Checkliste zur Umsetzung der DSGVO

Erstellt von ERP XT

Inhalt

DSGVO-Checkliste (Kurzversion)

Hier ist die Kurzversion unserer DSGVO-Checkliste. Du kannst einfach abhaken, was für dich zutrifft und Kommentare hinzufügen. **Die ausführliche Version mit Praxis- und Umsetzungsbeispielen findest du weiter hinten.**

Allgemeine Rahmenbedingungen

☐ Grundsätzlich werden alle Bemühungen, die Datenschutzgesetze einzuhalten, dokumentiert.

Kommentare

☐ Im Unternehmen besteht ein allgemeines Bewusstsein, dass Datenschutz ein wichtiges Thema und “Chefsache” ist.

Kommentare

☐ Alle Mitarbeiter, Geschäftsführer, Inhaber und sonstige Dritte, die mit personenbezogenen Daten betraut sind, wurden hinsichtlich des Datenschutzes geschult.

Kommentare

☐ Alle Ressourcen in Form von Personal, Weiterbildungen und / oder Softwareanschaffungen bzgl. Datenschutz wurden freigegeben.

Kommentare

☐ Es wird regelmäßig (1x pro Jahr) überprüft, ob der Datenschutz im Unternehmen eingehalten wird.

Kommentare

☐ Datensätze, bei denen keine Aufbewahrungspflicht mehr besteht oder deren Zweck erfüllt ist, werden regelmäßig gelöscht.

Kommentare

☐ Prozesse / Software / Datensammlungen wurden auf “Privacy by Design” (Datenschutz durch Technikgestaltung) hin überprüft.

Kommentare

☐ Prozesse / Software / Datensammlungen wurden auf “Privacy by Default” (Datenschutz durch datenschutzfreundliche Voreinstellungen) hin überprüft.

Kommentare

☐ Prozesse / Software / Datensammlungen wurden auf die DSGVO Grundprinzipien hin überprüft.

Kommentare

☐ Wesentliche datenschutzrechtlich relevante Prozesse wurden definiert.

Kommentare

Der Umgang mit Kundendaten

☐ Eventuell eingeholte Einwilligungen von Kunden und / oder Interessenten wurden korrekt erteilt.

Kommentare

☐ Anfragen von Kunden (bzw. Betroffenen im Allgemeinen) bzgl. Auskunft, Berichtigung, Einschränkung, Löschung, Widerspruch, Übertragung, Sperrung kann nachgekommen werden.

Kommentare

☐ Kunden und / oder Interessenten werden regelmäßig und automatisiert über die Grundsätze der Datenverarbeitung aufgeklärt (Einhaltung von Informationspflichten). Es gibt klare Prozesse, wann und wo über die Datenverarbeitung informiert wird.

Kommentare

Dienstleister und andere Dritte

☐ Alle Auftragsverarbeiter sind an rechtsgültige Verträge (Auftragsverarbeitungsverträge) gebunden.

Kommentare

☐ Im Falle von Datenübermittlungen in Drittländer i. S. d. Kommission wurde die Gewährleistung eines angemessen hohen Schutzniveaus der verarbeiteten Daten (Gewährleistung durch den Auftragsverarbeiter) geprüft. Es bestehen ggf. Ausnahmen von dieser Pflicht.

Kommentare

☐ Dienstleister oder sonstige externe Mitarbeiter sind auf das Datengeheimnis verpflichtet worden.

Kommentare

Webseiten und Apps

☐ Die Datenschutzerklärung(en) wurde(n) geprüft.

Kommentare

☐ Die Website ist technisch DSGVO-konform.

Kommentare

Einhaltung der Dokumentationspflichten nach DSGVO

☐ Ein Verzeichnis von Verarbeitungstätigkeiten wurde erstellt.

Kommentare

☐ Eine Risikoanalyse zu jeder Verarbeitungstätigkeit wurde durchgeführt.

Kommentare

☐ Jede Verarbeitungstätigkeit wurde auf die Notwendigkeit einer Datenschutzfolgenabschätzung (DSFA) hin überprüft.

Kommentare

☐ Eine DSFA muss durchgeführt werden.

Kommentare

☐ Technische und organisatorische Maßnahmen (TOM) wurden dokumentiert.

Kommentare

☐ Es gibt ein Löschkonzept und Löschungen werden protokolliert.

