Technisch Organisatorische Maßnahmen

edp Elsner Dühring & Partner | Markus Lange

Von-Arenberg-Str. 29a
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.

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 die Geschäftsführung per SMS informiert.

Risiken:

-

Verhaltensregeln:

-

2.2. Besucher werden beaufsichtigt

Beschreibung:

Eine Dienstanweisung legt fest, dass sich Besucher nicht unbeaufsichtigt im Gebäude bewegen dürfen.

Risiken:

Zutritt von Unbefugten, Diebstahl

Verhaltensregeln:

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

2.3. Dokumentierte Schlüssel- und Transpondervergabe

Beschreibung:

Die Vergabe von Schlüsseln und Transpondern 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- bzw. Transponder-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.

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

2.5. Manuelles Schließsystem

Beschreibung:

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

Risiken:

Zutritt Unbefugter

Verhaltensregeln:

-

2.6. Personenkontrolle beim Empfang

Beschreibung:

Durch die Personenkontrolle beim Pförtner/am Empfang wird das Gebäude vor unbefugtem Zutritt gesichert.

Risiken:

Zutritt Unbefugter

Verhaltensregeln:

-

2.7. Sicherheitsschlösser

Beschreibung:

Mithilfe von Sicherheitsschlössern wird das Gebäude vor unbefugtem Zutritt gesichert.

Risiken:

Zutritt von Unbefugten, Diebstahl

Verhaltensregeln:

-

2.8. Sorgfältige Auswahl von Reinigungspersonal (extern)

Beschreibung:

Das Reinigungspersonal (extern) wird sorgfältig ausgewählt.
Darüber hinaus ist im Vertrag mit dem externen Reinigungsdienst eine Verpflichtung auf Vertraulichkeit und das Datengeheimnis eingearbeitet.
Die tatsächlichen Verpflichtungserklärungen werden im Rahmen regelmäßiger Kontrollaudits überprüft.

Risiken:

Zutritt Unbefugter

Verhaltensregeln:

Unzulässiges Verhalten des Reinigungspersonals muss unverzüglich der Geschäftsleitung gemeldet werden.

2.9. Türen mit Knauf an der Außenseite

Beschreibung:

Türen sind überwiegend mit Außenknauf ausgestattet. Ein Türdrücker ist nur auf der Innenseite angebracht. Der Außenknauf verhindert ein Öffenen einer nicht verriegelten Türe von außen.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Technische Maßnahme

2.10. 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.

2.11. Türsprechsystem mit Kamera

Beschreibung:

Zur Identifizierung von Einlass suchenden Personen wird eine technische Einrichtung mit einer Freisprecheinrichtung und einer Videoübertragung für den Einlass zum Gebäude eingesetzt. Personen die Zutritt zum Gebäude möchten, können mit Hilfe der Türsprechanlage mit Kamera mit dem Auge erkannt werden, bevor der Türöffner betätigt wird. Damit wird der Zutritt von unbefugten Personen verhindert.

Risiken:

Zutritt von Unbefugten

Verhaltensregeln:

Technische Maßnahme

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 oder in einer unverschlüsselten Datei aufbewahrt werden.

3.2. Automatische Bildschirm-Sperrung

Beschreibung:

Alle im Einsatz befindlichen Arbeitsplatzrechner (PCs, Macs) rufen nach Inaktivität automatisch die Anmeldemaske des jeweiligen Betriebssystems auf. Ein Zugriff auf die Arbeitsplatzrechner ist dann nur nach vorheriger Eingabe des Nutzerpassworts möglich. So wird verhindert, dass Unbefugte beispielsweise während der Pausenzeiten Zugriff auf kritische Daten erlangen können.

Risiken:

Nutzung durch Unbefugte

Verhaltensregeln:

Die Bildschirmsperre darf nicht entfernt werden.

