teamware.eu
teamware.cloud
... we connect

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

Datenschutz Sicherheit

# Checkliste

**Version vom:** 2018.10.01 - 09:29

**Ausgearbeitet von:** Alex Mutschlechner – info@teamware.eu

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## Index



## Änderungsprotokoll

| | | |
|---|---|---|
| 2018-09-29 | erstellt | AM: Dokument erstellt |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 1. Einführung

Notwendig sind technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes, deren Aufwand in einem **angemessenen Verhältnis** zu dem angestrebten Schutzzweck steht. Die nachfolgenden Prüfpunkte stellen einen Überblick der grundlegenden erforderlichen Maßnahmen und Fragestellungen dar. Die Anwendung muss in Bezug auf den jeweiligen Anwendungszweck geprüft werden.

**Um den Schutz Ihrer Daten und Ihres Unternehmens gewährleisten zu können, müssen Sie kritische Fragen stellen.**

Abkürzungen:

| | |
|---|---|
| DV-Systeme | Datenverarbeitungs-Systeme |
| Mobilgeräte | PCs und Laptops, Tablets, Smartphones und jegliche andere Geräte die elektronische Daten verarbeiten. |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 2. Zutrittskontrolle:

**Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.**

**Prüffokus:**
**Welche technischen bzw. organisatorischen Maßnahmen werden zur Zutrittskontrolle, insbesondere auch zur Legitimation, eingesetzt?**

• Lage der Räume:
Sind die Zugänge der Räume ausreichend abgesichert (z. B. Türen, Türschlösser, Lichtschächte, Lüftungsöffnungen, Fenster, Verglasungsart, Rollos gegen Hochschieben, Feuerleiter, Feuertreppe, elektrische Türöffner)? Erfolgt eine Bewachung der Räumlichkeiten (z. B. durch einen Werkschutz)?
Handelt es sich um ein bewohntes Gebäude? Existiert eine Pforte und wann ist diese besetzt?

• Verschließbarkeit der Räume:
Erfolgt ein Auf- und Abschließen der Räume bei Arbeitsbeginn bzw. -ende? Gibt es ein geregeltes Konzept zur Schlüsselverwaltung? Findet eine Quittierung bei der Schlüsselausgabe statt? Wer besitzt einen Generalschlüssel?

• Überwachungseinrichtung:
Sind Alarmanlagen vorhanden? Wird der Zutritt in den Serverraum über Videokameras überwacht? Werden Bewegungssensoren eingesetzt?

• Schriftliche Festlegungen zur Zugangsberechtigung:
Tragen die Mitarbeiter den Ausweis sichtbar? Existieren hierfür klar Ausweisregelungen? Wird auf die Trennung von Bearbeitungs- und Publikumszonen geachtet? Sind schriftliche Besucherregelungen vorhanden? Werden Besuche in einem Besucherbuch dokumentiert? Wie findet die Kundenbetreuung statt (Schalterbetrieb)? Welches Zutrittskontrollsystem wird eingesetzt (z. B. Ausweisleser, Magnetkarte)?

• Reinigungs- und Wartungsarbeiten:
Ist sichergestellt, dass sowohl mit dem Reinigungspersonal als auch mit IT-Dienstleistern bei Wartungen entsprechende Regelungen getroffen sind?

• Anwesenheitskontrollen:
Wie wird die Anwesenheit überprüft (z. B. Stechuhren, Schichtbuch)? Werden auch kurzzeitige Abwesenheiten protokolliert?

• Beratung:
Findet ggf. eine Beratung durch kriminalpolizeiliche Beratungsstellen oder spezialisierte Dienstleister statt?

