Technisch Organisatorische Maßnahmen

DataFreshup GmbH

Von-Arenberg-Straße 38
40668 Meerbusch
Deutschland

1. Vertraulichkeit

1.1. Erläuterung der technischen und organisatorischen Maßnahmen zur Wahrung der Vertraulichkeit

Beschreibung:

Zutrittskotrolle:
Die im Unternehmen getroffenen Maßnahmen gewährleisten, dass Unbefugte nicht auf Datenverarbeitungsanlagen Einfluss nehmen können, auf denen personenbezogene Daten verarbeitet oder gespeichert werden.

Zugangskontrolle:
Durch folgende Maßnahmen wird die Benutzung der Datenverarbeitungssysteme durch Unbefugte verhindert.

Zugriffskontrolle:
Die im Unternehmen getroffenen Maßnahmen der Vertraulichkeit und Integrität gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Darüber hinaus wird sichergestellt, dass personenbezogene Daten bei der Verarbeitung, der Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Trennungskontrolle:
Die im Unternehmen getroffenen Maßnahmen der Trennungskontrolle gewährleisten darüber hinaus, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten ebenfalls getrennt verarbeitet werden können.

Pseudonymisierung:
Die im Unternehmen getroffenen Maßnahmen zur Pseudonymisierung führen dazu, dass ohne das Hinzuziehen weiterer Informationen der Datensatz nicht einer Person direkt zugeordnet werden kann. Dies gilt für den Fall, dass diese weiteren Informationen von den anderen getrennt aufbewahrt werden, welche den TOMs entspricht.

Risiken:

Verletzung der Vertraulichkeit

Verhaltensregeln:

Die konkreten Ausführungen der entsprechenden Kontrollen zur Wahrung der Vertraulichkeit werden auf den folgenden Seiten erläutert.

1.2. TOM STRATO AG | HiDrive (V1)

Beschreibung:

1.1 ZUTRITTSKONTROLLE STRATO AG
Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind. Festlegung von Sicherheitsbereichen

*Realisierung eines wirksamen Zutrittsschutzes
*Protokollierung des Zutritts
*Festlegung Zutrittsberechtigter Personen
*Verwaltung von personengebundenen Zutrittsberechtigungen
*Begleitung von Fremdpersonal
*Überwachung der Räume

1.2 ZUGANGSKONTROLLE STRATO AG
Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.

*Festlegung des Schutzbedarfs
*Zugangsschutz
*Umsetzung sicherer Zugangsverfahren, starke Authentisierung
*Umsetzung einfacher Authentisierung per Username Passwort
*Protokollierung des Zugangs
*Monitoring bei kritischen IT-Systemen
*Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
*Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter *Zugangskennungen
*Verbot Speicherfunktion für Passwörter und/oder Formulareingaben (Server/Clients)
*Festlegung befugter Personen
*Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und *Zugangsberechtigungen
*Automatische Zugangssperre und Manuelle Zugangssperre

1.3 ZUGRIFFSKONTROLLE STRATO AG
Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

*Erstellen eines Berechtigungskonzepts
*Umsetzung von Zugriffsbeschränkungen
*Vergabe minimaler Berechtigungen
*Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
*Vermeidung der Konzentration von Funktionen

1.4 VERWENDUNGSZWECKKONTROLLE STRATO AG
Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

*Datensparsamkeit im Umgang mit personenbezogenen Daten
*Getrennte Verarbeitung verschiedener Datensätze
*Regelmäßige Verwendungszweckkontrolle und Löschung
*Trennung von Test- und Entwicklungsumgebung

1.5 DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN STRATO AG
Sofern Daten zur Erreichung des Verwendungszwecks nicht erforderlich sind, werden die technischen Voreinstellungen so festgelegt, dass Daten nur durch eine Aktion der Betroffenen Person erhoben, verarbeitet, weitergegeben oder veröffentlicht werden.

Risiken:

Verletzung der Vertraulichkeit durch den Auftragsverarbeiter

Verhaltensregeln:

Wahrung der Vertraulichkeit im HiDrive

2. Zutrittskontrolle

2.1. Alarmanlage

Beschreibung:

Das Bürogebäude verfügt über eine Alarmanlage mit Bewegungsmeldern in allen relevanten Bereichen des Gebäudes. Die Alarmanlage wird aktiviert, wenn sich keine Mitarbeiter im Bürogebäude befinden. Wird ein Alarm ausgelöst, werden unverzüglich der Sicherheitsdienst sowie die Geschäftsführung per SMS informiert. Der Sicherheitsdienst verschafft sich innerhalb der vertraglich definierten Zeit vor Ort einen Überblick und informiert die Geschäftsführung über die Sachlage. Falls notwendig wird außerdem die Polizei informiert.

Risiken:

-

Verhaltensregeln:

-

2.2. Dokumentierte Schlüsselvergabe

Beschreibung:

Die Vergabe von Schlüsseln erfolgt ausschließlich an Mitarbeiter. Die Vergabe wird durch einen weiteren Mitarbeiter begleitet und erfolgt erst nach Unterzeichnung eines Übergabeprotokolls. Im Protokoll werden die beteiligten Personen, das Datum und die Uhrzeit der Vergabe und die Schlüssel-Nummer festgehalten. Das Protokoll wird an zentraler Stelle sicher verwahrt. Alle Inhaber werden zudem darüber informiert, dass Schüssel sicher zu verwahren sind und deren Verlust umgehend zu melden ist.

Risiken:

-

Verhaltensregeln:

Ein Verlust ist unverzüglich der Geschäftsleitung zu melden.

2.3. Jeder kennt jeden (KMU)

Beschreibung:

In einem kleinst- oder klein- und mittelständischen Unternehmen kann die Regel "Jeder kennt jeden" angewandt werden. Dies führt dazu, dass betriebsfremde Personen wohl schneller erkannt werden können.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Personen mit unzulässigen Berechtigungen ist diese nur nach direkter Rücksprache mit dem Vorgesetzten zu gewähren. Fremde Personen ohne Berechtigungsausweis, die allein in den Räumlichkeiten angetroffen werden, müssen unverzüglich höflich nach dem Grund ihres Aufenthalts oder den evtl. Gastgeber innerhalb des Gebäudes gefragt werden.