3.3. BIOS Schutz (separates Passwort)

Beschreibung:

Durch Vergabe eines gesonderten BIOS-Passworts wird sichergestellt, dass keine unberechtigte Person einen Computer ohne Eingabe dieses Passworts booten kann. Dadurch wird eine zusätzliche Sicherheitsbarriere aufgestellt, die Angreifer abhaltet an Daten zu gelangen. Für die Vergabe des BIOS-Passworts gelten die allgemein gültigen Regelungen für die Passwortsicherheit.

Risiken:

Zugriff von Unberechtigten, Diebstahl von Daten

Verhaltensregeln:

Technische Maßnahme

3.4. 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:

-

3.5. Dokumentierte Schlüssel- und Transpondervergabe

Beschreibung:

Die Vergabe von Schlüsseln und Transpondern 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- bzw. Transponder-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.

3.6. Einrichtung eines Accounts pro User

Beschreibung:

Sowohl für interne als auch für externe Systeme werden grundsätzlich personalisierte Logins vergeben. So kann sichergestellt werden, dass durchgeführte Aktionen nachträglich dem jeweiligen Benutzer zugeordnet werden können. Zudem können einzelne Zugänge zielgerichtet gesperrt oder gelöscht werden, ohne dass dies Einfluss auf die Zugänge anderer Mitarbeiter hat. Sammelaccounts werden vermieden.

Risiken:

Unbefugte Nutzung

Verhaltensregeln:

-

3.7. 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 im Zuge dessen werden die angelegten Firewall-Richtlinien überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Risiken:

Hacking

Verhaltensregeln:

-

3.8. 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 werden im Zuge dessen überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Risiken:

Hacking

Verhaltensregeln:

-

3.9. Einsatz von 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:

Hacking, Trojaner, Viren, Ransomware

Verhaltensregeln:

Einstellungen werden zentral von der IT-Abteilung/dem externen Dienstleister gesteuert.

3.10. Einsatz von geschütztem Wireless LAN (WLAN)

Beschreibung:

Das eingesetzte WLAN ist auf dem aktuellen Stand der Technik hinsichtlich der Security Implementierung. Bei der Positionierung der WLAN-Komponenten wurde darauf geachtet, dass diese vor unautorisiertem physischem Zugriff geschützt sind. Der Zugang zum Access-Point ist nicht über Standardpasswörter möglich. Das Passwort für einen Pre- Shared-Key muss gewisse Mindest-Anforderungen erfüllen.
Dass Verwenden von WPS ist untersagt und diese Funktion ist zu deaktivieren. Es wird dafür Sorge getragen, dass die WLAN-Komponenten regelmäßige Firmware-/Software-Updates erhalten.

Risiken:

Hacking, Zugriff von Unberechtigten

Verhaltensregeln:

Technische Maßnahme

3.11. Richtlinie Clear Screen (manuelle Desktopsperre)

Beschreibung:

Computer oder andere Geräte mit Benutzer-Login sind bei jedem Verlassen des Arbeitsplatzes zu sperren (auch bei kurzen Pausen). Der Zuständige hat die Mitarbeiter über diese Maßnahme informiert und die Durchsetzung der Maßnahme wird regelmäßig geprüft.

Risiken:

Dateneinsicht durch Unberechtigte

Verhaltensregeln:

Organisatorische Maßnahme

3.12. Richtlinie Datenschutz und Datensicherheit

Beschreibung:

Es wurde eine allgemein gültige Richtlinie zum Datenschutz und zur Datensicherheit erstellt, die für alle Mitarbeiter verpflichtend einzuhalten ist. In dieser werden die Grundsätze und Rollen im Datenschutz sowie diverse Verhaltensregeln festgelegt. Die Richtlinie wird periodisch überarbeitet und an den aktuellen Stand angepasst.

Risiken:

Datenschutzwidriges Verhalten, Dateneinsicht durch Unberechtigte

Verhaltensregeln:

Organisatorische Maßnahme

3.13. Sicherheitsschlösser

Beschreibung:

Mithilfe von Sicherheitsschlössern wird das Gebäude vor unbefugtem Zutritt gesichert.