Kommentare

☐ Es wurde geprüft, ob ein Datenschutzbeauftragter bestellt werden muss. Falls die Notwendigkeit der Bestellung besteht, wurde der Datenschutzbeauftragte gemeldet.

Kommentare

☐ Ein Datenschutzkonzept wurde ausgearbeitet und alle getroffenen Maßnahmen und Prozesse dokumentiert (Nachweisbarkeit).

Kommentare

Grundsätzliche technische Checks

☐ Es gibt Back-ups und diese wurden bereits getestet.

Kommentare

☐ Die Software ist auf dem aktuellsten Stand.

Kommentare

☐ Geeignete Maßnahmen, um die IT Infrastruktur zu schützen, wurden ergriffen.

Kommentare

☐ Es gibt ein Berechtigungskonzept.

Kommentare

DSGVO-Checkliste (Langversion mit Erläuterungen)

Hier ist unsere ausführliche DSGVO-Checkliste mit Erläuterungen und Praxisbeispielen. Damit kannst du die Umsetzung direkt angehen. Um dir die Umsetzung zu erleichtern, gibt es eine Klassifikation zu jedem Punkt:

Klassifizierung	Legende
Dringlichkeit	1 - Sofort erledigen / einführen. 2 - Zeitnah erledigen / einführen. 3 - Bei Bedarf erledigen / einführen.
Wichtigkeit	1 - Sehr wichtig, Bußgeld wahrscheinlich 2 - Wichtig 3 - Unklare Rechtslage / Nicht explizit gefordert
Aufwandsschätzung	1 - Sehr aufwändig, viel Zeit / Ressourcen einplanen 2 - Mittlere Aufwandsschätzung 3 - Wenig Aufwand

Beispiel: Dringlichkeit 3, Wichtigkeit 2, Aufwandsschätzung 1

⟶ Dieser Punkt ist nicht zwingend sofort zu erledigen. Er ist wichtig, aber sehr aufwändig. Überlege dir hier, wie groß dein Risiko und deine Umsetzungsressourcen sind.

Allgemeine Rahmenbedingungen

☐ Grundsätzlich werden alle Bemühungen, die Datenschutzgesetze einzuhalten, dokumentiert.

Praxisbeispiel: Der/die VersandhändlerIn C hat in 2020 einen Datenschutzberater engagiert und alle seine/ihre rechtlich relevanten Texte auf seiner/ihrer Webseite neu erstellen lassen. Er/Sie hat jede Änderung in einem Dokument aufgeschrieben. Dieses Dokument kann er/sie im Falle einer Behördenanfrage gut als Nachweis nutzen, dass er/sie den Datenschutz ernst genommen hat.

Klassifikation:
Dringlichkeit 2 Wichtigkeit 3 Aufwandsschätzung 1

Umsetzungsbeispiele:

- Fortlaufendes Dokument oder Ordner führen, in dem alle datenschutzrelevanten Verbesserungen enthalten sind.
- Eine/n DatenschutzberaterIn oder Anwalt/Anwältin engagieren und einen Abschlussbericht anfordern.
- Jährliche Rechenschaftsberichte des DSB einfordern und archivieren.

Kommentare

☐ Im Unternehmen besteht ein allgemeines Bewusstsein, dass Datenschutz ein wichtiges Thema und “Chefsache” ist.

Praxisbeispiel: Die Geschäftsführung der E GmbH schult alle Ihre Mitarbeiter zum Thema Datenschutz mithilfe einer E-Learning-Lösung. Die Einladung zum Workshop kommt direkt von der Geschäftsführung. In der E-Mail geht die Geschäftsführung darauf ein, welchen großen Stellenwert Datenschutz um Unternehmen hat.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 2 Aufwandsschätzung 3

Umsetzungsbeispiele:

- Wurde ein Gesellschafterbeschluss zum Datenschutz gefasst?
- Gab es eine unternehmensweite Datenschutzschulung, die von der Geschäftsführung initiiert wurde?

- Gab es bereits externe Audits zum Thema Datenschutz, bei denen die Geschäftsführung federführend war?

Kommentare

☐ Alle Mitarbeiter, Geschäftsführer, Inhaber und sonstige Dritte, die mit personenbezogenen Daten betraut sind, wurden hinsichtlich des Datenschutzes geschult.