2.4. Manuelles Schließsystem

Beschreibung:

Mithilfe eines manuellen Schließsystems wird das Gebäude vor unbefugtem Zutritt gesichert.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

-

2.5. Schlüsselvergabe

Beschreibung:

Für Büroräume, Kasse und die fest im NAS System eingebauten Festplatten werden Schlüssel vergeben. Über die genaue Vergabe der Schlüssel wird eine Liste geführt.

Risiken:

Zutritt von Unbefugten (da die Schlüssel nicht ohne weitere zuzuordnen sind, kann dieses Risiko gering eingeschätzt werden.

Verhaltensregeln:

Im Fall des Verlustes ist dies dem Arbeitgeber direkt anzuzeigen. Schlüssel dürfen nicht beschriftet werden, um eine Zuordnung durch Externe zu vermeiden.

2.6. TOM Placetel c/o Cisco Systems GmbH (04/22)

Beschreibung:

Zutrittskontrolle zu Räumlichkeiten und Einrichtungen, in denen Daten verarbeitet werden:
Das Gebäude der Broadsoft Germany GmbH in der Lothringer Straße 56 in Köln ist mit einer Alarmanlage gesichert. Es ist eine manuelle Schließanlage für Gebäude und Etage vorhanden. Zutrittsberechtigte Per- sonen sind nur Mitarbeiter und Reinigungskräfte. Unternehmensfremde / Gäste / Besucher / Wartungs- personal zu den Broadsoft Büro- und Betriebsräumen werden namentlich mit Ein- und Ausgangszeit dokumentiert. Das Empfangspersonal ist zum Thema Sicherheit geschult.

2.7. Türsicherung (elektrischer Türöffner)

Beschreibung:

Die Eingangstüren zum Unternehmen werden durch einen elektrischen Türöffner gesichert, der nur nach Rücksprache mit dem Empfang oder dem zuständigen Sekretariat betätigt wird.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Beschäftigte fragen die Person zunächst, welches Einlassbegehr sie vorweisen können, und überprüfen diesen Umstand.

3. Zugangskontrolle

3.1. Authentifikation mit Benutzername / Passwort

Beschreibung:

Sowohl für interne als auch für externe Systeme werden grundsätzlich personalisierte Logins mit Benutzernamen und Passwort vergeben.

Risiken:

Nutzung von Unbefugten

Verhaltensregeln:

Benutzername und Passwort dürfen nicht am Gerät angebracht werden oder in einer unverschlüsselten Datei aufbewahrt werden.

3.2. Dokumentation eingerichteter Zugänge für Mitarbeiter

Beschreibung:

Alle Zugänge zu internen und externen Systemen werden vor deren Einrichtung dokumentiert. Dabei werden der Name des Mitarbeiters, das jeweilige System sowie der eingerichtete Benutzername protokolliert. Diese Informationen stellen die Basis dafür dar, dass bei einem späteren Austritt zielgerichtet die Zugänge des jeweiligen Mitarbeiters gesperrt bzw. gelöscht werden können.

Risiken:

-

Verhaltensregeln:

-

3.3. Dokumentierte Schlüsselvergabe

Beschreibung:

Die Vergabe von Schlüsseln erfolgt ausschließlich an Mitarbeiter. Die Schlüsselvergabe wird durch einen weiteren Mitarbeiter begleitet und erfolgt erst nach Unterzeichnung eines Übergabeprotokolls. Im Protokoll werden die beteiligten Personen, das Datum und die Uhrzeit der Vergabe sowie die Schlüssel-Nummer festgehalten. Das Protokoll wird an zentraler Stelle sicher verwahrt. Alle Inhaber werden zudem darüber informiert, dass Schüssel sicher zu verwahren sind und deren Verlust umgehend zu melden ist.

Risiken:

Nutzung von Unbefugten

Verhaltensregeln:

Der Verlust eines Schlüssels ist unverzüglich der Geschäftsleitung zu melden.

3.4. Einsatz einer Hardware-Firewall

Beschreibung:

Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und dabei werden die angelegten Firewall-Richtlinien überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Risiken:

Hacking

Verhaltensregeln:

-

3.5. Einsatz von VPN-Technologie

Beschreibung:

Durch den Einsatz von VPN-Technologie und anderen sicheren Verschlüsselungsmethoden werden IT-Systeme vor unbefugter Nutzung und Hacking geschützt.

Risiken:

Nutzung von Unbefugten, Hacking

Verhaltensregeln:

Der VPN-Tunnel ist vor dem Zugriff auf den Server zu aktivieren.

3.6. Einsatz von Zwei-Faktor-Authentifizierung

Beschreibung:

Es wird eine Zwei-Faktor-Authentifizierung als Zugangskontrolle zu IT-Systemen gewählt.

Risiken:

Unbefugte Nutzung

Verhaltensregeln:

-

3.7. Passwortrichtlinie, inkl. Passwortlänge, Passwortwechsel

Beschreibung:

Sowohl für interne als auch für externe Zugänge werden ausschließlich sichere Passwörter mit einer Länge von mindestens zehn Zeichen verwendet. Die Passwörter beinhalten zudem mindestens einen Groß- und Kleinbuchstaben, eine Zahl sowie ein Sonderzeichen. Auch wird sichergestellt, dass ein Passwort nicht für mehrere Zugänge verwendet wird. Wird einer der genutzten Zugänge kompromittiert, bleibt die Sicherheit der übrigen Zugänge nach wie vor gewahrt.

Risiken:

Nutzung von Unbefugten

Verhaltensregeln:

Benutzername und Passwort dürfen nicht am Gerät angebracht werden oder in einer unverschlüsselten Datei aufbewahrt werden.

3.8. Sicherung der Arbeitsplätze bei Abwesenheit (Clean-Desk)

Beschreibung:

Arbeitsplätze sind bei Abwesenheit im Sinne der Clean-Desk-Regelung zu sichern. Auch bei kurzzeitigem Verlassen der Arbeitsräume (z.B. zum Kaffeekochen) sind die Räume abzuschließen oder anderweitige geeignete Maßnahmen zu treffen, die den unbefugten Zugriff auf die Arbeitsmittel, Daten oder Dokumente verhindern (z.B. Wegschließen von Papierunterlagen, Sperrung des Arbeitsrechners etc.).

Risiken:

Nutzung durch Unbefugte

Verhaltensregeln:

Auch bei kurzzeitigem Verlassen der Arbeitsräume sind die Räume abzuschließen oder anderweitige geeignete Maßnahmen zu treffen, die den unbefugten Zugriff auf die Arbeitsmittel, Daten oder Dokumente verhindern.