Risiken:

Nutzung von Unbefugten

Verhaltensregeln:

-

3.14. Sorgfältige Auswahl von Reinigungspersonal (extern)

Beschreibung:

Das Reinigungspersonal (extern) wird sorgfältig ausgewählt.
Darüber hinaus ist im Vertrag mit dem externen Reinigungsdienst eine Verpflichtung auf Vertraulichkeit und das Datengeheimnis eingearbeitet.
Die tatsächlichen Verpflichtungserklärungen werden im Rahmen regelmäßiger Kontrollaudits überprüft.

Risiken:

Zutritt Unbefugter

Verhaltensregeln:

Unzulässiges Verhalten des Reinigungspersonals muss unverzüglich der Geschäftsleitung gemeldet werden.

3.15. Verschlüsselung von Datenträgern in Laptops/Notebooks

Beschreibung:

Datenträger in Laptops/Notebooks werden verschlüsselt, um im Falle eines Verlustes die Nutzung durch Unbefugte auszuschließen.

Risiken:

Nutzung durch Unbefugte bei Verlust

Verhaltensregeln:

-

3.16. 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:

-

3.17. Zuordnung von Benutzerprofilen zu IT-Systemen

Beschreibung:

IT-Systemen werden Benutzerprofile, die auf die notwendigen Rechte beschränkt sind, zugeordnet, um die Nutzung durch Unbefugte zu verhindern.

Risiken:

Nutzung durch Unbefugte

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. 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:

-

4.3. physische Löschung von Datenträgern vor Wiederverwendung

Beschreibung:

Werden Daten mit personenbezogenem Inhalt auf lokalen Datenträgern gelöscht, erfolgt dies grundsätzlich durch Anwendung spezieller Löschprogramme. So werden auch vom Betriebssystem angelegte Schattenkopien sowie Daten auf SSD-Speichermedien zuverlässig gelöscht. Eine nachträgliche Wiederherstellung der gelöschten Daten ist so nicht mehr möglich.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.4. Protokollierung der Vernichtung

Beschreibung:

Die Vernichtung der Daten(-träger) wird protokolliert.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.5. Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten

Beschreibung:

Es ist sichergestellt, dass jeder Zugriff in relevanten Anwendungen protokolliert und damit nachvollziehbar ist. Die Zugriffsprotokolle werden periodisch auf Unregelmäßigkeiten hin ausgewertet.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.6. 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:

-

4.7. Sichere Aufbewahrung von Datenträgern

Beschreibung:

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

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.8. Sicheres Löschen nicht mehr benötigter Daten

Beschreibung:

Nicht mehr benötigte Daten wie zum Beispiel veraltete Kunden- sowie Projektdaten oder Daten aus Test- bzw. Entwicklungsumgebungen werden gelöscht, sobald diese nicht mehr für die jeweilige Vertragserfüllung benötigt werden. Die Löschung erfolgt unter Zuhilfenahme spezieller Löschprogramme, welche eine nachträgliche Wiederherstellung der Daten unmöglich machen.

Risiken:

-

Verhaltensregeln:

-

4.9. Sperrung von Zugängen beim Austritt von Mitarbeitern

Beschreibung:

Verlässt ein Mitarbeiter das Unternehmen, so erfolgt noch vor dessen Austritt die Sperrung bzw. Löschung aller ihm zugewiesenen Zugänge für interne und externe Systeme. Als Basis für diesen Vorgang wird die Dokumentation der zuvor angelegten Zugänge verwendet. In der Dokumentation wird abschließend ebenfalls die Sperrung bzw. Löschung der Zugänge vermerkt.

Risiken:

-

Verhaltensregeln:

-

4.10. Verschlüsselung von Datenträgern und Dateien

Beschreibung:

Datenträger und Dateien werden verschlüsselt, um im Falle eines Verlustes die Nutzung durch Unbefugte auszuschließen.

Risiken:

Datenzugriff durch Unbefugte bei Verlust

Verhaltensregeln:

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

4.11. Verwaltung der Rechte durch externen Dienstleister

Beschreibung:

Die Verwaltung der Rechte wird durch einen externen Dienstleister (Auftragsverarbeiter gem. § 29 KDG/Art. 28 DSGVO, Vertrag zur Auftragsverarbeitung unterzeichnet) durchgeführt.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.12. Verwaltung der Rechte durch Systemadministrator

Beschreibung:

Die Rechte werden durch den Systemadministrator verwaltet.