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | Alarmanlage | ☐ | ☐ | Schlüsselregelung / Liste |
| ☐ | ☐ | Automatisches Zugangskontrollsystem | ☐ | ☐ | Empfang / Rezeption / Pförtner |
| ☐ | ☐ | Biometrische Zugangssperren | ☐ | ☐ | Besucherbuch / Protokoll der Besucher |
| ☐ | ☐ | Chipkarten / Transpondersysteme | ☐ | ☐ | Mitarbeiter- / Besucherausweise |
| ☐ | ☐ | Manuelles Schließsystem | ☐ | ☐ | Besucher in Begleitung durch Mitarbeiter |
| ☐ | ☐ | Sicherheitsschlösser | ☐ | ☐ | Sorgfalt bei Auswahl des Wachpersonals |
| ☐ | ☐ | Schließsystem mit Codesperre | ☐ | ☐ | Sorgfalt bei Auswahl Reinigungsdienste |
| ☐ | ☐ | Absicherung der Gebäudeschächte | ☐ | ☐ | |
| ☐ | ☐ | Türen mit Knauf Außenseite | ☐ | ☐ | |
| ☐ | ☐ | Klingelanlage mit Kamera | ☐ | ☐ | |
| ☐ | ☐ | Videoüberwachung der Eingänge | ☐ | ☐ | |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 3. Zugangskontrolle:

**Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.**

**Prüffokus:**
**Welche Maßnahmen sind hinsichtlich der Benutzeridentifikation und Authentisierung technisch und organisatorisch vorhanden?**

• Firewall und Virenschutz:
Welche Produkte werden eingesetzt? Existiert eine zentrale Firewall? Welche dezentralen Lösungen werden an den Arbeitsplätzen verwendet?

• Benutzeridentifikation und Passwortverfahren:
Werden ausreichend sichere Passwörter verwendet (z.B. keine Eigennamen und Wörter aus dem Wörterbuch, auch Sonderzeichen verwenden, empfohlene Länge von min. zehn Stellen)? Ist ein regelmäßiger Passwortwechsel verpflichtend? Findet eine Auswertung der Protokolleinträge bei Falscheingaben des Passworts statt? Werden Verfahren zur Zwei-Faktor-Authentifizierung eingesetzt (z. B. Tokens, Smartcards)?

• Systemsperrung:
Erfolgt eine automatische Sperrung der Bildschirme mit Passwortschutz bei Pausen? Findet ein Sperren eines Zugangs bei mehr als drei Anmelde-Fehlversuchen statt? Hat die Falscheingabe eines Passworts eine zeitliche Verzögerung für einen Neuversuch zur Folge?

• Benutzerkennungen:
Wird auf Gruppenkennungen verzichtet? Besteht ein eigenes Benutzerkonto für jeden Mitarbeiter (d. h. Einrichtung eines Benutzerstammsatzes)?

• Verschlüsselung:
Werden Datenträger verschlüsselt? Welche Verschlüsselungsverfahren kommen zum Einsatz?

• Geräteanschlüsse:
Sind die relevanten PCs ohne USB-Steckplätze bzw. DVD/CD-Laufwerke?

• Sicherheit bei Heimarbeiten/Telearbeiten:
Wird auch bei fernangebundenen Arbeitsplätzen für ausreichende Sicherheit gesorgt?