3.9. TOM Placetel c/o Cisco Systems GmbH (04/22)

Beschreibung:

Das Firmennetzwerk (Office IT, LAN, Router, etc.) ist gegen das öffentliche Netzwerk durch eine Hardware Firewall geschützt. Die Mitarbeiter autorisieren sich über Benutzername und ein geheim zu haltendes Passwort mit einer Mindestlänge 8 Zeichen. Der Wechselrhythmus, ist 80 Tage. Es gibt eine automatische Verriegelung des Bildschirms nach 15 Minuten. Broadsoft setzt Virenscanner für die E-Mail-Accounts ein. Sicherheitsrelevante Software-Updates werden regelmäßig und automatisiert in die vorhandene Soft- ware eingespielt. Datenträgern in Laptops / Notebooks sind verschlüsselt.
Die Arbeitsplatzgeräte sind mit Virenschutz und einem Schutz vor Schadsoftware, sowie einem automa- tischen Update der Signatur ausgestattet. Die Betriebssysteme sowie die Software werden regelmäßig zur Minimierung der Sicherheitsanfälligkeit aktualisiert.
Alle Server von Broadsoft, die Daten des Auftraggebers oder des Verantwortlichen speichern oder ver- arbeiten, sind im Rechenzentrum von Equinix FR4/FR5, BT Sossenheim, GCP Frankfurt untergebracht. Alle Rechenzentren sind ISO 27001 zertifiziert. Die Unterauftragnehmer von Broadsoft gewährleisten die Einhaltung der Datensicherheit über Auftragsverarbeitungsverträge (AVV).
Produktivsysteme und Netzwerk sind von den Entwicklungs- oder Testsystemen separiert.
Broadsoft setzt aktuelle Techniken zur Entdeckung von Angriffen ein, welche am Netzwerk-Perimeter die Identifikation von Attacken ermöglicht. Broadsoft hat einen Prozess implementiert, um Sicherheitsver- letzungen zu erkennen und zu mindern. Broadsoft berichtet unverzüglich an den Auftraggeber etwaige Sicherheitszwischenfälle. Die Placetel Plattform sowie deren Rechenzentren wurden von der Mutterge- sellschaft Cisco Inc. strengsten Sicherheits- und Penetrationstest unterzogen die im täglichen Turnus au- tomatisiert ausgeführt werden, um aktuelle Sicherheitslücken direkt zu erkennen und die entsprechen- den Patches einzuspielen. Zudem setzt die Placetel Plattform auf Continous Operations und Deployment, d.h. die gesamte Plattform wird automatisiert ausgerollt und konfiguriert. Somit wird sichergestellt, dass bestehende Systeme und Konfigurationen nicht manuell verändert oder manipuliert werden können. Zudem erlaubt dieser Ansatz, das einfache und schnelle ausrollen neuster Security Updates.

3.10. Verschlüsselung von Websites

Beschreibung:

Die Website verwendet das verbreitete SSL-Verfahren (Secure Socket Layer) in Verbindung mit der jeweils höchsten Verschlüsselungsstufe, die von Ihrem Browser unterstützt wird. Ob eine einzelne Seite unserer Website verschlüsselt übertragen wird, erkennen Sie an der geschlossenen Darstellung des Schüssel- beziehungsweise Schloss-Symbols in der Statusleiste Ihres Browsers. Die gesicherte Verbindung zwischen Browser und Zielserver stellt sicher, dass Daten zwischen diesen beiden Systemen nicht von Dritten eingesehen oder manipuliert werden können.
Weiterführende Informationen unter: https://datafreshup.de/blog/websiteverschluesselung/

Risiken:

Unbefugte Nutzung, Manipulation, Verlust, Zerstörung

Verhaltensregeln:

-

3.11. Zuordnung von Benutzerrechten

Beschreibung:

Zuordnung von Benutzerrechten im Rahmen eines Berechtigungskonzeptes mit verbindlichen Berechtigungsverfahren.

Risiken:

Nutzung von Unbefugten

Verhaltensregeln:

-

4. Zugriffskontrolle

4.1. Anzahl der Administratoren auf das „Notwendigste“ reduziert

Beschreibung:

Um zu gewährleisten, dass lediglich autorisierte Personen Zugriff auf kritische IT-Systeme sowie darauf gespeicherte Daten haben, verfügen nur ausgewählte Mitarbeiter über die notwendigen administrativen Rechte. Diese Mitarbeiter schalten projektbezogen die Zugriffsrechte der anderen Mitarbeiter frei, sofern diese für ihre Arbeit notwendig sind. Nach Abschluss der jeweiligen Arbeiten werden die entsprechenden Rechte wieder entzogen. So wird die Anzahl der Mitarbeiter, die theoretisch Zugriff auf alle im Unternehmen gespeicherten personenbezogenen Daten haben, auf ein absolutes Minimum reduziert.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.2. Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

Beschreibung:

Gedruckte Dokumente mit sensiblem Inhalt werden nicht über den normalen Papiermüll entsorgt. Stattdessen stehen für deren sichere Entsorgung spezielle Aktenvernichter bzw. abschließbare Papiersammelbehälter zur Verfügung, die von einem Spezialunternehmen nachweislich vernichtet und entsorgt werden.

Risiken:

Datenzugriff von Unbefugten

Verhaltensregeln:

-

4.3. Festlegung von Datenbankrechten

Beschreibung:

Für die Datenbank werden Rechte und Rollen festgelegt, die regelmäßig auf Richtigkeit der Angaben überprüft werden.

Risiken:

Datenverlust, Datenpanne, unberechtigter Zugriff

Verhaltensregeln:

Die Benutzer agieren innerhalb der ihnen zugeordneten Datenbankrechte.