Risiken:

Datenzugriff durch Unbefugte

Verhaltensregeln:

-

4.13. Zentrale Verwaltung von Benutzerzugängen und -rechten

Beschreibung:

Zur Dokumentation aller Zugänge für interne und externe Systeme kommt eine Software zum Einsatz, in der alle Informationen zu Mitarbeitern sowie zu deren Zugängen erfasst werden. Die softwaregestützte Erfassung und Verwaltung aller Benutzerzugänge stellt u. a. sicher, dass beim Austritt von Mitarbeitern alle für diese angelegten Zugänge vollständig gesperrt bzw. gelöscht werden.

Risiken:

-

Verhaltensregeln:

-

5. Trennungsgebot

5.1. Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

Beschreibung:

Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System.

Risiken:

Datenverlust, Datenpanne

Verhaltensregeln:

-

5.2. Logische Mandantentrennung (softwareseitig)

Beschreibung:

Je höher der Schutzbedarf und das Risiko für personenbezogene Daten ist, desto höher sind die Ansprüche an Mandantentrennung. Daher wird darauf geachtet, dass relevante Datenanwendungen jedenfalls mandantenfähig sind. Es wird damit sichergestellt, dass mehrere Nutzer Anwendungen gleichzeitig verwenden können, ohne die Daten der anderen User einsehen zu können. Die Mandantenfähigkeit ist ein wichtiges Auswahlkriterien bei der Anschaffung von relevanten Softwareprodukten.

Risiken:

Datenverlust, Datenpanne

Verhaltensregeln:

-

5.3. Steuerung der Datentrennung über ein Berechtigungskonzept

Beschreibung:

Eine Trennung der Daten zu unterschiedlichen Zwecken erfolgt über ein sorgfältig erarbeitetes Berechtigungskonzept, welches den Zugriff auf personenbezogene Daten regelt. Die Datentrennung erfolgt dabei virtuell. Es ist sichergestellt, dass Nutzer nur die unbedingt erforderlichen Berechtigungen erhalten und diese nach Wegfall der Erforderlichkeit auch wieder entzogen werden.

Risiken:

Datenverlust, Datenpanne

Verhaltensregeln:

-

5.4. Trennung von internem WLAN und Gäste-WLAN

Beschreibung:

Gäste, denen ein Zugang zum Internet ermöglicht werden soll, erhalten einen individualisierten Zugang oder die Zugangsdaten zu einem eigenen WLAN. Von diesem separaten WLAN aus ist ein Zugriff auf das firmeninterne Netzwerk und

alle dort hinterlegten Daten nicht möglich. So wird verhindert, dass Gäste unberechtigterweise auf personenbezogene Daten im Firmennetzwerk zugreifen können.

Risiken:

-

5.5. Verbot der Nutzung privater Endgeräten im Firmennetzwerk

Beschreibung:

Die Nutzung privater Laptops oder Speichermedien wie Festplatten oder USB-Sticks, die nicht durch die Firma ausgegeben wurden, ist den Mitarbeitern im Unternehmen nicht gestattet. Eine entsprechende Erklärung wurde durch jeden Mitarbeiter unterzeichnet. So werden mögliche Schäden an kritischen IT- Systemen durch bewusst oder unbewusst eingeschleuste Schadsoftware verhindert und bereits kompromittierte Systeme aus dem Firmennetzwerk ferngehalten. Einzig Geräte, über die keine fremden Daten ins Firmennetzwerk übertragen werden können (z. B. Mäuse oder Tastaturen), dürfen nach ausdrücklicher Genehmigung im Unternehmen genutzt werden.

Risiken:

-

Verhaltensregeln:

-

5.6. Versehen der Datensätze mit Zweckattributen/Datenfeldern

Beschreibung:

Datensätze werden mit Datenfeldern ergänzt, die Eigenschaften und Zweck des jeweiligen Datensatzes bezeichnen. Das Zweckattribut beschreibt damit einen Datensatz näher. Dadurch kann die zweckgebundene Datenverarbeitung besser sicher gestellt werden.

