# Technisch Organisatorische Maßnahmen

## Katholischer Deutscher Frauenbund Diözesanverband Berlin e.V.

Wundtstr. 40-44
14057 Berlin
Deutschland

# 1. Zutrittskontrolle

## 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. 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 ohne Berechtigungsausweis, 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.

## 2.2. 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. 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.

## 2.4. Festlegung der zutrittsberechtigten Personen

**Beschreibung:**

Im Rahmen des Sicherheitskonzepts wird festgelegt, welche Personen Zutrittsrechte für die Räumlichkeiten erhalten. (Hier werden auch Honorarkräfte und ggf. ehrenamtliche Vorstände einbezogen.)

**Risiken:**

Zutritt von Unbefugten

**Verhaltensregeln:**

-

## 2.5. 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 ohne Berechtigungsausweis, 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.

## 2.6. Manuelles Schließsystem

**Beschreibung:**

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

**Risiken:**

Zutritt Unbefugter

**Verhaltensregeln:**

-

## 2.7. 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. 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. 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 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:**

Nutzung von Unbefugten

**Verhaltensregeln:**

Der Verlust eines Schlüssels ist unverzüglich der Geschäftsleitung zu melden.

## 3.4. 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:**

-

## 3.5. 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:**

-

## 3.6. 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.

## 3.7. 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 Unbefugter, Hacking

**Verhaltensregeln:**

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

## 3.8. Einsatz von Zwei-Faktor-Authentifizierung

**Beschreibung:**

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

**Risiken:**

Unbefugte Nutzung

**Verhaltensregeln:**

-

## 3.9. 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 Unbefugter

**Verhaltensregeln:**

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

## 3.10. Protokollierung der Zugänge

**Beschreibung:**

Die Zugänge zu IT-Systemen werden protokolliert, um unbefugte Nutzung nachweisen zu können. Darüber hinaus werden IP-Adressen auch beschränkt, soweit geprüft wurde, dass eine mögliche Gefahr von diesen ausgehen kann.

**Risiken:**

Unbefugte Nutzung

**Verhaltensregeln:**

-

## 3.11. 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.

## 3.12. 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:**

-

# 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 Unbefugter

**Verhaltensregeln:**

-

## 4.3. Erstellung eines Berechtigungskonzepts

**Beschreibung:**

Für alle IT-Systeme wird ein Berechtigungskonzept erstellt, das regelmäßig auf Richtigkeit der Angaben überprüft wird.

**Risiken:**

Datenverlust, Datenpanne

**Verhaltensregeln:**

-

## 4.4. Festlegung der personellen Zuständigkeiten (verbindliche Berechtigungsverfahren)

**Beschreibung:**

Personelle Zuständigkeiten sowie verbindliche Berechtigungsverfahren werden (für Beschäftigte des Auftragsverarbeiters) festgelegt.

**Risiken:**

Datenzugriff durch Unbefugte

**Verhaltensregeln:**

-

## 4.5. 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:**

-

## 4.6. 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:**

Datenzugriff durch Unbefugte

**Verhaltensregeln:**

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

## 4.7. Protokollierung der Vernichtung

**Beschreibung:**

Die Vernichtung der Daten(-träger) wird protokolliert.

**Risiken:**

Datenzugriff durch Unbefugte

**Verhaltensregeln:**

-

## 4.8. 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:**

-

## 4.9. Sichere Aufbewahrung von Datenträgern

**Beschreibung:**

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

**Risiken:**

Datenzugriff durch Unbefugte

**Verhaltensregeln:**

-

## 4.10. 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.

**Risiken:**

-

**Verhaltensregeln:**

-

## 4.11. Sicherheitsupdates (Auftragsverarbeiter)

**Beschreibung:**

Unberechtigtem Zugriff wird durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) (durch den Auftragsverarbeiter) entgegengewirkt.

**Risiken:**

Unberechtigter Zugriff

**Verhaltensregeln:**

-

## 4.12. 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:**

-

## 4.13. 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.

## 4.14. 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:**

-

## 4.15. Verwaltung der Rechte durch Systemadministrator

**Beschreibung:**

Die Rechte werden durch den Systemadministrator verwaltet.

**Risiken:**

Datenzugriff durch Unbefugte

**Verhaltensregeln:**

-

### 4.16. 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. Datenintegrität

### 5.1. 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.

## 6. Weitergabekontrolle

### 6.1. 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:**

-

## 6.2. 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:**

-

## 6.3. 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.

## 6.4. Verwendung von SSL-Zertifikaten für Hostingumgebungen

**Beschreibung:**

Alle von uns betreuten Webseiten sowie die hierfür genutzten Hostingumgebungen, über die personenbezogene Daten über das Internet übermittelt werden, z. B. durch Kontaktformulare oder Eingabemasken, werden von uns mit SSL-Zertifikaten geschützt. Die Zertifikate werden in regelmäßigen Abständen neu ausgestellt, um einen Diebstahl des Zertifikats und somit das Abgreifen von Daten zu verhindern.