Praxisbeispiel: Die A GmbH hat nur wenige Mitarbeiter. Diese werden in einem Meeting zum Thema Datenschutz geschult. Anschließend werden die Schulungsprotokolle von allen Teilnehmern unterschrieben und im Datenschutz Ordner abgeheftet.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 2 Aufwandsschätzung 1

Umsetzungsbeispiele:
- Schulung via E-Learning (Selbststudium).
- Präsenzschulung.
- Rundmail zur Sensibilisierung.
- Anfertigung von Schulungsprotokollen mit Unterschrift der Beteiligten.
- Vertragliche Verpflichtung auf den Datenschutz und das Datengeheimnis.
- E-Mail mit einer Präsentation zum Thema Datenschutz im Anhang.

Kommentare

☐ Alle Ressourcen in Form von Personal, Weiterbildungen und / oder Softwareanschaffungen bzgl. Datenschutz wurden freigegeben.

Praxisbeispiel: Ein/e EinzelunternehmerIn kauft sich einen Generator für sein/ihre Datenschutzerklärung und bringt sein/ihre Datenschutzerklärung auf den neuesten Stand. Außerdem hat er/sie ihre US-amerikanische E-Mail-Marketing Lösung hin zu einem deutschen Anbieter gewechselt.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 2 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Anschaffung von DSGVO-Software z. B. zur Erstellung von Dokumentationen.
- Abonnement von Fachliteratur.
- Abstellung von Mitarbeitern für das Thema Datenschutz.
- Wechsel von Softwaresystemen hin zu datenschutzfreundlichen Alternativen.

Kommentare

☐ Es wird regelmäßig (1x pro Jahr) überprüft, ob der Datenschutz im Unternehmen eingehalten wird.

Praxisbeispiel: Die Bravo AG lässt einmal im Jahr einen Datenschutzaudit von einem/einer externen BeraterIn durchführen und veröffentlicht diesen auf seiner Webseite.

Klassifikation:
Dringlichkeit 2 Wichtigkeit 2 Aufwandsschätzung 1

Umsetzungsbeispiele:

- Jährliche Neuerstellung aller Dokumentationen zur DSGVO.
- Jährliche Rechenschaftsberichte des DSB.
- Regelmäßige Datenschutzaudits.
- IST Analyse zum Datenschutz inkl. kontinuierlichem Verbesserungsprozess.

Kommentare

☐ Datensätze, bei denen keine Aufbewahrungspflicht mehr besteht oder deren Zweck erfüllt ist, werden regelmäßig gelöscht?

Praxisbeispiel: Im Dokumentenmanagementsystem der S GmbH werden alle Dokumente, die keine besondere Kennzeichnung haben, nach spätestens 11 Jahren gelöscht.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 3 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Automatische Löschung von Datensätzen, die nicht mehr benötigt werden oder deren gesetzliche Aufbewahrungsfrist abgelaufen ist.
- Manuelle jährliche Kontrolle aller Datensätze, ob sie gelöscht werden können.

Kommentare

☐ Prozesse / Software / Datensammlungen wurden auf "Privacy by Design" (Datenschutz durch Technikgestaltung) hin überprüft.

Praxisbeispiel: Abonnenten eines Unternehmensnewsletters können sich mit einem Klick aus dem Newsletter austragen und Ihre Einwilligung widerrufen.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 3 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Datensätze werden automatisiert gelöscht oder anonymisiert.
- Datensätze werden bei Unregelmäßigkeiten automatisch gesperrt.
- Betroffene können Datenschutzeinstellungen leicht und automatisiert vornehmen.

Kommentare

☐ Prozesse / Software / Datensammlungen wurden auf “Privacy by Default” (Datenschutz durch datenschutzfreundliche Voreinstellungen) hin überprüft.

Praxisbeispiel: Auf einem Kontaktformular werden nur die E-Mail-Adresse und ein Freitext erfasst, alle anderen Angaben sind freiwillig.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 3 Aufwandsschätzung 2

Umsetzungsbeispiele:
- Schon bei der Erfassung von Daten wird nur so viel erhoben, wie unbedingt nötig.
- Auch nicht technikaffine Nutzer können Ihre Daten steuern.

Kommentare

☐ Prozesse / Software / Datensammlungen wurden auf die DSGVO Grundprinzipien hin überprüft.

