DatenschutzManager

Benutzerhandbuch und Betriebshandbuch

Version: 0.9.4 DE
Stand: 12.06.2026

Autor:
Armin Fimberger

Hersteller und Verfasser sowie inhaltlich Verantwortlicher:
Digitales Erbe Fimberger

Armin Fimberger
Kathreinweg 33
81827 München

Support:
datenschutzmanager@digitaleserbe.net

Webseite:
www.digitaleserbe.net

© 2026 Digitales Erbe Fimberger

Hinweise

Die in diesem Handbuch enthaltenen Abbildungen dienen der Veranschaulichung und können von der tatsächlich installierten Softwareversion abweichen.

Funktionsumfang, Benutzeroberfläche und Inhalte des DatenschutzManagers werden kontinuierlich weiterentwickelt. Einzelne Darstellungen, Funktionen oder Menüeinträge können sich daher ohne vorherige Ankündigung ändern.

Dieses Handbuch beschreibt den Funktionsumfang zum Zeitpunkt der Erstellung. Maßgeblich ist stets die aktuell eingesetzte Version der Software.

Alle Angaben wurden mit größter Sorgfalt erstellt. Für die Vollständigkeit, Aktualität und Richtigkeit der Inhalte wird jedoch keine Gewähr übernommen.

Der DatenschutzManager unterstützt die Umsetzung datenschutzrechtlicher Anforderungen. Die Nutzung der Software ersetzt keine rechtliche Beratung oder die fachliche Bewertung durch einen Datenschutzbeauftragten.

© 2026 Digitales Erbe Fimberger

Alle Rechte vorbehalten. Kein Teil dieses Handbuchs darf ohne vorherige schriftliche Genehmigung des Herstellers vervielfältigt, verbreitet oder veröffentlicht werden.

Haftungsausschluss

Die Software DatenschutzManager wurde mit größter Sorgfalt entwickelt und getestet. Dennoch kann trotz sorgfältiger Entwicklung und Qualitätssicherung nicht ausgeschlossen werden, dass Fehler, Funktionsstörungen oder unerwartete Programmverhalten auftreten.

Der Hersteller übernimmt keine Gewähr dafür, dass die Software jederzeit fehlerfrei, unterbrechungsfrei oder für jeden Einsatzzweck geeignet ist.

Dem Anwender wird ausdrücklich empfohlen, regelmäßig Datensicherungen (Backups) anzufertigen und die Wiederherstellbarkeit der Sicherungen regelmäßig zu überprüfen.

Der Hersteller haftet nicht für Datenverluste, entgangenen Gewinn, Betriebsunterbrechungen oder sonstige mittelbare Schäden, die durch die Nutzung, Nichtnutzung oder Fehlfunktionen der Software entstehen, soweit gesetzlich zulässig.

Die Verantwortung für die ordnungsgemäße Datensicherung, Archivierung und Wiederherstellung der Daten liegt ausschließlich beim Anwender.

Die Nutzung der Software erfolgt auf eigenes Risiko des Anwenders.

Die Software dient der Unterstützung datenschutzrechtlicher und organisatorischer Prozesse. Sie ersetzt weder eine rechtliche Beratung noch die fachliche Bewertung durch einen Datenschutzbeauftragten, Auditor oder Rechtsanwalt.

Funktionsumfang, Benutzeroberfläche und Inhalte können im Rahmen der Weiterentwicklung jederzeit geändert werden.

Die in diesem Handbuch enthaltenen Abbildungen dienen der Veranschaulichung und können von der tatsächlich installierten Softwareversion abweichen.

© 2026 Digitales Erbe Fimberger

Alle Rechte vorbehalten.

Systemvoraussetzungen

Unterstützte Betriebssysteme

Der DatenschutzManager ist für Apple macOS entwickelt.

Unterstützte Version:

- macOS 26 oder höher

Der Betrieb auf älteren Versionen wird nicht unterstützt.

Bildschirmauflösung

Für die Nutzung wird eine Mindestauflösung von:

`1024 × 1000 Pixel`

vorausgesetzt.

Bei geringeren Auflösungen können einzelne Inhalte, Dialoge oder Bedienelemente nur eingeschränkt dargestellt werden.

Für eine komfortable Nutzung empfehlen eine Auflösung von mindestens:

`1920 × 1080 Pixel`

oder höher.

Arbeitsspeicher

Der Speicherbedarf der Anwendung hängt maßgeblich von der Anzahl der verwalteten Datensätze sowie den hinterlegten Dokumenten ab.