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

**Checkliste:**

| Ja | Nein | Technische Maßnahmen | Ja | Nein | Organisatorische Maßnahmen |
|---|---|---|---|---|---|
| ☐ | ☐ | Login mit Passwort oder biometrisch am Server | ☐ | ☐ | Erstellen von Benutzerprofilen |
| ☐ | ☐ | Login mit Passwort oder biometrisch am Client | ☐ | ☐ | Verwalten von Benutzerberechtigungen |
| ☐ | ☐ | Login mit Passwort oder biometrisch an mobilen Geräten | ☐ | ☐ | Richtlinie „Löschen / Vernichten“ |
| ☐ | ☐ | Anti-Viren-Software Server | ☐ | ☐ | Richtlinie „Clean desk“ |
| ☐ | ☐ | Anti-Virus-Software Clients | ☐ | ☐ | Richtlinien für „Heimarbeit/Telearbeit“ |
| ☐ | ☐ | Anti-Virus-Software mobile Geräte | ☐ | ☐ | Allg. Richtlinie Datenschutz/Sicherheit |
| ☐ | ☐ | Firewall | ☐ | ☐ | Mobile Device Policy |
| ☐ | ☐ | Intrusion Detection Systeme | ☐ | ☐ | Anleitung „Manuelle Desktopsperre“ |
| ☐ | ☐ | Mobile Device Management | ☐ | ☐ | |
| ☐ | ☐ | Einsatz VPN bei Remote-Zugriffen | ☐ | ☐ | |
| ☐ | ☐ | Verschlüsselung von Client-Datenträgern | ☐ | ☐ | |
| ☐ | ☐ | Verschlüsselung von mobilen Datenträgern | ☐ | ☐ | |
| ☐ | ☐ | Verschlüsselung Smartphones | ☐ | ☐ | |
| ☐ | ☐ | Gehäuseverriegelung | | | |
| ☐ | ☐ | BIOS Schutz (separates Passwort) | ☐ | ☐ | |
| ☐ | ☐ | Sperre externer Schnittstellen (USB) | ☐ | ☐ | |
| ☐ | ☐ | Automatische Desktopsperre nach angemessener Zeit | ☐ | ☐ | |
| ☐ | ☐ | Verschlüsselung von Notebooks / Tablet | ☐ | ☐ | |
| ☐ | ☐ | Einsatz von aktueller (vom Hersteller unterstützter) Hard- und Software für welche auch Sicherheitsupdates geliefert werden | ☐ | ☐ | |
| ☐ | ☐ | Zeitnahes Einspielen von Sicherheitsupdates am Server | ☐ | ☐ | |
| ☐ | ☐ | Zeitnahes Einspielen von Sicherheitsupdates am Client | ☐ | ☐ | |
| ☐ | ☐ | Zeitnahes Einspielen von Sicherheitsupdates an mobilen Geräten | ☐ | ☐ | |
| ☐ | ☐ | | ☐ | ☐ | |

**Checkliste Passwörter:**

| Ja | Nein | Technische Maßnahmen | Ja | Nein | Organisatorische Maßnahmen |
|---|---|---|---|---|---|
| ☐ | ☐ | Speicherung der Passwörter ausschließlich in sicheren Safes (Soft- und/oder Hardware) | ☐ | ☐ | Zentrale Passwortvergabe |
| ☐ | ☐ | Masterpassword im Browser aktiviert | ☐ | ☐ | Richtlinie „Sicheres Passwort“ |
| ☐ | ☐ | | ☐ | ☐ | Richtlinie „verschiedene Passwörter“ für unterschiedliche Logins |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 4. Zugriffskontrolle

**Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.**

**Prüffokus:**
**Welche Maßnahmen sind vorhanden, um die unerlaubte Tätigkeit in DV-Systemen außerhalb eingeräumter Berechtigungen zu verhindern?**

• Berechtigungskonzept und Zugriffsrechte:
Entspricht das Konzept sowohl für Anwender als auch für Administratoren den aufgabenbedingten und datenschutzrechtlichen Erfordernissen? Existieren differenzierte Berechtigungen für Auswertungen, Kenntnisnahme, Veränderung und Löschung?

• Schutz gegen unberechtigte Zugriffe:
Bestehen Schutzmaßnahmen gegen unbefugte interne und externe Zugriffe (z. B. durch Verschlüsselung, Firewalls, abschließbare Schränke)? Werden Verfahren zur Data Leak Prevention (Erkennung unerwünschter Datenabflüsse) eingesetzt? Werden regelmäßig Penetrationstests gegen Attacken von Hackern durchgeführt?

• Überwachung und Protokollierung:
Werden Zugriffe bzw. Zugriffsversuche protokolliert? Wann findet eine Auswertung der Protokolle statt? Wo und wie lange werden die Protokolle aufbewahrt (mindestens ein Jahr)?

• Datenträgerverwaltung:
Sind die Datenträger inventarisiert (Art und Anzahl)? Wird die Lagerung von Datenträgern überprüft (dauernd/zeitweise, Bestandsverzeichnisse)? Werden Nachweise über Eingang, Ausgang sowie Bestand von Datenträgern festgehalten? Wo werden die Datenträger, insbesondere mobile wie USB-Festplatten, nach Dienstschluss aufbewahrt (abschließbare Schränke, Schlüsselregelung)? Findet eine Auslagerung von Sicherungsdatenträgern statt?