4.4. Nutzung von Benutzer- und Rollenkonzepten

Beschreibung:

Für interne und externe Systeme, die diese Funktionalität unterstützen, werden Benutzer- und Rollenkonzepte beim Anlegen von Zugängen verwendet. Anstatt jeden einzelnen Zugang mit entsprechenden Berechtigungen auszustatten, wird jedem

Zugang eine Rolle zugewiesen. Diesen übergeordneten Rollen werden wiederum die notwendigen Berechtigungen zugewiesen. So können Änderungen an den Berechtigungen zentral über die Anpassung der jeweiligen Rolle erfolgen. So kann verhindert werden, dass einzelne Zugänge über Berechtigungen verfügen, die diesen eigentlich nicht gestattet sind.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.5. Regelmäßige Sicherheitsupdates und Backups interner Systeme (nach dem jeweiligen Stand der Technik)

Beschreibung:

Alle im Einsatz befindlichen Betriebssysteme sowie darauf installierte Anwendungen und Bibliotheken werden stets aktuell gehalten. Entsprechende Updates werden regelmäßig eingespielt. Zur Verfügung gestellte Security-Patches werden ebenfalls zeitnah eingespielt, um die entsprechenden Sicherheitslücken schnellstmöglich zu schließen. Werden für Anwendungen oder Bibliotheken keine Security-Updates mehr ausgeliefert oder wird die Anwendung vom Hersteller nicht mehr weiterentwickelt oder betreut, findet ein Upgrade auf eine aktuelle Version statt oder es findet ein Wechsel auf eine noch unterstützte alternative Anwendung statt.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.6. Sichere Aufbewahrung von Datenträgern

Beschreibung:

Datenträger werden sicher aufbewahrt, sodass sie vor Datenzugriff durch Unbefugte geschützt sind.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.7. TOM Placetel c/o Cisco Systems GmbH (04/22)

Beschreibung:

Bei Broadsoft sind Berechtigungskonzepte vorhanden, wie die Zuordnung von Benutzerrechten, Pass- wortvergabe inkl. Passwortlänge sowie Passwortwechsel, Zuordnung von Benutzerprofilen zu IT-Syste- men) und diese werden dokumentiert. Die Rechte werden durch einen Systemadministrator verwaltet. Die Authentifikation erfolgt über Benutzername und Passwort. Die Berechtigungsvergabe wird namens- scharf dokumentiert (insbesondere wer darf welche Rechte vergeben). Die vergebenen Berechtigungen werden ebenfalls namensscharf aktualisiert und dokumentiert. Broadsoft ist SOX compliant.
Die Unterauftragsverarbeiter von Broadsoft kontrollieren zu jederzeit den Zugang zu deren Rechenzen- tren und anderen Bereichen, in denen Daten von Broadsoft, des Auftraggebers oder des Verantwortli- chen gespeichert oder aufbewahrt werden. Der Zugriff wird nur für solche Mitarbeiter der Unterauf- tragsverarbeiter oder deren Unter-Auftragnehmer mit einem geschäftlichen Bedarf gewährt. Jeder Zu- griff auf ein Rechenzentrum der Unterauftragsverarbeiter wird protokolliert, Protokolle müssen nach geltendem Recht, jedoch nicht weniger als 90 Tagen gespeichert werden. Die Rechenzentren der Unter- auftragsverarbeiter verfügen über voll funktionsfähige Angriffsdetektionen, so dass der unbemerkte Zu- griff sowie der

Zugriff unberechtigter Personen effizient verhindert wird. Die Unterbeauftragten der Broadsoft Germany haben keinen Zugriff auf die installierte Software oder das OS auf dem die Placetel Plattform ausgeführt wird.
Die Datenträger werden ordnungsgemäß (DIN 32757) vernichtet und die Vernichtung wird protokolliert. Es wird ein Aktenvernichter bzw. Dienstleister mit Datenschütz-Gütesiegel genutzt.

5. Trennungsgebot

5.1. Festlegung von Datenbankrechten

Beschreibung:

Für die Datenbank werden Rechte und Rollen festgelegt, die regelmäßig auf die Richtigkeit der Angaben überprüft werden.

Risiken:

Datenverlust, Datenpanne, unberechtigter Zugriff

Verhaltensregeln:

-

5.2. Logische Mandantentrennung (softwareseitig)

Beschreibung:

Die logische Trennung der Mandanten erfolgt systemseitig über eine Ordnerstruktur je Kunde.

Risiken:

Datenverlust, Datenpanne

Verhaltensregeln:

-

6. Datenintegrität

6.1. Erläuterung der technischen und organisatorischen Maßnahmen zur Wahrung der Datenintegrität

Beschreibung:

Weitergabekontrolle:
Die im Unternehmen getroffenen Maßnahmen gewährleisten eine hinreichende Weitergabekontrolle. Personenbezogene Daten werden bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt, ohne das dies überprüft, festgestellt bzw. unterbunden werden kann.

Eingabekontrolle:
Die im Unternehmen getroffenen Maßnahmen zur Datenintegrität gewährleisten eine hinreichende Eingabekontrolle. Es kann in den Geschäftsprozessen nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Risiken:

Verletzung der Datenintegrität

Verhaltensregeln:

Die konkreten Ausführungen der entsprechenden Kontrollen zur Wahrung der Integrität der Daten werden auf den folgenden Seiten erläutert.

6.2. TOM STRATO AG | HiDrive (V1)

Beschreibung:

2.1 WEITERGABEKONTROLLE STRATO AG
Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

*Festlegung empfangs- /weitergabeberechtigter Instanzen/Personen
*Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
*Protokollierung von Übermittlungen gemäß Protokollierungskonzept
*Sichere Datenübertragung zwischen Server und Client
*Sicherung der Übertragung im Backend
*Sichere Übertragung zu externen Systemen
*Risikominimierung durch Netzseparierung
*Implementation von Sicherheitsgateways an den Netzübergabepunkten
*Härtung der Backendsysteme
*Beschreibung der Schnittstellen
*Umsetzung einer Maschine-Maschine-Authentisierung
*Sichere Ablage von Daten, inkl. Backups
*Gesicherte Speicherung auf mobilen Datenträgern
*Einführung eines Prozesses zur Datenträgerverwaltungen
*Prozess zur Sammlung und Entsorgung
*Datenschutzgerechter Lösch- und Zerstörungsverfahren
*Führung von Löschprotokollen

2.2 EINGABEKONTROLLE STRATO AG
Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind.

*Protokollierung der Eingaben
*Dokumentation der Eingabeberechtigungen

Risiken:

Verletzung der Integrität

Verhaltensregeln:

Wahrung der Integrität

7. Weitergabekontrolle

7.1. Einrichtungen von Standleitungen bzw. VPN-Tunneln

Beschreibung:

Ein externer Zugriff auf das Firmennetzwerk ist nur mittels einer VPN-Verbindung möglich. Die hierfür verwendeten Komponenten werden regelmäßig aktualisiert. Zugriffe über VPN werden vollständig protokolliert, um durchgeführte Aktionen nachträglich nachvollziehen zu können. Außerdem sind Zugriffe von außerhalb Europas grundsätzlich gesperrt. Zur Nutzung von VPN wird jedem Mitarbeiter, der einen solchen Zugang für seine Arbeit benötigt, ein individueller Zugang erstellt.