Insbesondere folgende Faktoren beeinflussen den Speicherbedarf:

- Anzahl der Mandanten
- Anzahl der Verarbeitungstätigkeiten
- Anzahl der Dokumente
- Umfang der hochgeladenen Nachweise
- Größe der importierten Dateien

Speicherplatz

Der erforderliche Festplattenspeicher ist abhängig von den durch den Benutzer hochgeladenen Dokumenten und Nachweisen.

Die eigentliche Anwendungsdatenbank benötigt in der Regel nur vergleichsweise wenig Speicherplatz (ca. 50 Mbyte).

Der überwiegende Speicherbedarf entsteht durch:

- PDF-Dokumente
- Office-Dokumente
- Auditberichte
- Nachweise
- Schulungsunterlagen
- Datenschutzfolgenabschätzungen
- sonstige hochgeladene Dateien

Es wird empfohlen, ausreichend freien Speicherplatz für zukünftige Dokumentenimporte vorzuhalten. Die Software prüft nicht verfügbaren freien Speicherplatz.

Datensicherung

Für den produktiven Einsatz wird empfohlen, regelmäßig Datensicherungen zu erstellen.

Die Verantwortung für die Datensicherung und Wiederherstellung liegt beim Anwender.

Internetverbindung

Für den Betrieb des DatenschutzManagers ist grundsätzlich keine dauerhafte Internetverbindung erforderlich.

Die Anwendung kann vollständig lokal betrieben werden.

Eine Internetverbindung wird lediglich für optionale Funktionen, Softwareaktualisierungen oder externe Verlinkungen benötigt.

Praxiserprobte KI-Unterstützung (Optional)

Die im DatenschutzManager vorhandenen KI-Schnittstellen wurden nicht ausschließlich für zukünftige Erweiterungen entwickelt, sondern werden bereits produktiv eingesetzt.

Digitales Erbe Fimberger nutzt die firmeninterne vorhandene Architektur seit mehreren Monaten erfolgreich mit einer eigenen KI-Lösung zur Unterstützung datenschutzrechtlicher und organisatorischer Aufgaben. Hauseigenen KI-Lösungen sind äußerst datenschutzfreundlich.

Dabei werden unter anderem unterstützt:

- Analyse umfangreicher Datenschutzdokumentationen
- Zusammenfassungen großer Datenbestände
- Unterstützung bei Audits und Bewertungen
- Auswertung von Maßnahmen und Feststellungen
- Vorbereitung von Managementinformationen
- Recherche innerhalb umfangreicher Datenschutzbestände

Der DatenschutzManager kann vollständig ohne künstliche Intelligenz betrieben werden.

Sämtliche Funktionen des Datenschutzmanagementsystems stehen unabhängig von einer KI-Anbindung zur Verfügung.

Die KI-Funktionalität ist optional!

Die praktische Nutzung zeigt insbesondere bei größeren Datenmengen erhebliche Vorteile hinsichtlich Übersichtlichkeit, Recherchegeschwindigkeit und Wissensmanagement.

Die KI-Unterstützung ersetzt dabei weder die fachliche Bewertung durch einen Datenschutzbeauftragten noch rechtliche Entscheidungen. Sie dient als Werkzeug zur Analyse, Unterstützung und Effizienzsteigerung.

Unternehmen, die eine vergleichbare KI-Umgebung aufbauen möchten, können durch Digitales Erbe Fimberger bei Planung, Installation, Konfiguration und Inbetriebnahme unterstützt werden. Lesen sie weiter bei Kapitel 22

IINHALTSVERZEICHNIS

Kapitel 1 – Erste Schritte

Was ist der DatenschutzManager?

Der DatenschutzManager unterstützt beim Aufbau und Betrieb eines Datenschutzmanagementsystems (DSMS) nach DSGVO sowie eines Privacy Information Management Systems (PIMS) nach ISO 27701.

Die Software besteht aus mehreren Modulen, die miteinander verknüpft sind.

In welcher Reihenfolge sollte ich arbeiten?

Schritt 1: Mandant anlegen

Legen Sie zunächst einen Mandanten an und öffnen Sie diesen.

Schritt 2: Kataloge pflegen

Pflegen Sie zunächst die Stammdaten:

- Betroffenengruppen
- Datenkategorien
- Risikoeinstufungen
- Aufbewahrungsfristen

Diese Informationen werden später in Verarbeitungstätigkeiten verwendet.

Schritt 3: Stammdaten erfassen

Erfassen Sie anschließend:

- Dienstleister
- TOM
- Informationspflichten
- Steuerungsdokumente
- PIMS-Kontrollen

Schritt 4: Verarbeitungstätigkeiten anlegen

Erstellen Sie nun Ihre Verarbeitungstätigkeiten.

Hier werden die zuvor angelegten Stammdaten miteinander verknüpft.