• Datentrennung:
Findet eine äußerliche Kennzeichnung der eigenen Datenträger zur Unterscheidung von fremden statt? Werden Datenträger verschiedener Auftraggeber getrennt behandelt? Gibt es einen eigenen Datenträger-Pool für jeden Kunden? Besteht eine Regelung/Verbot des Einsatzes privater Datenträger?

• Datenlöschung:
Werden Datenträger vor neuer Verwendung vollständig von bestehenden Daten bereinigt? Werden Daten auf den Datenträger vor Weitergabe, wie z. B. Verkauf, gelöscht?

• Entsorgung/Vernichtung:
Werden auch Fehldrucke sorgfältig entsorgt? Werden veraltete Datenträger geregelt vernichtet (entsprechende Lagerung der zu vernichtenden Datenträger, Datenträgerlöschgeräte, Verbrennen/Zerstören)? Findet Kontrollen der tatsächlichen Vernichtung bei Dienstleistern statt (zuverlässiges

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

Entsorgungsunternehmen, vertragliche Regelung, Entsorgungsbescheinigung)? Welche Schredder werden im Unternehmen eingesetzt (Sicherheitsstufe)?

• Regelung für das Kopieren von Datenträgern:
Existieren Richtlinien für das Kopieren von Datensätzen bzw. auch für das vollständige Kopieren von Datenträgern? Besteht ein Taschenverbot bzw. erfolgen Kontrollen von Taschen?

• Regelungen für mobile Geräte:
Gibt es Anweisungen zum Umgang mit mobilen Datenträgern und Geräte (z. B. USB-Sticks, PDAs, externe Festplatten, Tablets, Smartphones)? Wird BYOD (Bring-Your-Own-Device) in der Organisation gelebt?

• Fernwartung:
Bestehen Regelungen und gezielte Kontrollen bei Wartungsarbeiten durch Dienstleister (externe Wartung und Fernwartung)?

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | Aktenschredder (mind. Stufe 3, cross cut) | ☐ | ☐ | Einsatz Berechtigungskonzepte |
| ☐ | ☐ | Externer Aktenvernichter (DIN 32757) | ☐ | ☐ | Minimale Anzahl an Administratoren |
| ☐ | ☐ | Physische Löschung von Datenträgern | ☐ | ☐ | Datenschutztresor |
| ☐ | ☐ | Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten | ☐ | ☐ | Verwaltung Benutzerrechte durch Administratoren |
| ☐ | ☐ | Sind Akten vor dem Zugriff durch unberechtigte geschützt (z.B. Aktenschränke) | ☐ | ☐ | Richtlinien zum Umgang mit internen und externen Datenträgern |
| ☐ | ☐ | Werden Zugriffe umgehend gesperrt, wenn ein Mitarbeiter die Firma verlässt | ☐ | ☐ | Richtlinien für das Kopieren von Daten |
| ☐ | ☐ | | ☐ | ☐ | Richtlinien für die Nutzung der Geräte von Mitarbeitern |
| ☐ | ☐ | | ☐ | ☐ | |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

**Checkliste Parteienverkehr:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | Haben Sie einen Diskretionsbereich eingerichtet? Diskretionslinie auf dem Boden? | ☐ | ☐ | Alle in einem Großraumbüro beschäftigten Mitarbeiter sind eindringlich bezüglich der Beachtung des Persönlichkeits-rechts geschult und sensibilisiert. |
| ☐ | ☐ | Ist der Warteraum so abgetrennt, dass Dritte keine Gespräche am Empfang (und Telefon) oder in den Arbeits-/ Behandlungsräumen mithören können? | ☐ | ☐ | |
| ☐ | ☐ | Ist der Warteraum so abgetrennt, dass Dritte keine Dokumente am Empfang oder in den Arbeits-/ Behandlungsräumen einsehen können? | ☐ | ☐ | |
| ☐ | ☐ | Monitore sind so aufgestellt, dass Dritte den Bildschirminhalt nicht mitlesen können. | ☐ | ☐ | |
| ☐ | ☐ | Ist die ununterbrochene Besetzung des Empfangs während der Öffnungszeiten gewährleistet? | ☐ | ☐ | |
| ☐ | ☐ | Alternativ: Ist sichergestellt, dass unter Abwesenheit des Mitarbeiters/Arztes keine Fremdinformationen durch den Patienten eingesehen werden können? | ☐ | ☐ | |
| ☐ | ☐ | Sind Kunden/Patienten niemals allein in einem Arbeits-/ Behandlungsraum? | ☐ | ☐ | |
| ☐ | ☐ | Werden die Anmelde- und Patienten-/Kundendaten des Betroffenen diskret erhoben? | ☐ | ☐ | |
| ☐ | ☐ | Werden die Patienten auf die Freiwilligkeit des Ausfüllens eines Anamneseformulars hingewiesen? | ☐ | ☐ | |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 5. Weitergabekontrolle