Praxisbeispiel: Die L GmbH wechselt Ihren Hosting-Anbieter, um die Daten Ihrer Kunden ausfallsicher zur Verfügung zu stellen.

Klassifikation:
Dringlichkeit 2 Wichtigkeit 2 Aufwandsschätzung 1

Umsetzungsbeispiele:
- Vereinbarkeit des Zweckes mit der DSGVO.
- Anzuwendende Rechtsgrundlagen.
- Transparenz.
- Verarbeitung nach Treu und Glauben.
- Datenminimierung.
- Datenrichtigkeit.
- Datenintegrität, -vertraulichkeit und -verfügbarkeit.

Kommentare

☐ Wesentliche datenschutzrechtlich relevante Prozesse wurden definiert.

Praxisbeispiel: Die H GmbH hat alle Service-Mitarbeiter darüber informiert, dass alle Anfragen bzgl. DSGVO von Betroffenen oder Behörden direkt an die Vorgesetzten weitergeleitet werden sollen.

Klassifikation:
Dringlichkeit 1 Wichtigkeit 1 Aufwandsschätzung 2

Umsetzungsbeispiele:
- Prozess "Sicherstellung der Betroffenenrechte" wurde definiert.
- Prozess "Behörde fragt an" wurde definiert.
- Prozess "Verletzungen des Schutzes personenbezogener Daten" wurde definiert.
- Prozess "Löschung von personenbezogenen Daten" wurde definiert.
- Prozess "Evaluierung neuer Soft- und Hardware bzgl. Datenschutz" wurde definiert.
- Prozess "Kontinuierlicher Verbesserungsprozess Datenschutz" wurde definiert.

Kommentare

Der Umgang mit Kundendaten

☐ Eventuell eingeholte Einwilligungen von Kunden und / oder Interessenten wurden korrekt erteilt.

Praxisbeispiel: Die V GmbH hat eine Tabelle, in der sie alle Einwilligungen von Kunden sammelt und genau nachvollziehen kann, wann diese erteilt oder widerrufen wurden und welcher Text verwendet wurde.

Klassifikation:
Dringlichkeit 1 Wichtigkeit 1 Aufwandsschätzung 1

Umsetzungsbeispiele:
- Führen einer Einwilligungsdatenbank.
- Prüfen (lassen) aller Einwilligungstexte auf rechtliche Richtigkeit.
- Einwilligungen möglichst sparsam verwenden und auf andere Rechtsgrundlagen abstellen.

Kommentare

☐ Anfragen von Kunden (bzw. Betroffenen im Allgemeinen) bzgl. Auskunft, Berichtigung, Einschränkung, Löschung, Widerspruch, Übertragung, Sperrung kann nachgekommen werden.

Praxisbeispiel: Der/die BetreiberIn eines Internetforums kann in seiner/ihrer Datenbank jeden Nutzer eindeutig identifizieren und allen Anfragen bzgl. der personenbezogenen Daten nach kommen. Er/Sie hat den Fall einer Löschanfrage bereits durchgespielt und ist sich sicher, jeder Anfrage nach kommen zu können.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 2 Aufwandsschätzung 3

Umsetzungsbeispiele:

- Eindeutige Identifizierung von Kunden und Nutzern.
- Routine etablieren, die vollständiges Löschen von Daten erlaubt.
- Button im persönlichen Bereich des Kunden, der mit einem Klick alle Daten exportiert und zur Verfügung stellt.

Kommentare

☐ Kunden und / oder Interessenten werden regelmäßig und automatisiert über die Grundsätze der Datenverarbeitung aufgeklärt (Einhaltung von Informationspflichten). Es gibt klare Prozesse, wann und wo über die Datenverarbeitung informiert wird.

Praxisbeispiel: Ein/e GroßhändlerIn verlinkt seine/ihre Datenschutzerklärung unter jeder Rechnung zur Information seiner/ihrer Kunden.

Klassifikation:
Dringlichkeit 1 Wichtigkeit 2 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Einfügen / Verlinken von Datenschutzhinweisen auf Rechnungen, Angeboten, E-Mail-Signaturen und / oder sonstigen Unterlagen.
- Aushängen / Auslegen einer Datenschutzinformation im Kundenbereich.
- Unterschreiben lassen einer Kundeninformation beim Erstkontakt (keine Einwilligung!).