Schritt 5: Erweiterte Dokumentation

Danach können Sie weitere Module verwenden:

- Datenschutzfolgenabschätzungen (DSFA)
- Audits
- Maßnahmen
- Datenschutzvorfälle
- Betroffenenersuchen

Warum sehe ich manchmal keine Auswahlmöglichkeiten?

Viele Auswahllisten beziehen ihre Daten aus den zuvor gepflegten Stammdaten.

Wenn beispielsweise noch keine Dienstleister oder TOM vorhanden sind, können diese auch nicht in einer Verarbeitungstätigkeit ausgewählt werden.

Kapitel 2 – Verarbeitungstätigkeiten

Was ist eine Verarbeitungstätigkeit?

Die Verarbeitungstätigkeit bildet das zentrale Element des DatenschutzManagers.

Sie beschreibt einen datenschutzrelevanten Prozess innerhalb Ihrer Organisation, bei dem personenbezogene Daten verarbeitet werden.

Beispiele:

- Personalverwaltung
- Bewerbermanagement
- Kundenverwaltung
- Newsletterversand
- Videoüberwachung
- Zeiterfassung
- Lieferantenverwaltung

Fast alle anderen Module werden später mit einer Verarbeitungstätigkeit verknüpft.

Neue Verarbeitungstätigkeit anlegen

Öffnen Sie das Modul:

Verarbeitungstätigkeiten

und klicken Sie auf:

Neu

Die neue Verarbeitung wird sofort angelegt und erhält eine interne ID.

Anschließend können die Details ergänzt werden.

Allgemeine Angaben

Erfassen Sie mindestens:

- Bezeichnung
- Zweck der Verarbeitung
- Rechtsgrundlage
- Speicherkonzept
- Risiko
- Status

Diese Angaben bilden die Grundlage für das Verzeichnis der Verarbeitungstätigkeiten.

Betroffenengruppen

Ordnen Sie die Personen zu, deren Daten verarbeitet werden.

Beispiele:

- Beschäftigte
- Bewerber
- Kunden
- Lieferanten
- Besucher
- Interessenten

Die Auswahl erfolgt über die zuvor gepflegten Kataloge.

Datenkategorien

Ordnen Sie die verarbeiteten Datenarten zu.

Beispiele:

- Stammdaten
- Kontaktdaten
- Vertragsdaten
- Gesundheitsdaten
- Finanzdaten
- Kommunikationsdaten

Die Auswahl erfolgt ebenfalls über die Kataloge.

Dienstleister zuordnen

Wenn externe Dienstleister an der Verarbeitung beteiligt sind, können diese direkt zugeordnet werden.

Beispiele:

- Microsoft 365
- DATEV
- Hostinganbieter
- Cloud-Dienstleister

Die Dienstleister müssen zuvor im Modul **Dienstleister** angelegt worden sein.

TOM zuordnen

Technische und organisatorische Maßnahmen können direkt einer Verarbeitung zugeordnet werden.

Beispiele:

- Zugriffskontrolle
- Verschlüsselung
- Datensicherung

- Rollen- und Berechtigungskonzepte

Die Maßnahmen müssen zuvor im Modul **TOM** angelegt worden sein.

Informationspflichten

Vorhandene Informationspflichten können mit einer Verarbeitung verknüpft werden.

Dadurch wird nachvollziehbar, welche Datenschutzhinweise zu welcher Verarbeitung gehören.

Steuerungsdokumente

Steuerungsdokumente dienen als Nachweis.

Beispiele:

- Richtlinien
- Verfahrensanweisungen
- Arbeitsanweisungen
- Konzepte

Empfehlung:

Steuerungsdokumente sollten als zentrale Nachweisquelle genutzt werden. Dokumente sollten nicht mehrfach hochgeladen werden.

PIMS-Kontrollen

Im Rahmen eines Privacy Information Management Systems (PIMS) können PIMS-Kontrollen direkt mit einer Verarbeitung verknüpft werden.

Dadurch wird die Umsetzung der Anforderungen aus ISO 27701 nachvollziehbar dokumentiert.

Datenschutzfolgenabschätzung (DSFA)

Falls für eine Verarbeitung eine Datenschutzfolgenabschätzung erforderlich ist, kann diese direkt zugeordnet werden.

Die Zuordnung erfolgt über die DSFA-Chips im Bereich DSFA-Zuordnung.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘**S**

gespeichert.

Nach erfolgreichem Speichern erscheint eine Bestätigungsmeldung.

Löschen

Verarbeitungstätigkeiten können gelöscht werden.

Vor dem Löschen erscheint eine Sicherheitsabfrage.