Risiken:

Dateneinsicht durch Dritte

Verhaltensregeln:

-

7.2. TOM Placetel c/o Cisco Systems GmbH (04/22)

Beschreibung:

Broadsoft nutzt zur webbasierten Datenübertragung zu Kunden oder Dienstleistern SSL Verschlüsselung auf allen Wegstrecken. Verbindungen zwischen Rechenzentren sind mittels dedizierter Leitungen oder durch verschlüsselte IPSEC Tunnels abgesichert und verschlüsselt.
Die Telefonverbindungen von Placetel zu seinen Kunden werden über die Standardprotokolle SIP und RTP durchgeführt. Die Übertragung erfolgt zustandslos über das UDP Protokoll. Da UDP im Gegensatz zu TCP zustandlos ist, sind die Pakete im Internet an einer beliebigen Stelle nicht zusammenfügbar und somit durch den Zugriff von Dritten aufgrund der Wesensart des Protokolls geschützt.
Back-ups werden sicher auf Maschinen ohne externen Zugriff aus dem Internet aufbewahrt. Die Back- ups werden unverschlüsselt durchgeführt.

7.3. Verschlüsselung der Website

Beschreibung:

Die Website verwendet das verbreitete SSL-Verfahren (Secure Socket Layer) in Verbindung mit der jeweils höchsten Verschlüsselungsstufe, die von Ihrem Browser unterstützt wird. Ob eine einzelne Seite unserer Website verschlüsselt übertragen wird, erkennen Sie an der geschlossenen Darstellung des Schüssel- beziehungsweise Schloss-Symbols in der Statusleiste Ihres Browsers. Die gesicherte Verbindung zwischen Browser und Zielserver stellt sicher, dass Daten zwischen diesen beiden Systemen nicht von Dritten eingesehen oder manipuliert werden können.
Weiterführende Informationen unter: https://datafreshup.de/blog/websiteverschluesselung/

Risiken:

Dateneinsicht durch Dritte

Verhaltensregeln:

-

7.4. Verschlüsselung von Dateien

Beschreibung:

Dateien werden verschlüsselt, um im Fall eines Verlustes die Nutzung durch Unbefugte auszuschließen.

Risiken:

Dateneinsicht durch Dritte

Verhaltensregeln:

Weiterführende Hinweise zum Thema Verschlüsselung von Dateien können Benutzer unter https://datafreshup.de/blog /verschluesselung/ einsehen. Wichtig: Alle Maßnahmen immer mit dem Vorgesetzten/der IT-Abteilung/Geschäftsleitung /Datenschutzbeauftragten absprechen.

7.5. Verschlüsselung von E-Mails

Beschreibung:

Werden Daten digital ausgetauscht, die unter Umständen personenbezogene Daten enthalten, findet dies ausschließlich auf sicheren und verschlüsselten Übertragungswegen statt. Es werden insbesondere SSH-Verbindungen genutzt und keine unverschlüsselten Protokolle verwendet, wenn verschlüsselte Alternativen zur Verfügung stehen. So werden E-Mails zum Beispiel via IMAP nur mit SSL/TLS oder HTTPS-Verbindungen versandt.

Risiken:

Dateneinsicht durch Dritte

Verhaltensregeln:

-

8. Eingabekontrolle

8.1. Datenschutzfreundliche Voreinstellungen

Beschreibung:

Der Verantwortliche trifft technische und organisatorische Maßnahmen, die geeignet sind, durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, zu verarbeiten.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

8.2. Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz- Gütesiegel)

Beschreibung:

Gedruckte Dokumente mit sensiblem Inhalt werden nicht über den normalen Papiermüll entsorgt. Stattdessen stehen für deren sichere Entsorgung spezielle Aktenvernichter bzw. abschließbare Papiersammelbehälter zur Verfügung. Darüber hinaus werden Daten über ein Spezialunternehmen nachweislich vernichtet und entsorgt.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

Personenbezogene Daten, insbesondere sensible Daten, werden nach Erfüllung des Zwecks und nach Ablauf der (gesetzlichen) Aufbewahrungsfristen fachgerecht vernichtet.

8.3. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Beschreibung:

Die Eingabe, Änderung und Löschung von Daten ist durch individuelle Benutzernamen (nicht Benutzergruppen) nachvollziehbar.

Risiken:

Verfälschung von Daten, Datenverlust

Verhaltensregeln:

-

8.4. ordnungsgemäße Vernichtung von Datenträgern

Beschreibung:

Datenträger werden ordnungsgemäß durch Aktenvernichter bzw. Dienstleister zur Aktenvernichtung (nach Möglichkeit mit Datenschutz-Gütesiegel) vernichtet.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

Datenträger, insbesondere solche mit sensiblen Daten, werden nach Erfüllung des Zwecks und nach Ablauf der (gesetzlichen) Aufbewahrungsfristen fachgerecht vernichtet.

9. Eingabekontrolle

9.1. TOM Placetel c/o Cisco Systems GmbH (04/22)

Beschreibung:

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist gewährleistet. Broad- soft loggt alle Datenein- und -ausgaben, die von den Nutzern und den Administratoren bei der Nutzung der Systeme und Applikationen durchgeführt werden. Diese Dokumentationen finden mit Fokus auf die Sicherheit der Datenverarbeitung statt. Diese Daten werden einer automatischen Abgleichs-Routine und Kontrolle unterzogen, um Unregelmäßigkeiten festzustellen. Die Logs werden je nach Inhalt und / oder gesetzlichen Vorgaben archiviert. Nach Ablauf der Archivierungsfrist oder Zweckerfüllung werden die Logs gelöscht bzw. gesperrt. Es werden Log-Files für die Nachvollziehbarkeit der Löschung/Änderung von Daten des Auftraggebers namensscharf je Mitarbeiter angelegt. Es besteht ein restriktives Zugriffskon- zept für vorgenannte Log-Files.