Kommentare

Dienstleister und andere Dritte

☐ Alle Auftragsverarbeiter sind an rechtsgültige Verträge (Auftragsverarbeitungsverträge) gebunden.

Praxisbeispiel: Ein/e BloggerIn schließt einen AV-Vertrag mit seinem/ihrem Hoster und seinem/ihrem Newsletter-Anbieter ab.

Klassifikation:
Dringlichkeit 1 Wichtigkeit 1 Aufwandsschätzung 3

Umsetzungsbeispiele:

- Abschluss eines AV-Vertrages.
- Tabellarische Erfassung aller Auftragsdatenverarbeiter.

Kommentare

☐ Im Falle von Datenübermittlungen in Drittländer i. S. d. Kommission wurde die Gewährleistung eines angemessen hohen Schutzniveaus der verarbeiteten Daten (Gewährleistung durch den Auftragsverarbeiter) geprüft. Es bestehen ggf. Ausnahmen von dieser Pflicht.

Praxisbeispiel: Der/die WebseitenbetreiberIn P schließt einen Zusatz zur Datenverarbeitung mit Google ab, weil er/sie Google Analytics verwendet und der Anbieter in den USA sitzt. Darüber hinaus nutzt der Betreiber "AnonymizeIP" zur Datensparsamkeit.

Klassifikation:
Dringlichkeit 1 Wichtigkeit 1 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Anbieter mit Privacy Shield Zertifizierung bevorzugen.
- DPAs oder Zusatz zur Datenverarbeitung abschließen.
- Deutsche Anbieter wählen oder Verarbeitungen in House durchführen.

Kommentare

☐ Dienstleister oder sonstige externe Mitarbeiter sind auf das Datengeheimnis verpflichtet worden.

Praxisbeispiel: Die F GmbH verpflichtet jeden Dienstleister bei Abschluss des Dienstleistungsvertrages direkt auf den Datenschutz und das Datengeheimnis.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 3 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Verpflichtungen auf den Datenschutz und das Datengeheimnis abschließen.

Kommentare

Webseiten und Apps

☐ Die Datenschutzerklärung(en) wurde(n) geprüft.

Praxisbeispiel: Der/die Webshop-BetreiberIn R aktualisiert jedes Jahr seine/ihre Datenschutzerklärung auf allen seinen/ihren Seiten und prüft die Verfügbarkeit.

Klassifikation:
Dringlichkeit 1 Wichtigkeit 1 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Ist die Datenschutzerklärung der Website aktuell?
- Ist die Datenschutzerklärung der Social Media Seiten aktuell?
- Ist die Datenschutzerklärung von jeder Seite aus mit einem Klick erreichbar?

Kommentare

☐ Die Website ist technisch DSGVO-konform.

Praxisbeispiel: Der/die Webshop-BetreiberIn K gibt seinem/ihrem Programmierer die Aufgabe, die gesamte Shopumgebung auf alte Pixel und nicht verwendeten Code zu untersuchen.

Klassifikation:
Dringlichkeit 1 Wichtigkeit 1 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Wurde das Kontaktformular SSL verschlüsselt?
- Wurde die Webseite auf nicht verwendeten oder benötigten Trackingcode überprüft?
- Wurden Opt-Out Möglichkeiten für Tracking aktiviert?
- Wurde ein Cookie-Banner installiert?

Kommentare

Einhaltung der Dokumentationspflichten nach DSGVO

Hier werden weder Praxisbeispiele noch Umsetzungsbeispiele genannt. Dies würde den Umfang der Liste übersteigen. Die Klassifikation ist immer die gleiche:

Dringlichkeit 1 Wichtigkeit 1 Aufwandsschätzung 2

☐ Ein Verzeichnis von Verarbeitungstätigkeiten wurde erstellt.

Kommentare

☐ Eine Risikoanalyse zu jeder Verarbeitungstätigkeit wurde durchgeführt.

Kommentare

☐ Jede Verarbeitungstätigkeit wurde auf die Notwendigkeit einer Datenschutzfolgenabschätzung (DSFA) hin überprüft.

Kommentare

☐ Eine DSFA muss durchgeführt werden.

Kommentare

☐ Technische und organisatorische Maßnahmen (TOM) wurden dokumentiert.