Gelöschte Datensätze können nicht automatisch wiederhergestellt werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 3 – Dienstleister und Auftragsverarbeitung

Zweck des Moduls

Im Modul **Dienstleister** werden alle externen Anbieter erfasst, die Leistungen für Ihr Unternehmen erbringen.

Dazu gehören insbesondere:

- Cloud-Anbieter
- Hosting-Anbieter
- Softwarehersteller
- IT-Dienstleister
- Lohnabrechnungsanbieter
- Support-Dienstleister
- externe Berater

Das Modul dient gleichzeitig als zentrale Verwaltung für Auftragsverarbeiter nach Art. 28 DSGVO.

Neuen Dienstleister anlegen

Öffnen Sie das Modul:

Dienstleister

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Stammdaten erfassen

Pflegen Sie mindestens:

- Firmenname
- Ansprechpartner
- Anschrift
- E-Mail-Adresse
- Webseite

Empfehlung:

Erfassen Sie möglichst den rechtlichen Vertragspartner.

Beispiel:

Nicht:

```
Microsoft 365
```

sondern:

```
Microsoft Ireland Operations Limited
```

Risikoeinstufung

Für jeden Dienstleister kann eine Risikoeinstufung vorgenommen werden.

Beispiele:

Niedrig

- einfache Webseiten
- reine Informationsangebote

Mittel

- Standard-Cloud-Dienste
- Kommunikationsplattformen

Hoch

- Verarbeitung besonderer Kategorien personenbezogener Daten
- umfangreiche Datenbestände
- kritische Geschäftsprozesse

Die Risikoeinstufung unterstützt spätere Audits und Bewertungen.

Hinweis: Risiken können unter Einstellungen selbst definiert werden.

Auftragsverarbeitung (AVV)

Sofern der Dienstleister personenbezogene Daten im Auftrag verarbeitet, sollte geprüft werden, ob ein Auftragsverarbeitungsvertrag (AVV) erforderlich ist.

Beispiele:

- Microsoft 365
- Hosting-Anbieter
- Cloud-Speicher
- externe Lohnabrechnung

Der AVV kann im AVV-Modul dokumentiert und dem Dienstleister zugeordnet werden.

Nachweise hinterlegen

Zu jedem Dienstleister können Nachweise dokumentiert werden.

Beispiele:

- AVV
- Zertifikate
- ISO-27001-Nachweise
- Datenschutzerklärungen
- TOM-Dokumente
- Auditberichte

Empfehlung:

Dokumente möglichst zentral über die Steuerungsdokumente verwalten.

Zuordnung zu Verarbeitungstätigkeiten

Nachdem ein Dienstleister angelegt wurde, kann er einer oder mehreren Verarbeitungstätigkeiten zugeordnet werden.

Beispiel:

Dienstleister

Microsoft 365

Zugeordnete Verarbeitungstätigkeiten

- Personalverwaltung
- Bewerbermanagement
- Kundenverwaltung

Dadurch wird nachvollziehbar, welche Dienstleister an welchen Verarbeitungen beteiligt sind.

Drittlandtransfer

Falls Daten außerhalb der EU bzw. des EWR verarbeitet werden, sollte geprüft werden:

- In welchem Land erfolgt die Verarbeitung?
- Welche Garantien bestehen?
- Sind Standardvertragsklauseln vorhanden?
- Liegt ein Angemessenheitsbeschluss vor?

Diese Informationen können im Datenschutzmanagement dokumentiert werden.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘**S**

gespeichert.

Löschen

Vor dem Löschen eines Dienstleisters erscheint eine Sicherheitsabfrage.

Bereits bestehende Verknüpfungen zu Verarbeitungstätigkeiten sollten vor dem Löschen überprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 4 – Technische und organisatorische Maßnahmen (TOM)

Zweck des Moduls

Technische und organisatorische Maßnahmen (TOM) dienen dem Schutz personenbezogener Daten.

Sie beschreiben, welche Sicherheitsmaßnahmen innerhalb der Organisation umgesetzt wurden, um die Anforderungen der DSGVO zu erfüllen.

Das Modul unterstützt insbesondere die Dokumentation gemäß:

- Art. 24 DSGVO
- Art. 25 DSGVO
- Art. 32 DSGVO
- ISO 27001
- ISO 27701

Neue TOM anlegen

Öffnen Sie das Modul:

TOM

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Aufbau einer TOM

Eine TOM besteht typischerweise aus:

- Bezeichnung
- Bereich
- Beschreibung
- Status
- Wirksamkeit
- Risikoeinstufung

Typische TOM-Bereiche

Zutrittskontrolle

Schutz vor unbefugtem Zutritt zu Gebäuden und Räumen.

Beispiele:

- Schließsysteme
- Alarmanlagen
- Besucherkonzepte

Zugangskontrolle

Schutz vor unbefugter Nutzung von IT-Systemen.