**Maßnahmen, die 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.**

**Prüffokus:**
**Welche Regelungen existieren bezüglich der Weitergabe personenbezogener Daten (elektronische Übertragung, Datentransport, Übermittlungskontrolle)?**

• Datenträgertransportart:
Welche unterschiedlichen Datenträgertransporte finden statt (z. B. nur innerhalb des Unternehmens, zur Auslagerung, zwischen Auftraggeber/-nehmer, zu Dritten)?

• Versendungsarten:
Wie werden die Daten versendet (z. B. Post, Bahn, Kuriere, Taxi, elektronisch)?

• Transportregelungen:
Sind die Bereiche festgelegt, in denen sich Datenträger befinden dürfen? Ist definiert, welche Personen die Datenträger befugt entnehmen dürfen? Gibt es schriftliche Festlegung der Transportwege und der Transportverfahren? Werden beim Transport Datenträgerbegleitpapiere ausgestellt bzw. mitgenutzt? Existiert eine verbindliche Regelung, wer als Datenempfänger fungieren darf und wer zur Weitergabe berechtigt ist? Findet eine Vollständigkeitsüberprüfung bei Rücklieferung vom Auftragnehmer statt?

• Transportsicherung:
Sind die Datenträger beim Transport durch verschlossene Transportbehälter ausreichend gesichert? Werden ausschließlich zuverlässige Boten bzw. Transportunternehmen eingesetzt? Werden durchgängig sichere Versendungsformen verwendet (z.B. Wertpaket, Einschreibesendung, Datentransport-/E-Mail-Verschlüsselung, elektronische Signatur, VPN/Virtual Private Network)? Werden elektronische Datentransporte Ende-zu-Ende verschlüsselt?

• Dokumentation:
Werden die Abruf- und Übermittlungsvorgänge dokumentiert? Wird der Eingang und Ausgang von Datenträgern durch Lieferscheine/Quittierverfahren schriftlich festgehalten? Gibt es Legitimation der Abholer, Empfangsbestätigungen, Ein-/Ausgangsbücher, Protokollierung?

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | Email-Verschlüsselung | ☐ | ☐ | Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen |
| ☐ | ☐ | Einsatz von VPN | ☐ | ☐ | Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen |
| ☐ | ☐ | Protokollierung der Zugriffe und Abrufe | ☐ | ☐ | Weitergabe in anonymisierter oder pseudonymisierter Form |
| ☐ | ☐ | Sichere Transportbehälter | ☐ | ☐ | Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen |
| ☐ | ☐ | Bereitstellung über verschlüsselte Verbindungen wie sftp, https | ☐ | ☐ | Persönliche Übergabe mit Protokoll |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 6. Eingabekontrolle

**Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.**

**Prüffokus:**

**Welche Maßnahmen werden insbesondere zur Protokollierung bei Änderungen in den Datenverarbeitungssystemen ergriffen?**

• Protokollierung:
Welche Protokollierungs- und Protokollauswertungssysteme kommen zum Einsatz? Was wird im Rahmen der Protokollierung aufgezeichnet (z. B. wer erfasst, wer hat wann was eingegeben)? Werden auch Aktivitäten der Heimarbeiter erfasst? Findet eine Kennzeichnung der erfassten Belege oder Laufzettel mit Namenszeichen/Stempel statt? Werden auch Online-Eingaben bzw. Änderungen sorgfältig protokolliert? Welche Regelungen zur Aufbewahrungsdauer der Protokolle bestehen?