10. Verfügbarkeit und Belastbarkeit der Systeme

10.1. TOM Placetel c/o Cisco Systems GmbH (04/22)

Beschreibung:

Datensicherungsmaßnahmen werden alle 15 Minuten durchgeführt.
Es bestehen Verträge mit Dritten zur Wartung der IS Systeme. Die Server-Räume sind ausgestattet mit unterbrechungsfreier Stromversorgung, Klimaanlage, System zur Überwachung von Temperatur und Feuchtigkeit, Feuer- und Rauchmeldeanlagen, Feuerlöschgeräten und Alarmmeldungen bei unberechtig- tem Zutritt.
Tests zur Datenwiederherstellung werden durchgeführt. Es bestehen Back-up- und Recovery-Konzepte und ein Notfallplan ist vorhanden. Datensicherungen werden an einem sicheren, ausgelagerten Ort auf- bewahrt.

10.2. TOM STRATO AG | HiDrive (V1)

Beschreibung:

3.1 VERFÜGBARKEIT UND BELASTBARKEIT (Art. 32 Abs. 1 lit. b DSGVO)
*Brandschutz
*Redundanz der Primärtechnik
*Redundanz der Stromversorgung
*Redundanz der Kommunikationsverbindungen
*Monitoring
*Resourcenplanung und Bereitstellung
*Abwehr von systembelastendem Missbrauch
*Datensicherungskonzepte und Umsetzung
*Regelmäßige Prüfung der Notfalleinrichtungen

3.2 DESASTER RECOVERY - RASCHE WIEDERHERSTELLUNG NACH ZWISCHENFALL (Art. 32 Abs. 1 lit. c DSGVO)
*Notfallplan
*Datensicherungskonzepte und Umsetzung

Risiken:

Datenverlust

Verhaltensregeln:

Sicherung der Daten via HiDrive

11. Verfügbarkeitskontrolle und Belastbarkeit

11.1. Dokumentation datenschutzrelevanter Zwischenfälle

Beschreibung:

Datenschutzrelevante Zwischenfälle, bei denen nicht aus geschlossen werden kann, dass personenbezogene Daten gelöscht oder an unberechtigte Dritte weitergeleitet wurden, werden umfassend dokumentiert. Die Unterlagen dienen zum einen einer lückenlosen Kommunikation an die Datenschutzbehörden sowie an die betroffenen Kunden, zum anderen können auf Basis dieser Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.

Risiken:

-

Verhaltensregeln:

-

11.2. Einsatz einer Anti-Viren-Software

Beschreibung:

Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virenscanner vor den Auswirkungen schädlicher Dateien geschützt. Die zur Erkennung aktueller Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch ausgewählte Mitarbeiter möglich. Um die korrekte Funktion des eingesetzten Virenscanners sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von allen aktuellen Virenschutzlösungen erkannt wird.

Risiken:

Datenverlust

Verhaltensregeln:

-

11.3. Einsatz einer Hardware-Firewall

Beschreibung:

Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien dabei überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Risiken:

Datenverlust

Verhaltensregeln:

-

11.4. Einsatz einer Software-Firewall

Beschreibung:

Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien dabei überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Risiken:

Datenverlust

Verhaltensregeln:

-

11.5. Erläuterung der technischen und organisatorischen Maßnahmen zur Wahrung der Verfügbarkeit und der Belastbarkeit der Systeme

Beschreibung:

Die im Unternehmen getroffenen Maßnahmen zur Verfügbarkeitskontrolle gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Risiken:

Datenverlust

Verhaltensregeln:

Die konkreten Ausführungen der entsprechenden Kontrollen zur Wahrung der Verfügbarkeit und der Belastbarkeit der Systeme werden auf den folgenden Seiten erläutert.

11.6. Erstellen eines Backup- & Recoverykonzepts

Beschreibung:

Ein Backup- & Recoverykonzept (on- und offline) wurde erstellt und wird laufend weiterentwickelt.

Risiken:

Datenverlust

Verhaltensregeln:

-

11.7. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Beschreibung:

Bei einem physischen oder technischen Zwischenfall ist eine rasche Wiederherstellbarkeit der personenbezogenen Daten und des Zugangs zu diesen gewährleistet.

Risiken:

-

Verhaltensregeln:

-

11.8. Regelmäßige Updates

Beschreibung:

Alle im Einsatz befindlichen Betriebssysteme sowie darauf installierte Anwendungen und Bibliotheken werden stets aktuell gehalten. Entsprechende Updates werden regelmäßig eingespielt. Zur Verfügung gestellte Security-Patches werden ebenfalls zeitnah eingespielt, um die entsprechenden Sicherheitslücken schnellstmöglich zu schließen. Werden für Anwendungen oder Bibliotheken keine Security-Updates mehr ausgeliefert oder wird die Anwendung vom Hersteller nicht mehr weiterentwickelt oder betreut, findet ein Upgrade auf eine aktuelle Version oder ein Wechsel auf eine noch unterstützte alternative Anwendung statt.

Risiken:

Datenverlust

Verhaltensregeln:

-

11.9. Synology C2 Backup

Beschreibung:

Tägliches Backup sämtlicher Daten des NAS-Systems in das Synology Rechenzentrum in Frankfurt am Main.
Der Zugriff auf Daten in den Synology C2-Rechenzentren ist nur für das Synology-Konto möglich, mit dem sie hochgeladen wurden. Die Synology NAS kommuniziert über eine sichere verschlüsselte SSL-Verbindung mit dem C2 Rechenzentrum. Die Daten werden vor der Speicherung auf dem Laufwerk unlesbar gemacht und die Entschlüsselungsschlüssel befinden sich in einem anderen System. Zusätzlich ist eine clientseitige Verschlüsselung aktiviert, die sämtliche Daten vor der Übertragung mittels AES-256-Verschlüsselung unlesbar macht. Zugriff auf das Synology Konto ist nur über eine zweisVerlust des AES-256-Schlüssels, wodurch eine Entschlüsselung des Backups unmöglich ist.
tufige Verifizierung möglich.
Die Kollokationseinrichtungen im deutschen Rechenzentrum von Synology C2 Backup sind ISO 27001-zertifiziert.

Risiken:

Verlust des AES-256-Schlüssels, wodurch eine Entschlüsselung des Backups unmöglich ist.