Beispiele:

- Kennwortrichtlinien
- Multi-Faktor-Authentifizierung
- Benutzerkonten

Zugriffskontrolle

Schutz vor unberechtigtem Zugriff auf Daten.

Beispiele:

- Rollen- und Berechtigungskonzepte
- Dateiberechtigungen
- Mandantentrennung

Weitergabekontrolle

Schutz bei der Übermittlung von Daten.

Beispiele:

- TLS-Verschlüsselung
- VPN
- sichere Dateiübertragung

Eingabekontrolle

Nachvollziehbarkeit von Änderungen.

Beispiele:

- Protokollierung
- Änderungsnachweise
- Audit-Logs

Verfügbarkeitskontrolle

Sicherstellung der Verfügbarkeit von Daten.

Beispiele:

- Backup
- Notfallkonzept
- Redundanzen

Trennungskontrolle

Trennung unterschiedlicher Datenbestände.

Beispiele:

- Mandantentrennung
- getrennte Datenbanken
- Rollenmodelle

Wirksamkeit bewerten

Für jede TOM sollte eine Wirksamkeitsbewertung vorgenommen werden.

Beispiele:

Hoch

Die Maßnahme ist vollständig umgesetzt und regelmäßig geprüft.

Mittel

Die Maßnahme ist umgesetzt, jedoch noch nicht vollständig überprüft.

Niedrig

Die Maßnahme ist geplant oder nur teilweise umgesetzt.

Nachweise hinterlegen

Zu jeder TOM können Nachweise dokumentiert werden.

Beispiele:

- Richtlinien
- Verfahrensanweisungen
- Screenshots
- Zertifikate
- Auditberichte
- Schulungsnachweise

Empfehlung:

Nachweise möglichst zentral über die Steuerungsdokumente verwalten.

Zuordnung zu Verarbeitungstätigkeiten

Eine TOM kann mehreren Verarbeitungstätigkeiten zugeordnet werden.

Beispiel:

TOM

Multi-Faktor-Authentifizierung

Zugeordnete Verarbeitungstätigkeiten

- Personalverwaltung
- Bewerbermanagement
- Kundenverwaltung

Dadurch wird nachvollziehbar, welche Schutzmaßnahmen für welche Verarbeitung gelten.

Zusammenhang mit Audits

TOM bilden häufig die Grundlage für:

- Datenschutz-Audits
- ISO-27001-Audits
- ISO-27701-Audits
- interne Kontrollen

Deshalb sollten Status und Wirksamkeit regelmäßig überprüft werden.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘**S**

gespeichert.

Löschen

Vor dem Löschen einer TOM erscheint eine Sicherheitsabfrage.

Vorhandene Zuordnungen zu Verarbeitungstätigkeiten sollten vor dem Löschen geprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 5 – Datenschutzfolgenabschätzung (DSFA)

Zweck des Moduls

Die Datenschutzfolgenabschätzung (DSFA) dient der Bewertung von Verarbeitungstätigkeiten mit erhöhtem Risiko für die Rechte und Freiheiten betroffener Personen.

Die Verpflichtung ergibt sich aus:

- Art. 35 DSGVO
- Erwägungsgründe 84, 89 bis 95 DSGVO

Eine DSFA soll Risiken frühzeitig erkennen und geeignete Schutzmaßnahmen dokumentieren.

Wann ist eine DSFA erforderlich?

Eine DSFA kann insbesondere erforderlich sein bei:

- umfangreicher Verarbeitung personenbezogener Daten
- Verarbeitung besonderer Kategorien personenbezogener Daten
- systematischer Überwachung
- Videoüberwachung
- Profiling
- automatisierten Entscheidungen
- innovativen Technologien
- umfangreichen Mitarbeiterüberwachungen

Im Zweifel sollte die Notwendigkeit dokumentiert geprüft werden.

Neue DSFA anlegen

Öffnen Sie das Modul:

DSFA

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Erfassen Sie mindestens:

Titel

- Beschreibung
- Status
- Risiko vor Maßnahmen
- Risiko nach Maßnahmen

Empfehlung:

Der Titel sollte eindeutig zur betroffenen Verarbeitungstätigkeit passen.

Beispiel:

```
DSFA Bewerbermanagement

DSFA Videoüberwachung

DSFA KI-gestützte Bewerberauswertung
```

Risikoanalyse

Dokumentieren Sie:

Risiken

Welche Risiken bestehen für betroffene Personen?

Beispiele:

- Verlust der Vertraulichkeit
- Identitätsdiebstahl
- Diskriminierung
- unberechtigte Offenlegung
- wirtschaftliche Nachteile

Eintrittswahrscheinlichkeit

Wie wahrscheinlich ist das Risiko?

