverarbeitungen sicher, dass die personenbezogenen Daten streng nach den Weisungen des Kunden verarbeitet werden.

6.2. Der Kunde erteilt Avaya klare Weisungen im Hinblick auf den Umfang der Verarbeitung personenbezogener Daten und Avaya wird diese Weisungen beachten.

7. Verfügbarkeitskontrolle

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

7.1. Avaya unterhält eine unterbrechungsfreie Stromversorgung, Brand- und Rauchmelder, Feuerlöschanlagen, Generatoren, Kühlsystemen und erhöhten Fußböden.

7.2. Avaya unterhält einen Disaster Recovery Plan, der jährlich überprüft und getestet wird.

7.3. Avaya unterhält eine Backup-Strategie sowie von Backup-Verfahren.

7.4. Avaya verwendet Antivirensoftware und Firewall Systeme .

8. Datentrennungskontrolle

Avaya unterhält geeignete Maßnahmen, um eine getrennte Verarbeitung von für verschiedene Zwecke erhobenen Daten zu gewährleisten. Dies geschieht jedenfalls durch folgende Maßnahmen:

8.1. Avaya trennt personenbezogene Daten unterschiedlicher Kunden durch Speicherung der personenbezogenen Daten in logisch getrennten Datenbanken.

8.2. Avaya unterscheidet zwischen produktiven Daten und Testdaten.

- ENDE DER TOMs -