Verhaltensregeln:

Tägliche Berichtsprüfung, ob Fehler bei der Erstellung des Backups aufgetreten sind und das Backup ordnungsgemäß durchgeführt wurde.

11.10. Testen von Datenwiederherstellung und Notfallszenarien

Beschreibung:

Für die im Vorfeld definierten kritischen Prozesse im Unternehmen findet regelmäßig ein Testdurchlauf statt. Hierfür wird zu einem zufällig ausgewählten Zeitpunkt ein bestimmtes Szenario definiert und unter realen Bedingungen durchgespielt. Allen beteiligten Mitarbeitern wird mitgeteilt, dass es sich um einen Testlauf handelt, damit keine unerwünschte Kommunikation an Externe (z. B. an Kunden) erfolgt. Auffälligkeiten sowie Optimierungspunkte werden im Nachgang gesammelt und, sofern sinnvoll, direkt umgesetzt.

Risiken:

Datenverlust

Verhaltensregeln:

-

12. Auftragskontrolle

12.1. Aufklärung von Kunden zum Thema Datenschutz

Beschreibung:

Nach Auftragserteilung klären wir Kunden über die von uns ergriffenen Maßnahmen zum Datenschutz auf und binden diese so gut wie möglich in die entsprechenden Prozesse ein. Falls notwendig empfehlen und installieren wir beim Kunden entsprechende Anwendungen, um einen optimalen Schutz personenbezogener Daten auf Kundenseite zu ermöglichen. So soll ein gleichermaßen hohes Sicherheitsniveau bei beiden Vertragspartnern sichergestellt werden.

Risiken:

-

Verhaltensregeln:

-

12.2. Auftragnehmer hat Datenschutzbeauftragten bestellt

Beschreibung:

Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt (soweit notwendig).

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

12.3. Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

Beschreibung:

Bei der Beauftragung von Dienstleistern und Partnern erfolgt vorab ein Vergleich möglicher Anbieter unter Datenschutzaspekten. Hierzu holen wir je nach Art und Umfang des Auftrags Informationen zur Verarbeitung personenbezogener Daten beim jeweiligen Anbieter ein. Bewertet werden Aspekte wie die Übermittlung von Daten, deren konkrete Verarbeitung sowie die getroffenen technischen und organisatorischen Schutzmaßnahmen. Eine Zusammenarbeit erfolgt ausschließlich mit Dienstleistern/Partnern, die das geforderte und Datenschutzniveau glaubhaft sicherstellen können.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

12.4. Datenschutz-Management

Beschreibung:

Im Unternehmen ist ein umfangreiches Datenschutz-Management in Form einer Datenschutz-Dokumentation und eines Datenschutz-Management-Systems implementiert.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

12.5. Dokumentation datenschutzrelevanter Zwischenfälle

Beschreibung:

Datenschutzrelevante Zwischenfälle, bei denen nicht ausgeschlossen werden kann, dass personenbezogene Daten gelöscht oder an unberechtigte Dritte weitergeleitet wurden, werden umfassend dokumentiert. Die Unterlagen dienen zum einen einer lückenlosen Kommunikation an die Datenschutzbehörden sowie die betroffenen Kunden, zum anderen können auf Basis dieser Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.

Risiken:

-

Verhaltensregeln:

-

12.6. Erläuterung der technischen und organisatorischen Maßnahmen im Rahmen von Auftragsverarbeitungen

Beschreibung:

Auftragskontrolle:
Die im Unternehmen getroffenen Maßnahmen gewährleisten ebenfalls ein hohes Schutzniveau im Bereich der Auftragskontrolle. Die im Auftrag verarbeiteten personenbezogenen Daten werden nur entsprechend den Weisungen des Auftraggebers verarbeitet.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

Die konkreten Ausführungen der entsprechenden Kontrollen zur Wahrung der technischen und organisatorischen Maßnahme im Rahmen von Auftragsverarbeitungen werden auf den folgenden Seiten erläutert.

12.7. Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter

Beschreibung:

Bei Eintritt in das Unternehmen werden alle wesentlichen Verhaltensrichtlinien zum Thema Datenschutz in schriftlicher wie persönlicher Form an neue Mitarbeiter kommuniziert. Neben unserem grundsätzlichen Verständnis vom Umgang mit personenbezogenen Daten vermitteln wir auch das notwendige Wissen zur korrekten Anwendung aller technischen und organisatorischen Datenschutzmaßnahmen.

Risiken:

-

Verhaltensregeln:

-

12.8. laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

Beschreibung:

Eine regelmäßige Überprüfung des Auftragnehmers und seiner Tätigkeiten wird in Form von Stichprobenkontrollen durchgeführt.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

12.9. Regelmäßige Unterweisung und Fortbildung von Mitarbeitern zum Thema Datenschutz

Beschreibung:

Unsere Mitarbeiter werden regelmäßig zu datenschutzrelevanten Themen geschult. Dabei werden sowohl Grundlagen aufgefrischt als auch aktuelle Themen sowie rechtliche Änderungen vermittelt. Neben den entsprechenden datenschutztechnischen Kompetenzen soll so eine hohe Sensibilität für den Schutz personenbezogener Daten bei allen Mitarbeitern gefördert werden.

Risiken:

-

Verhaltensregeln:

-

12.10. schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)

Beschreibung:

Mit allen Dienstleistern, Partnern und Kunden, mit denen ein Austausch sowie eine Verarbeitung von personenbezogenen Daten erfolgt, wird ein Vertrag zur Auftragsdatenverarbeitung (AV-Vertrag) gemäß Art. 28 DSGVO/§ 29 KDG geschlossen. In dem AV-Vertrag werden u. a. die folgenden Aspekte zwischen den beiden Vertragspartnern geregelt: “Anwendungsbereich und Verantwortlichkeit”, “Gegenstand und Dauer des Auftrages”, “Beschreibung der Verarbeitung, Daten und betroffener Personen”, “Technische und organisatorische Maßnahmen zum Datenschutz”, “Berichtigung, Einschränkung und Löschung von Daten”, “Pflichten des Auftragnehmers”, “Rechte und Pflichten des Auftraggebers”, “Wahrung von Rechten der betroffenen Person”, “Kontrollbefugnisse”, “Unterauftragsverhältnisse”, “Datengeheimnis und Geheimhaltungspflichten”, “Haftung” und “Informationspflichten, Schriftformklausel, Rechtswahl”. Der AV- Vertrag wird von beiden Vertragsparteien in schriftlicher oder alternativ in digitaler Form geschlossen. Beide Vertragsparteien verpflichten sich zudem, unverzüglich über relevante Änderungen zu informieren, so dass der AV-Vertrag entsprechend geändert und erneut abgeschlossen werden kann.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

Sollte den Beschäftigten ein datenschutzrechtlich unangemessenes Verhalten des Auftragsverarbeiters auffallen, so ist dieses unverzüglich dem Geschäftsführer und dem Datenschutzbeauftragten zu melden.