Beispiele:

- Niedrig
- Mittel
- Hoch

Schadensausmaß

Welche Auswirkungen hätte ein Schadensfall?

Beispiele:

- Gering
- Mittel
- Hoch

Maßnahmen dokumentieren

Beschreiben Sie die Maßnahmen zur Risikominimierung.

Beispiele:

- Verschlüsselung
- Pseudonymisierung
- Zugriffskontrollen
- Berechtigungskonzepte
- Schulungen
- Protokollierung

Zuordnung zu Verarbeitungstätigkeiten

Jede DSFA kann einer oder mehreren Verarbeitungstätigkeiten zugeordnet werden.

Die Zuordnung erfolgt im Modul:

Verarbeitungstätigkeiten

über den Bereich:

DSFA-Zuordnung

Dort können vorhandene DSFA direkt ausgewählt und verknüpft werden.

Nachweise hinterlegen

Zur DSFA können Nachweise dokumentiert werden.

Beispiele:

- Risikobewertungen
- Stellungnahmen
- Gutachten
- technische Dokumentationen
- Verfahrensbeschreibungen

Empfehlung:

Nachweise möglichst zentral über die Steuerungsdokumente verwalten.

Zusammenhang mit Maßnahmen

Aus einer DSFA ergeben sich häufig konkrete Maßnahmen.

Beispiele:

- Einführung einer Verschlüsselung
- Anpassung von Berechtigungskonzepten
- zusätzliche Schulungen
- organisatorische Änderungen

Diese können im Modul:

Maßnahmen

dokumentiert und nachverfolgt werden.

Zusammenhang mit Audits

DSFA sollten regelmäßig überprüft werden.

Anlässe für eine Überprüfung:

- neue Technologien
- geänderte Prozesse
- neue Risiken
- neue gesetzliche Anforderungen
- Datenschutzvorfälle

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘**S**

gespeichert.

Löschen

Vor dem Löschen einer DSFA erscheint eine Sicherheitsabfrage.

Vorhandene Zuordnungen zu Verarbeitungstätigkeiten sollten vor dem Löschen geprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 6 – Datenschutzvorfälle

Zweck des Moduls

Das Modul **Datenschutzvorfälle** dient der Dokumentation und Bewertung von Datenschutzverletzungen.

Die Dokumentation unterstützt insbesondere die Anforderungen aus:

- Art. 33 DSGVO (Meldung von Datenschutzverletzungen)
- Art. 34 DSGVO (Benachrichtigung betroffener Personen)

Nicht jeder Vorfall führt automatisch zu einer Meldepflicht. Dennoch sollten Vorfälle dokumentiert und bewertet werden.

Was ist ein Datenschutzvorfall?

Ein Datenschutzvorfall liegt vor, wenn personenbezogene Daten:

- verloren gehen
- verändert werden
- unbefugt offengelegt werden
- unbefugt eingesehen werden
- nicht verfügbar sind

Beispiele für Datenschutzvorfälle

Verlust von Datenträgern

Beispiele:

- verlorener USB-Stick
- verlorenes Notebook
- verlorenes Smartphone

Fehlversand von Informationen

Beispiele:

- E-Mail an falschen Empfänger
- Brief an falschen Empfänger
- versehentliche Freigabe von Dokumenten

Unberechtigter Zugriff

Beispiele:

- Hackerangriff
- kompromittierte Benutzerkonten
- unberechtigte Einsichtnahme durch Mitarbeiter

Technische Störungen

Beispiele:

- Ransomware
- Datenbankfehler
- Backup-Probleme
- Systemausfälle

Neuen Datenschutzvorfall anlegen

Öffnen Sie das Modul:

Datenschutzvorfälle

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Dokumentieren Sie mindestens:

- Datum
- Kategorie
- Beschreibung
- betroffene Daten
- betroffene Personen
- Status

Je genauer die Dokumentation erfolgt, desto einfacher ist die spätere Bewertung.

Risikobewertung

Bewerten Sie:

Eintrittswahrscheinlichkeit

Wie wahrscheinlich sind negative Auswirkungen?

Schwere der Auswirkungen

Welche Folgen können entstehen?

Beispiele:

Identitätsdiebstahl

Diskriminierung

Rufschädigung

finanzielle Schäden

Meldepflicht prüfen

Prüfen Sie, ob eine Meldung an die zuständige Datenschutzaufsichtsbehörde erforderlich ist.

Die DSGVO sieht grundsätzlich eine Frist von:

```
72 Stunden
```

ab Bekanntwerden des Vorfalls vor.