• Dokumentation:
Erfolgt eine Dokumentation der Eingabeverfahren mit Festlegung der für die Erstellung von Datenträgern und der Bearbeitung von Daten Befugten (z. B. mit Stellenbeschreibung, Dienstanweisung, Geschäftsverteilungsplan)?

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | Technische Protokollierung der Eingabe, Änderung und Löschung von Daten | ☐ | ☐ | Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können |
| ☐ | ☐ | Manuelle oder automatisierte Kontrolle der Protokolle | ☐ | ☐ | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen) |
| ☐ | ☐ | | ☐ | ☐ | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |
| ☐ | ☐ | | ☐ | ☐ | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden |
| ☐ | ☐ | | ☐ | ☐ | Klare Zuständigkeiten für Löschungen |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 7. Auftragskontrolle

**Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (vgl. § 11 BDSG).**

**Prüffokus:**
**Welche Regelungen bestehen im Umgang mit Auftragnehmern?**

• Auswahl von Auftragnehmer:
Findet Auswahl der Auftragnehmer sorgfältig statt? Welche Kriterien zur Auswahl des Auftragnehmers bestehen?

• Unterauftragnehmer:
Ist das geprüfte Unternehmen selbst als Auftragnehmer tätig? Welche Auftragnehmer werden dort nach welchen Kriterien ausgewählt?

• Schriftliches Auftragsverhältnis:
Bestehen detaillierte schriftliche Regelungen der Auftragsverhältnisse und Formalisierung des gesamten Auftragsablaufes - auch zum Einsatz von Subunternehmen (Erfassung, Scannen, Entsorgung)? Gibt es eindeutige Regelungen der Zuständigkeiten und Verantwortlichkeiten (speziell auch bei der Datensicherung und beim Datenträgertransport)? Erfolgt eine formalisierte Auftragserteilung (Auftragsformular)?

• Kontrolle:
Findet eine regelmäßige Kontrolle der Arbeitsergebnisse statt (formal, inhaltlich)? Erfolgt auch eine Kontrolle der Unterauftragnehmer (z. B. durch den DSB)?

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | | ☐ | ☐ | Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation |
| ☐ | ☐ | | ☐ | ☐ | Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit |
| ☐ | ☐ | | ☐ | ☐ | Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln |
| ☐ | ☐ | | ☐ | ☐ | Schriftliche Weisungen an den Auftragnehmer |
| ☐ | ☐ | | ☐ | ☐ | Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis |
| ☐ | ☐ | | ☐ | ☐ | Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht |
| ☐ | ☐ | | ☐ | ☐ | Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer |
| ☐ | ☐ | | ☐ | ☐ | Regelung zum Einsatz weiterer Subunternehmer |
| ☐ | ☐ | | ☐ | ☐ | Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| ☐ | ☐ | | ☐ | ☐ | Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 8. Verfügbarkeitskontrolle

**Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.**

**Prüffokus:**
**Welche Regelungen bestehen, um die Daten dauerhaft verfügbar bereitzustellen?**

• Brandschutz:
Welche Einrichtungen zum Brandschutz sind vorhanden (z. B. Feuerlöscher, Rauch- oder Brandmelder)? Besteht Rauchverbot? Existieren effektive Wasserschutzeinrichtungen?

• Stromversorgung:
Ist eine unterbrechungsfreie Stromversorgung (USV) etabliert?

• Sicherungen:
Werden Sicherungsdatenträger getrennt aufbewahrt? Wo erfolgen die Backup-Verfahren? Werden Speichereinheiten redundant ausgelegt? Sind die Datensicherungen verschlüsselt? Werden Cloud-Lösungen zur Datensicherung eingesetzt?

• Virenschutz/Firewall:
Bestehen ausreichende Schutzmaßnahmen durch Security-Werkzeuge?

• Notfallplan:
Gibt es auch für einen Katastrophenfall entsprechende Vorkehrungen (z. B. durch Angriffe von intern/extern, Schäden durch Feuer)?