12.11. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Beschreibung:

Auftragsbezogene Daten mit personenbezogenen Inhalten, die zur Verarbeitung an uns übermittelt werden, werden bei Beendigung des Auftrags gelöscht, sofern diese nicht aus wichtigem Grund aufbewahrt werden müssen. Dies kann zum Beispiel dann notwendig sein, wenn sich aus dem Auftrag weitere Folgeaufträge ergeben, für deren vertragliche Umsetzung die Daten noch einmal benötigt werden. Eine ordnungsgemäße Löschung erfolgt dann nach Abschluss des letzten Folgeauftrags.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

12.12. TOM Placetel c/o Cisco Systems GmbH (04/22)

Beschreibung:

Die Mitarbeiter sind schriftlich auf die Einhaltung des Daten- gem. DSGVO und Fernmeldegeheimnis gem. § 88 TKG geschult und verpflichtet.
Die weisungsgemäße Auftragsdatenverarbeitung ist über den Endkunden AVV gewährleistet. Eine Da- tenverarbeitung durch Dritte (gem. Artikel 28 DSGVO) ist gemäß den Anweisungen des Auftraggebers/ Datenexporteurs erlaubt. Die Weitergabe von Daten zur Erfüllung Verträge an Unterauftragnehmer, Va- lue Added Reseller etc. erfolgt auf der Grundlage von EU Standard Vertragsklauseln, Unterauftragverar- beitungsverträgen bzw. Funktionsübertragungen.
Daten unterschiedlicher Kunden werden separat verarbeitet (über eine logische Trennung). Es ist eine funktionale Trennung zwischen der Produktionssystemen und Test-Systemen eingerichtet. Produktions- daten werden zum Test in Test-Systemen nur nach Rücksprache mit dem Auftraggeber und mit gleichem Sicherheitsstandard des Testsystems verwendet. Die Tests verringern nicht das Schutzniveau hinsichtlich der Vertraulichkeit, Integrität oder Verfügbarkeit der personenbezogenen Daten.
Ein Datenschutzbeauftragter ist bestellt.

12.13. TOM Placetel c/o Cisco Systems GmbH (04/22)

Beschreibung:

VERWENDUNGSZWECKKONTROLLE
Daten, die für unterschiedliche Zwecke erhoben werden, werden in der Datenbank logisch getrennt. Der Datenzugriff von Mitarbeitern ist über ein Berechtigungskonzept eingeschränkt.

UNTERAUFTRAGNEHMER
Datenverarbeitungen im Auftrag durch Unterauftragnehmer werden wie oben beschrieben geschützt und durch den Unterauftragsverarbeiter kontrolliert. Der Unterauftragsverarbeiter wird ihm anvertraute Daten nur in der mit dem Auftraggeber vertraglich vereinbarten Art und Weise verarbeiten. Kontrollmaß- nahmen werden gemeinsam mit dem Auftraggeber definiert und dann technisch und organisatorisch in die Verarbeitung implementiert. Der Unterauftragsverarbeiter setzt nur Unterauftragnehmer in der vertraglich vereinbarten Weise ein.

12.14. TOM STRATO AG | HiDrive (V1)

Beschreibung:

4. DATENSCHUTZORGANISATION
*Festlegung von Verantwortlichkeiten
*Umsetzung und Kontrolle geeigneter Prozesse
*Melde- und Freigabeprozess
*Umsetzung von Schulungsmaßnahmen
*Verpflichtung auf Vertraulichkeit
*Regelungen zur internen Aufgabenverteilung
*Beachtung von Funktionstrennung und –zuordnung
*Einführung einer geeigneten Vertreterregelung

5. AUFTRAGSKONTROLLE
Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

*Auswahl weiterer Auftragnehmer nach geeigneten Garantien
*Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern
*Abschluss einer Vereinbarung zur Auftragsverarbeitung mit STRATO

6. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG und EVALUIERUNG (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

*Informationssicherheitsmanagement nach ISO 27001
*Prozess zur Evaluation der Technischen und Organisatorischen Maßnahmen
*Prozess Sicherheitsvorfall-Management
*Durchführung von technischen Überprüfungen

Risiken:

Datenschutzverstöße

Verhaltensregeln:

Wahrung des Datenschutzes

12.15. Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter

Beschreibung:

Alle Mitarbeiter unterzeichnen beim Eintritt in das Unternehmen eine gesonderte Verschwiegenheitserklärung. Darin verpflichten sich die Mitarbeiter, personenbezogene Daten vertraulich zu behandeln und diese ausschließlich auf Weisung ihrer Vorgesetzten zu verarbeiten. Darüber hinaus werden Mitarbeiter über mögliche Folgen von Verstößen gegen die Vertraulichkeitsverpflichtung aufgeklärt. Alle in der Verschwiegenheitserklärung vereinbarten Punkte gelten auch über den Zeitraum der Anstellung hinaus.

Risiken:

-

Verhaltensregeln:

-

12.16. Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Beschreibung:

Die Beschäftigten des Auftragnehmers sind auf das Datengeheimnis verpflichtet. Die Überprüfung erfolgt im Rahmen regelmäßiger Stichprobenkontrollen.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

12.17. vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

Beschreibung:

Vor Abschluss der Verträge wird die Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen geprüft.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

12.18. Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

Beschreibung:

Gemäß dem Vertrag wurden wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart. Nach vorheriger Anmeldung führen wir stichprobenartige Überprüfungen zum Thema Datenschutz bei unseren Dienstleistern durch. Hierbei überprüfen wir zum einen, ob zugesicherte Datenschutzmaßnahmen wie vertraglich vereinbart durchgeführt werden. Zum anderen sprechen wir Empfehlungen für Optimierungen zum Datenschutz aus und unterstützen bei Bedarf bei deren Implementierung.

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-