Benachrichtigung betroffener Personen

Zusätzlich kann eine Information der betroffenen Personen erforderlich sein.

Beispiele:

Datenverlust

Identitätsmissbrauch

hohe Risiken für Betroffene

Die Entscheidung sollte dokumentiert werden.

Maßnahmen dokumentieren

Erfassen Sie die eingeleiteten Maßnahmen.

Beispiele:

Passwortänderung

Kontosperrung

Wiederherstellung aus Backup

Schulungen

technische Nachbesserungen

Verknüpfung mit Maßnahmen

Aus Datenschutzvorfällen ergeben sich häufig neue Maßnahmen.

Beispiele:

Einführung von MFA

Verbesserung von Backup-Konzepten

Anpassung von Richtlinien

zusätzliche Sensibilisierung

Diese können im Modul:

Maßnahmen

nachverfolgt werden.

Nachweise hinterlegen

Zu einem Datenschutzvorfall können Nachweise dokumentiert werden.

Beispiele:

Screenshots

Log-Dateien

E-Mail-Verkehr

Untersuchungsberichte

Stellungnahmen

Statusverwaltung

Empfohlene Statuswerte:

Offen

Vorfall wird noch untersucht.

In Bearbeitung

Bewertung und Maßnahmen laufen.

Abgeschlossen

Vorfall wurde vollständig bearbeitet.

Audits und Nachvollziehbarkeit

Datenschutzvorfälle werden häufig im Rahmen von Audits geprüft.

Eine vollständige Dokumentation erleichtert:

interne Audits

externe Audits

Nachweise gegenüber Aufsichtsbehörden

Speichern

Änderungen werden über:

Speichern in der Symbolleiste

- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen eines Datenschutzvorfalls erscheint eine Sicherheitsabfrage.

Aus Gründen der Nachvollziehbarkeit sollte geprüft werden, ob eine Löschung tatsächlich erforderlich ist.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 7 – Betroffenenersuchen

Zweck des Moduls

Das Modul **Betroffenenersuchen** dient der Bearbeitung und Dokumentation von Anfragen betroffener Personen.

Die DSGVO gewährt betroffenen Personen verschiedene Rechte, die von Unternehmen und Organisationen innerhalb gesetzlicher Fristen bearbeitet werden müssen.

Das Modul unterstützt die vollständige Nachvollziehbarkeit dieser Vorgänge.

Rechte betroffener Personen

Typische Betroffenenrechte sind:

Auskunft

Die betroffene Person möchte wissen:

welche Daten gespeichert werden

zu welchem Zweck Daten verarbeitet werden

an wen Daten weitergegeben werden

Berichtigung

Die betroffene Person verlangt die Korrektur fehlerhafter Daten.

Löschung

Die betroffene Person verlangt die Löschung ihrer Daten.

Dieses Recht wird häufig auch als:

`Recht auf Vergessenwerden`

bezeichnet.

Einschränkung der Verarbeitung

Die betroffene Person verlangt eine vorübergehende Einschränkung der Verarbeitung.

Datenübertragbarkeit

Die betroffene Person verlangt die Herausgabe ihrer Daten in einem strukturierten Format.

Widerspruch

Die betroffene Person widerspricht einer Verarbeitung.

Neues Betroffenenersuchen anlegen

Öffnen Sie das Modul:

Betroffenenersuchen

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Dokumentieren Sie mindestens:

Art des Ersuchens

Datum des Eingangs

Name der betroffenen Person

Beschreibung des Anliegens

Status

Fristen

Grundsätzlich gilt:

```
1 Monat
```

Bearbeitungsfrist nach Eingang des Ersuchens.

In begründeten Ausnahmefällen kann die Frist verlängert werden.

Die Verlängerung sollte dokumentiert werden.

Betroffenengruppen

Ordnen Sie die passenden Betroffenengruppen zu.

Beispiele:

Bewerber

Beschäftigte

Kunden

Lieferanten

Besucher

Datenkategorien

Ordnen Sie die betroffenen Datenkategorien zu.

Beispiele:

Stammdaten

Kontaktdaten

Vertragsdaten

Kommunikationsdaten

Gesundheitsdaten

Verknüpfung mit Verarbeitungstätigkeiten

Ein Betroffenenersuchen kann einer oder mehreren Verarbeitungstätigkeiten zugeordnet werden.

Dadurch wird nachvollziehbar:

wo die Daten verarbeitet werden

welche Systeme betroffen sind

welche Verantwortlichen beteiligt sind

Identitätsprüfung

Vor der Herausgabe personenbezogener Daten sollte geprüft werden, ob die anfragende Person tatsächlich die betroffene Person ist.

Dokumentieren Sie die durchgeführte Identitätsprüfung.