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | Feuer- und Rauchmeldeanlagen | ☐ | ☐ | Backup & Recovery-Konzept (ausformuliert) |
| ☐ | ☐ | Feuerlöscher Serverraum | ☐ | ☐ | Kontrolle des Sicherungsvorgangs |
| ☐ | ☐ | Serverraumüberwachung Temperatur und Feuchtigkeit | ☐ | ☐ | Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse |
| ☐ | ☐ | Serverraum klimatisiert | ☐ | ☐ | Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums (idealerweise in einem anderen Gebäude) |
| ☐ | ☐ | Unterbrechungsfreie Stromversorgung (USV) | ☐ | ☐ | Keine sanitären Anschlüsse im oder oberhalb des Serverraums |
| ☐ | ☐ | Schutzsteckdosenleisten Serverraum | ☐ | ☐ | Existenz eines Notfallplans |
| ☐ | ☐ | Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.) | ☐ | ☐ | Getrennte Partitionen für Betriebssysteme und Daten |
| ☐ | ☐ | RAID System / Festplattenspiegelung | ☐ | ☐ | |
| ☐ | ☐ | Videoüberwachung Serverraum | ☐ | ☐ | |
| ☐ | ☐ | Alarmmeldung bei unberechtigtem Zutritt zu Serverraum | ☐ | ☐ | |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 9. Trennungskontrolle

**Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.**

**Prüffokus:**
**Wie wird gewährleistet, dass Daten getrennt voneinander verarbeitet werden können?**

• Getrennte Speicherung:
Welche Regelungen/Maßnahmen zur Sicherstellung der getrennten Speicherung existieren? Wie erfolgt die Veränderung, Löschung und Übermittlung von Daten mit unterschiedlichen Vertragszwecken (z. B. getrennte DV-Systeme für unterschiedliche Verarbeitungszwecke)? Wie werden Daten mit hohem Schutzbedarf verarbeitet?

• Mandantenfähigkeit:
Werden Systeme verwendet, die eine interne Mandantenaufteilung ermöglichen (Zweckbindung)? Besteht ein Konzept zur Mandantentrennung?

• Funktionstrennung:
Werden Produktion- und Testumgebungen stets voneinander getrennt? Werden personenbezogene Daten zu Entwicklungszwecken pseudonymisiert/anonymisiert?

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | Trennung von Produktiv- und Testumgebung | ☐ | ☐ | Steuerung über Berechtigungskonzept |
| ☐ | ☐ | Physikalische Trennung (Systeme / Datenbanken / Datenträger) | ☐ | ☐ | Festlegung von Datenbankrechten |
| ☐ | ☐ | Mandantenfähigkeit relevanter Anwendungen | ☐ | ☐ | Datensätze sind mit Zweckattributen versehen |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

## 10.Organisationskontrolle

**Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation den besonderen Anforderungen des Datenschutzes gerecht wird.**

**Prüffokus:**
**Welche innerbetrieblichen Reglungen bestehen, um ein entsprechendes Datensicherheitsniveau zu gewährleisten?**

• IT-Sicherheitskonzept:
Bestehen schriftliche Regelungen über den Betrieb und die Abläufe der Datenverarbeitung sowie zu den verschiedenen Datensicherheitsmaßnahmen (z. B. Richtlinien, Arbeitsanweisungen, Stellenbeschreibungen)? Erfolgen Sicherungen des Datenbestandes nach festgelegtem Schema?

• Standards:
Wird auf etablierte Standards für die IT-Sicherheit bzw. zur Abwicklung von IT-Projekten zurückgegriffen (IT-Grundschutz, ISO 27001, etc.)?

• Revision:
Findet eine Revision der Datenverarbeitung statt? Besteht eine interne Revisionsabteilung? Werden Protokollierungen und Log-Dateien ausgewertet (z. B. stichprobenartig)? Werden im Falle der Mitbenutzung der Anlagen durch Fremdfirmen auch hier entsprechende Überprüfungen durchgeführt? Finden auch gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmaßnahmen statt?

• Mitarbeiter:
Ist im Urlaub- und Krankheitsfall für eine Vertretung gesorgt (z. B. Vertreterregelungen, Freigaben, Berechtigungen)? Werden die Mitarbeiter über den sicheren Umgang mit den Daten entsprechend geschult? Gibt es regelmäßige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern? Werden mobile Datenträger der Mitarbeiter standardmäßig verschlüsselt? Besteht eine ausreichende Funktionstrennung? Findet bei wichtigen Datenverarbeitungen das „4-Augen-Prizip“ Anwendung?