Risiken:

Datenverlust, Datenpanne

Verhaltensregeln:

-

6. Pseudonymisierung

6.1. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Beschreibung:

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:

Datenverlust, Datenpanne

Verhaltensregeln:

-

7. Datenintegrität

7.1. Erläuterung der technischen und organisatorischen Maßnahmen zur Wahrung der Datenitegrität

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 Datenintegrität werden auf den folgenden Seiten erläutert.

8. Weitergabekontrolle

8.1. Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

Beschreibung:

Beim physischen Transport personenbezogener Daten (z. B. Übermittlung großer Datenmengen auf einer Blu-ray Disc durch einen Kurier) werden nur ausgesuchte und zuverlässige Transportunternehmen mit einwandfreier Reputation beauftragt, die zudem über die notwendige Erfahrung für einen Transport von sensiblen Daten verfügen. Auch die Verfügbarkeit geeigneter Transportfahrzeuge hat Einfluss auf die Auswahl. Nach erfolgreicher Übermittlung wird zudem die Rückmeldung des Empfängers eingeholt, welcher ebenfalls zu seiner Erfahrung mit dem Transportunternehmen befragt wird.

Risiken:

Dateneinsicht durch Dritte

Verhaltensregeln:

-

8.2. 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:

-

8.3. Fax-Protokoll

Beschreibung:

In einem Fax-Protokoll wird der Verbindungsaufbau, die Übertragung von Rufnummer, Datum und Uhrzeit sowie die Empfangsquittierung definiert. Somit kann nach der Übermittlung diese nochmals überprüft werden. Mit der Ablage dieses Protokolls ist ein der Rechenschaftspflicht angemessenes Nachhalten der Übertragungsparameter möglich.

Risiken:

-

Verhaltensregeln:

Die Aufbewahrung gilt insbesondere für die Übertragung sensibler Daten mit dem Fax.

8.4. 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:

-

8.5. 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.

8.6. Verschlüsselung von E-Mails

Beschreibung:

Werden Daten digital ausgetauscht, die unter Umständen personenbezogene Daten enthalten könnten, 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:

-

8.7. Verwendung verschlüsselter Übertragungswege für den Datenaustausch

Beschreibung:

Werden Daten digital ausgetauscht, die unter Umständen personenbezogene Daten enthalten könnten, 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:

-

Verhaltensregeln:

-

9. Eingebekontrolle

9.1. Datenschutzfreundliche Voreinstellungen

Beschreibung:

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

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

9.2. Dokumentenmanagement

Beschreibung:

Im Rahmen des Dokumentenmanagements wurde ein Dokumentenmanagementsystem eingeführt, das die Datenintegrität durch nachvollziehbares Loggen der Änderungen an Datensätzen fördert.

Risiken:

Verfälschung von Daten, Datenverlust

Verhaltensregeln:

-

9.3. Interne Meldewege für Prozesse festgelegt

Beschreibung:

Für Prozesse (z. B. Schulungen, Betroffenenrechte, Löschung ...) wurden bereits diverse interne Meldewege festgehalten. Diese werden regelmäßig auditiert und angepasst. Darüber hinaus wird regelmäßig überprüft, ob für weitere Prozesse interne Meldewege für eine sichere Abwicklung dieser datenschutzrelevanten Prozesse von Nöten sind.

Risiken:

-

Verhaltensregeln:

Die internen Meldewege sind in jedem Fall einzuhalten.

9.4. Protokollierung der Eingabe, Änderung und Löschung von Daten

Beschreibung:

Die Eingabe, Änderung und Löschung von Daten wird protokolliert.