Kommentare

☐ Es gibt ein Löschkonzept und Löschungen werden protokolliert.

Kommentare

☐ Es wurde geprüft, ob ein Datenschutzbeauftragter bestellt werden muss. Falls die Notwendigkeit der Bestellung besteht, wurde der Datenschutzbeauftragte gemeldet.

Kommentare

☐ Ein Datenschutzkonzept wurde ausgearbeitet und alle getroffenen Maßnahmen, Prozesse und Dokumentationen dokumentiert (Nachweisbarkeit).

Kommentare

Grundsätzliche technische Checks

☐ Es gibt Back-ups und diese wurden bereits getestet.

Praxisbeispiel: Die N GmbH prüft jährlich, ob sich die Back-ups auch in das Livesystem überspielen lassen und protokolliert die Ergebnisse.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 1 Aufwandsschätzung 2

Umsetzungsbeispiele:
- Incident Response Management.
- Back-up-Tests.
- Multiredundante Back-ups.

Kommentare

☐ Die Software ist auf dem aktuellsten Stand.

Praxisbeispiel: Ein/e EinzelunternehmerIn aktualisiert mindestens einmal im Monat die Software auf seinem/ihrem Laptop.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 3 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Einschalten von automatischen Updates.
- Regelmäßige Kontrolle von Updates.
- Update Richtlinie im Unternehmen.

Kommentare

☐ Geeignete Maßnahmen, um die IT Infrastruktur zu schützen, wurden ergriffen.

Praxisbeispiel: Die G AG blockiert alle Internetverbindungen von außen mit einer Firewall. Der/die IT-AdministratorIn muss einzelne Verbindungen und Ports freigeben.

Klassifikation:
Dringlichkeit 3 Wichtigkeit 3 Aufwandsschätzung 2

Umsetzungsbeispiele:

- Virenschutz.
- Firewalls.
- Verschlüsselung von Datenträgern.

Kommentare

☐ Es gibt ein Berechtigungskonzept.

Praxisbeispiel: Ein/e WebseitenbetreiberIn unterscheidet zwischen Administrator, Benutzern und Redakteuren, welche lediglich Texte für ihn/sie einpflegen können und keinen Zugriff auf personenbezogene Daten haben. Der Datenzugriff ist auf das erforderliche Maß reduziert.

Klassifikation:
Dringlichkeit 2 Wichtigkeit 3 Aufwandsschätzung 1

Umsetzungsbeispiele:

- Zugriff auf personenbezogene Daten nur für einen kleinen Kreis von Benutzern.
- Abschirmen von kritischer Infrastruktur durch Berechtigungen.

Kommentare

TOM-Checkliste

☐ Eine Dokumentation zu allen umgesetzten TOM existiert.

Praxisbeispiel: Eine Excel Tabelle, in der alle Bestandteile der TOM in einer Liste dargestellt sind.

Kommentare

☐ Ein Löschkonzept, das für alle personenbezogenen Daten umgesetzt wird, existiert.

Praxisbeispiel: Eine Excel Tabelle, in der alle verarbeiteten Datenkategorien verzeichnet sind inkl. Löschfristen. Erstellung von Löschprotokollen oder sonstigen Nachweisen.

Kommentare

☐ Alle Maßnahmen zur Umsetzung der Zutrittskontrolle wurden dokumentiert und durchgeführt.

Praxisbeispiel: Alarmanlagen, Schließsysteme.

Kommentare

☐ Alle Maßnahmen zur Umsetzung der Zugangskontrolle wurden dokumentiert und durchgeführt.

Praxisbeispiel: Installation einer Firewall, Verschlüsselung von Datenträgern.

Kommentare

☐ Alle Maßnahmen zur Umsetzung der Zugriffskontrolle wurden dokumentiert und durchgeführt.

Praxisbeispiel: Passwortrichtlinien, Löschanweisungen.

Kommentare

☐ Alle Maßnahmen zur Umsetzung der Weitergabekontrolle wurden dokumentiert und durchgeführt.

Praxisbeispiel: E-Mail Verschlüsselung, Einsatz von VPN Technologie.

Kommentare

☐ Alle Maßnahmen zur Umsetzung der Eingabekontrolle wurden dokumentiert und durchgeführt.

Praxisbeispiel: Eingabeprotokollierung, Nutzerrollen.