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

**Checkliste:**

| Ja | Nein | Technische Maßnahmen | Ja | Nein | Organisatorische Maßnahmen |
|---|---|---|---|---|---|
| ☐ | ☐ | Software-Lösungen für Datenschutz-Management im Einsatz | ☐ | ☐ | Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten |
| ☐ | ☐ | Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …) | ☐ | ☐ | Mitarbeiter geschult und auf Vertraulichkeit /Datengeheimnis verpflichtet |
| ☐ | ☐ | Sicherheitszertifizierung z.B. nach ISO 27001, ISIS12 | ☐ | ☐ | Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich |
| ☐ | ☐ | Anderweitiges dokumentiertes Sicherheitskonzept | ☐ | ☐ | Interner / externer Informationssicherheits-Beauftragter Name / Firma Kontakt |
| ☐ | ☐ | Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt | ☐ | ☐ | Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt |
| ☐ | ☐ | | ☐ | ☐ | Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach |
| ☐ | ☐ | | ☐ | ☐ | Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

### 10.1. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

**Checkliste:**

| Ja | Nein | Technische Maßnahmen | Ja | Nein | Organisatorische Maßnahmen |
|---|---|---|---|---|---|
| ☐ | ☐ | Einsatz von Firewall und regelmäßige Aktualisierung | ☐ | ☐ | Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) |
| ☐ | ☐ | Einsatz von Spamfilter und regelmäßige Aktualisierung | ☐ | ☐ | Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen |
| ☐ | ☐ | Einsatz von Virenscanner und regelmäßige Aktualisierung | ☐ | ☐ | Einbindung von Behörden in Sicherheitsvorfälle und Datenpannen |
| ☐ | ☐ | Intrusion Detection System (IDS) | ☐ | ☐ | Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem |
| ☐ | ☐ | Intrusion Prevention System (IPS) | ☐ | ☐ | Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

### 10.2. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind | ☐ | ☐ | |
| ☐ | ☐ | Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen | ☐ | ☐ | |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

### 10.3. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen (mögl. verschlüsselt) | ☐ | ☐ | Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |

www.teamware.eu
info@teamware.eu
Skype: teamware_eu
Tel. +39 331 9593664

### 10.4. Daten in der Cloud

Bei Speichern der Daten in der Cloud gilt im Besonderen darauf zu achten, wem die Daten gehören, welche Rechte Dritten abgetreten werden und im Speziellen welche Rechte sich der Betreiber des Rechenzentrums sichert.
Sind alle Daten in der EU gespeichert, und unterliegen diese der DSGVO?
Was passiert, wenn Sie den Cloudservice wechseln müssen? Ist eine längerfristige Nutzung der Services gesichert, oder können die Services kurzfristig nicht mehr zur Verfügung stehen?

**Checkliste:**

| Ja | Nein | **Technische Maßnahmen** | Ja | Nein | **Organisatorische Maßnahmen** |
|---|---|---|---|---|---|
| ☐ | ☐ | | ☐ | ☐ | Hauptsitz des Anbieters in der EU (noch besser: Es besteht keine Tochtergesellschaft / Niederlassung im EU-Ausland) |
| ☐ | ☐ | | ☐ | ☐ | Konzept zur Zugriffs- und Berechtigungssteuerung liegt vor |
| ☐ | ☐ | | ☐ | ☐ | Daten werden auf Servern in der EU gespeichert |
| ☐ | ☐ | | ☐ | ☐ | Wurden die notwendigen Verträge zur Datensicherung abgeschlossen? Anbieter bietet bei Bedarf den Abschluss des Vertrages zur Auftragsdatenverarbeitung an? |
| ☐ | ☐ | | ☐ | ☐ | Die Daten werden in Zertifizierten Rechenzentren gespeichert |
| ☐ | ☐ | | ☐ | ☐ | |

**Weitere Maßnahmen bitte hier beschreiben:**

| |
|---|
| |