Risiken:

Verfälschung von Daten, unberechtigter Zugriff

Verhaltensregeln:

-

9.5. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

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:

Verfälschung von Daten, Datenverlust

Verhaltensregeln:

-

9.6. Vier-Augen-Prinzip

Beschreibung:

Im Fall von risikoreichen oder komplexen Verarbeitungen wird das Vier-Augen-Prinzip angewandt. Dies kann auch für einfache Verarbeitungen gelten, die einen großen Datenumfang aufweisen, z. B. Kontrolle von ausführlichen Tabellen auf die Richtigkeit der Angaben oder Tippfehler.

Risiken:

-

Verhaltensregeln:

Das Vier-Augen-Prinzip ist soweit vorgeschrieben unbedingt anzuwenden.

10. Verfügbarkeitskontrolle und Belastbarkeit

10.1. Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Beschreibung:

Die Datensicherung wird an einem sicheren, ausgelagerten Ort aufbewahrt.

Risiken:

Datenverlust

Verhaltensregeln:

-

10.2. 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 an die betroffenen Kunden, zum anderen können auf Basis dieser Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.

Risiken:

-

Verhaltensregeln:

-

10.3. 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:

-

10.4. 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 die angelegten Firewall-Richtlinien dabei überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Risiken:

Datenverlust

Verhaltensregeln:

-

10.5. 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 werden dabei überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Risiken:

Datenverlust

Verhaltensregeln:

-

10.6. 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.

10.7. Erstellen eines Backup- & Recoverykonzepts

Beschreibung:

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

Risiken:

Datenverlust

Verhaltensregeln:

-

10.8. Feuer- und Rauchmeldeanlagen

Beschreibung:

Im Serverraum sind Feuer- und Rauchmeldeanlagen vorhanden.
Zur Vermeidung von Schäden durch Feuer werden Brandmelder verwendet. Diese wurden in jedem Bereich des Bürogebäudes angebracht und untereinander vernetzt. Im unwahrscheinlichen Fall eines Feuers kann so der betroffene Bereich schnell identifiziert und mit Hilfe öffentlich zugänglicher Feuerlöscher bei Bedarf gelöscht werden. Die Brandmeldeanlage wird regelmäßig durch ein Spezialunternehmen gewartet, um deren ordnungsgemäße Funktion sicherzustellen.

Risiken:

Datenverlust

Verhaltensregeln:

-

10.9. IT-Sicherheitskonzept inkl. Notfallplan

Beschreibung:

Für die aus Datenschutzsicht kritischen Prozesse im Unternehmen wurden spezielle Notfallpläne sowie ein IT-Sicherheitskonzept erstellt. Diese beinhalten Informationen zum geplanten Vorgehen in datenschutzrelevanten Notfallsituationen (z. B. Verlust personenbezogener Daten). Auch die notwendigen Kommunikationsinhalte, -kanäle und -empfänger werden konkret benannt, um sicherzustellen, dass alle betroffenen Personen zeitnah über den jeweiligen Notfall informiert werden. Welche Prozesse als kritisch einzustufen sind, wurde von allen Datenschutzverantwortlichen im Unternehmen gemeinsam definiert. Eine zukünftige Erweiterung des Konzeptes sowie der Notfallpläne wird durch das gleiche Gremium initiiert und durchgeführt.

10.10. Monitoring durch Auftragsverarbeiter

Beschreibung:

Der Auftragsverarbeiter betreibt Monitoring, damit ein möglicher Angriff auf die IT-Systeme erkannt und verhindert werden kann.

Risiken:

-

Verhaltensregeln:

-

10.11. 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:

-

10.12. 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:

-

10.13. Unterbrechungsfreie Stromversorgung (USV)

Beschreibung:

Kritische IT-Systeme wie beispielsweise Server, auf denen Unternehmens- oder Kundendaten gespeichert werden, sind mit einer USV vor kurzzeitigen Stromausfällen geschützt. So können kritische IT-Systeme bei Stromausfällen gezielt heruntergefahren und unerwünschte Datenverluste vermieden werden. Bei einer Erweiterung von kritischen IT-Systemen wird auch die Kapazität der USV entsprechend angepasst, um einen ordnungsgemäßen Betrieb für einen bestimmten Zeitraum sicherzustellen. Die unterbrechungsfreie Stromversorgung wird regelmäßig durch ein Spezialunternehmen gewartet, um deren ordnungsgemäße Funktion sicherzustellen.