**Risiken:**

-

**Verhaltensregeln:**

-

# 7. Eingebekontrolle

## 7.1. Datenlöschung nach Auftragsbeendigung (Auftragsverarbeiter)

**Beschreibung:**

Eine datenschutzgerechte Löschung der Daten nach der Auftragsbeendigung durch den Auftragsverarbeiter wird vertraglich festgelegt und nach Vertragsende kontrolliert.

**Risiken:**

Verletzung der Datenintegrität

**Verhaltensregeln:**

-

## 7.2. 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:**

-

## 7.3. Protokollführung Meetings

**Beschreibung:**

Besprechungsinhalte von internen Meetings, Gremiensitzungen oder anderen Zusammenkünften werden in einem Protokoll (Aufzeichnung der Inhalte und Absprachen einer internen Zusammenkunft (Ergebnisprotokoll)) festgehalten, teilweise werden die Inhalte der Reden und Diskussionen der Teilnehmenden wiedergegeben (Verlaufsprotokoll).

**Risiken:**

-

**Verhaltensregeln:**

-

# 8. Verfügbarkeitskontrolle und Belastbarkeit

## 8.1. Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

**Beschreibung:**

Die Datensicherung wird an einem sicheren, ausgelagerten Ort aufbewahrt.

**Risiken:**

Datenverlust

**Verhaltensregeln:**

-

## 8.2. 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:**

-

## 8.3. 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:**

-

## 8.4. 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:**

-

## 8.5. 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.

## 8.6. Erstellen eines Backup- & Recoverykonzepts

**Beschreibung:**

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

**Risiken:**

Datenverlust

**Verhaltensregeln:**

-

## 8.7. 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:**

-

## 8.8. Getrennte Aufbewahrung der Sicherungen

**Beschreibung:**

Die Sicherungen werden an unterschiedlichen sicheren Orten aufbewahrt.

**Risiken:**

Datenverlust

**Verhaltensregeln:**

-

## 8.9. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)v

**Beschreibung:**

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

**Risiken:**

-

**Verhaltensregeln:**

-

## 8.10. 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:**

-

## 8.11. 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:**

-

# 9. Auftragskontrolle

## 9.1. 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:**

-

## 9.2. Auftragnehmer hat Datenschutzbeauftragten bestellt

**Beschreibung:**

Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt (soweit notwendig).

**Risiken:**

Missbräuchliche Verwendung der Personendaten

**Verhaltensregeln:**

-

## 9.3. Auftragskontrolle (Verträge)

**Beschreibung:**

Im Rahmen der implementierten Auftragskontrolle wird insbesondere eine eindeutige Vertragsgestaltung, ein formalisiertes Auftragsmanagement und eine strenge Auswahl des Dienstleisters beachtet. Darüber hinaus besteht eine Vorabüberzeugungspflicht und es werden Nachkontrollen angesetzt.

**Risiken:**

Missbräuchliche Verwendung der Personendaten

**Verhaltensregeln:**

Bei der Einbeziehung eines (neuen) externen Dienstleisters muss im Sinne der Auftragskontrolle der Vorgesetzte sowie ggf. der Datenschutzbeauftragte vor Vertragsunterzeichnung einbezogen werden.

## 9.4. 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 Datenschutzniveau glaubhaft sicherstellen können.

**Risiken:**

Missbräuchliche Verwendung der Personendaten

**Verhaltensregeln:**

-

## 9.5. 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:**

-

## 9.6. 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:**

-

## 9.7. 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.

## 9.8. 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.

## 9.9. 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:**

-

## 9.10. 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:**

-

## 9.11. schriftliche Weisungen an den Auftragnehmer (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/§ 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.

## 9.12. 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:**

-

## 9.13. 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:**

-

## 9.14. 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:**

-

## 9.15. vorherige Prüfung der 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:**

-

## 9.16. 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:**

-

## 9.17. 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:**

-

# 10. Trennungsgebot

## 10.1. physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

**Beschreibung:**

Die Speicherung der Daten erfolgt physikalisch getrennt und auf gesonderten Systemen oder Datenträgern.

**Risiken:**

Datenverlust, Datenpanne

**Verhaltensregeln:**

-

## 10.2. 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:**

-

**Verhaltensregeln:**

-

## 10.3. 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:**

-

## 10.4. Verwendung von Zugriffsberechtigungen für interne Systeme

**Beschreibung:**

Alle internen Systeme sind vor unbefugtem Zugriff gesichert. Es ist nicht möglich, diese ohne eine weitere Anmeldung zu verwenden, wenn man sich im Firmennetzwerk befindet. Die Berechtigungen zur Nutzung der verschiedenen Systeme werden individuell vergeben und können individuell und systembezogen widerrufen werden. Ein genereller Zugriff auf alle im Firmennetzwerk befindlichen Daten wird somit unterbunden.

**Risiken:**

-

**Verhaltensregeln:**

-