Kommentare

☐ Alle Maßnahmen zur Umsetzung der Verfügbarkeitskontrolle wurden dokumentiert und durchgeführt.

Praxisbeispiel: Feuer- und Rauchmelder, automatische Löschanlagen.

Kommentare

☐ Alle Maßnahmen zur Umsetzung des Trennungsgebots wurden dokumentiert und durchgeführt.

Praxisbeispiel: Physische Trennung von Datenträgern, Speicherung von personenbezogenen Daten je nach Zweck in unterschiedlichen Datenbanken.

Kommentare

☐ Alle Auftragsverarbeiter wurden hinsichtlich der Einhaltung der Datenschutzgrundsätze geprüft.

Praxisbeispiel: Vorabkontrolle beim Auftragsverarbeiter, Prüfung der TOM des Auftragsverarbeiters.

Kommentare

☐ Es existieren Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall.

Praxisbeispiel: Back-ups, Incident Response Management.

Kommentare

☐ Es gibt Vertretungsregelungen für die IT-Verantwortlichen.

Praxisbeispiel: Wenn der/die IT-LeiterIn krank ist, kann der/die stellvertretende IT-LeiterIn seine/ihre Aufgaben übernehmen.

Kommentare

☐ Die Verantwortlichen für die IT-Sicherheit sind angemessen ausgebildet und in alle Unternehmensstrukturen eingebunden, die mit personenbezogenen Daten zu tun haben.

Praxisbeispiel: Der IT-Sicherheitsbeauftragte des Unternehmens wird bei jeder Tool-Neuanschaffung mit eingebunden.

Kommentare

☐ Es existieren Verfahren zur Gewährleistung der Belastbarkeit der Systeme und Dienste.

Praxisbeispiel: Regelmäßige Tests der Belastbarkeit mittels Stresstests.

Kommentare

☐ Es existiert ein Datensicherheitskonzept bzw. eine Datensicherheitsrichtlinie.

Praxisbeispiel: Ausarbeitung einer Datensicherheitsrichtlinie mit einem/einer BeraterIn.

Kommentare

☐ Alle Mitarbeiter, die mit personenbezogenen Daten zu tun haben, wurden auf das Datengeheimnis verpflichtet und im Umgang mit den Daten geschult.

Praxisbeispiel: Aushändigung einer Schulungsunterlage im Jahresrhythmus, Verpflichtung aller Mitarbeiter auf das Datengeheimnis mit Unterschrift.

Kommentare

☐ Es existieren Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Praxisbeispiel: Die TOM werden jedes Jahr unabhängig geprüft, die Prüfung und die Findings werden dokumentiert.

Kommentare

☐ Die TOM entsprechen dem aktuellen Stand des technischen Fortschritts und sind gemäß festgelegten Schutzzielen und Risikoprofil angemessen.

Kommentare

Die Datenschutzbehörden

Die Datenschutzbehörden sind unabhängige Behörden, die die Anwendung der Datenschutzvorschriften überwachen und Verstöße verfolgen. Sie sind überdies Ansprechpartner für Fragen zur Auslegung des Gesetzes oder zur praktischen Anwendung.

Auf Bundesebene:	**https://www.bfdi.bund.de/**
Baden-Württemberg:	**https://www.baden-wuerttemberg.datenschutz.de/**
Bayern:	**https://www.datenschutz-bayern.de/**
Berlin:	**https://www.datenschutz-berlin.de/**
Brandenburg:	**https://www.lda.brandenburg.de/**
Bremen:	**https://www.datenschutz.bremen.de/**
Hamburg:	**https://datenschutz-hamburg.de/**
Hessen:	**https://datenschutz.hessen.de/**
Mecklenburg-Vorpommern:	**https://www.datenschutz-mv.de/**
Niedersachsen:	**https://www.lfd.niedersachsen.de/**
Nordrhein-Westfalen:	**https://www.ldi.nrw.de/**
Rheinland-Pfalz:	**https://www.datenschutz.rlp.de/de/startseite/**
Saarland:	**https://datenschutz.saarland.de/**
Sachsen:	**https://www.saechsdsb.de/**
Sachsen-Anhalt:	**http://www.datenschutz.sachsen-anhalt.de/**
Schleswig-Holstein:	**https://www.datenschutzzentrum.de/**
Thüringen:	**https://www.tlfdi.de/tlfdi/**