Risiken:

Datenverlust

Verhaltensregeln:

-

10.14. Verwendung von RAID-Systemen

Beschreibung:

Zum Schutz vor Hardwareausfällen und Datenverlusten durch defekte Festplatten werden diese in kritischen IT-Systemen (z. B. lokale Datei- oder Entwicklungsserver) in Form eines RAID-Systems verbaut. In diesem werden Daten auf mindestens zwei Festplatten gespeichert. Auf die in einem RAID- System gespeicherten Daten kann somit auch bei einem Ausfall einer Festplatte weiterhin zugegriffen werden. Defekte Festplatten werden umgehend vom System gemeldet und können entsprechend ausgetauscht werden. Ein Datenverlust kann so vermieden werden.

Risiken:

-

Verhaltensregeln:

-

11. Auftragskontrolle

11.1. 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:

-

11.2. Auftragsverarbeiter hat Datenschutzbeauftragten bestellt

Beschreibung:

Der Auftragsverarbeiter hat einen Datenschutzbeauftragten bestellt (soweit notwendig).

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

11.3. 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:

-

11.4. 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 Maßnahmen im Rahmen von Auftragsverarbeitungen werden auf den folgenden Seiten erläutert.

11.5. Interne Meldewege für Prozesse festgelegt

Beschreibung:

Für Prozesse (z. B. Schulungen, Betroffenenrechte, Löschung ...) wurden bereits diverse interne Meldewege festgehalten. Diese werden regelmäßig auditiert und angepasst. Darüber hinaus wird regelmäßig überprüft, ob für weitere Prozesse interne Meldewege für eine sichere Abwicklung dieser datenschutzrelevanten Prozesse von Nöten sind.

Risiken:

-

Verhaltensregeln:

Die internen Meldewege sind in jedem Fall einzuhalten.

11.6. 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:

-

11.7. laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

Beschreibung:

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

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

11.8. 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:

-

11.9. schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)

Beschreibung:

Mit allen Dienstleistern, Partnern und Kunden, mit denen ein Austausch sowie eine Verarbeitung personenbezogener Daten erfolgt, wird ein Vertrag zur Auftragsdatenverarbeitung (AV-Vertrag) gemäß Art. 28 DSGVO 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.

11.10. 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:

-

11.11. 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:

-

11.12. Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis

Beschreibung:

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

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

11.13. vorherige Prüfung der Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen

Beschreibung:

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

Risiken:

Missbräuchliche Verwendung der Personendaten

Verhaltensregeln:

-

11.14. Weisungsbefugnisse festlegen

Beschreibung:

Im Rahmen von Auftragsverarbeitungen oder allgemein externen Dienstleistungen wurden Weisungsbefugnisse festgelegt. Diese führen dazu, dass Kommunikationsfehler weniger wahrscheinlich sind, da beide Seiten klare Ansprechpersonen haben und somit der Kommunikationsfluss transparenter ist.

Risiken:

-

Verhaltensregeln:

Die Kommunikation über die weisungsbefugten Beschäftigten ist einzuhalten.

11.15. Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart

Beschreibung:

Gemäß dem Vertrag wurden wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter 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:

-

11.16. Zuteilung datenschutzrelevanter Verantwortungsbereiche

Beschreibung:

Datenschutzrelevante Verantwortungsbereiche werden je nach Tätigkeitsbereich auf Mitarbeiter verteilt. Dabei wird die Eignung der Mitarbeiter für den jeweiligen Verantwortungsbereich stets sichergestellt. Ggf. notwendige Schulungen oder Fortbildungen erfolgen vor der Übertragung eines Verantwortungsbereichs an einen Mitarbeiter. Alle datenschutzrelevanten Verantwortungsbereiche werden schriftlich festgehalten und auch in AV-Verträgen mit Endkunden berücksichtigt. Bei Austritt eines Mitarbeiters wird unverzüglich ein geeigneter Nachfolger benannt.

Risiken:

-

Verhaltensregeln:

-