Antwort dokumentieren

Dokumentieren Sie:

Datum der Antwort

Inhalt der Antwort

übermittelte Informationen

verwendeten Kommunikationsweg

Dokumente hinterlegen

Zu jedem Betroffenenersuchen können Dokumente gespeichert werden.

Beispiele:

Anfrage der betroffenen Person

Identitätsnachweise

Antwortschreiben

interne Bewertungen

E-Mail-Kommunikation

Statusverwaltung

Empfohlene Statuswerte:

Offen

Anfrage wurde erfasst.

In Bearbeitung

Prüfung und Bearbeitung laufen.

Beantwortet

Antwort wurde versendet.

Abgeschlossen

Vorgang ist vollständig abgeschlossen.

Audits und Nachweise

Betroffenenersuchen gehören regelmäßig zu den Prüfpunkten interner und externer Audits.

Eine vollständige Dokumentation erleichtert den Nachweis der DSGVO-Konformität.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen eines Betroffenenersuchens erscheint eine Sicherheitsabfrage.

Aus Gründen der Nachvollziehbarkeit sollte geprüft werden, ob eine Löschung tatsächlich erforderlich ist.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 8 – Audits

Zweck des Moduls

Das Modul **Audit** dient der Planung, Durchführung und Dokumentation von Datenschutz- und PIMS-Audits.

Es unterstützt die Nachweisführung für:

- DSGVO
- ISO 27001
- ISO 27701
- interne Datenschutzkontrollen
- Managementbewertungen

Audits helfen dabei, Schwachstellen zu erkennen und Verbesserungspotenziale systematisch umzusetzen.

Was ist ein Audit?

Ein Audit ist eine strukturierte Überprüfung von Prozessen, Dokumentationen und Maßnahmen.

Dabei wird bewertet:

- ob Anforderungen erfüllt werden
- ob Maßnahmen wirksam sind
- ob Nachweise vorhanden sind
- ob Verbesserungsbedarf besteht

Neuen Audit-Eintrag anlegen

Öffnen Sie das Modul:

Audit

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Dokumentieren Sie mindestens:

- Auditdatum
- Auditor
- Auditobjekt
- Referenz
- Status

Auditobjekt

Das Auditobjekt beschreibt, was geprüft wurde.

Beispiele:

- Verarbeitungstätigkeit
- Dienstleister
- TOM
- PIMS-Kontrolle
- Steuerungsdokument
- gesamtes Datenschutzmanagementsystem

Feststellungen dokumentieren

Während des Audits sollten sämtliche Feststellungen dokumentiert werden.

Beispiele:

- fehlende Dokumentation
- unvollständige Nachweise
- nicht umgesetzte Maßnahmen
- positive Beobachtungen

Abweichungen bewerten

Der DatenschutzManager unterstützt verschiedene Arten von Feststellungen.

Keine Abweichung

Anforderung erfüllt.

Anmerkung

Verbesserungspotenzial vorhanden.

Nebenabweichung

Teilweise Nichterfüllung einer Anforderung.

Hauptabweichung

Wesentliche Nichterfüllung einer Anforderung.

Eine Hauptabweichung sollte zeitnah bearbeitet werden.

Risiken dokumentieren

Zu jeder Feststellung kann ein Risiko dokumentiert werden.

Beispiele:

- Niedrig
- Mittel
- Hoch

Dadurch können Maßnahmen priorisiert werden.

Maßnahmen festlegen

Aus Audits entstehen häufig Maßnahmen.

Beispiele:

- Richtlinie erstellen
- Nachweis ergänzen
- Schulung durchführen
- technische Anpassungen umsetzen

Die Maßnahmen können zusätzlich im Modul:

Maßnahmen

verfolgt werden.

Fristen setzen

Für jede Abweichung oder Maßnahme kann eine Frist festgelegt werden.

Dadurch lassen sich offene Punkte systematisch nachverfolgen.

Dokumente hinterlegen

Zu einem Audit können Dokumente gespeichert werden.

Beispiele:

- Auditberichte
- Checklisten
- Screenshots
- Nachweise
- Maßnahmenpläne

Statusverwaltung

Empfohlene Statuswerte:

Offen

Audit wurde angelegt.

In Bearbeitung

Feststellungen werden bearbeitet.

Abgeschlossen

Alle Maßnahmen wurden umgesetzt.

Zusammenhang mit PIMS

PIMS-Kontrollen können über Audits regelmäßig überprüft werden.

Dadurch entsteht ein nachvollziehbarer Verbesserungsprozess gemäß ISO 27701.

Managementbewertung

Audit-Ergebnisse bilden häufig die Grundlage für:

- Managementbewertungen
- Jahresberichte
- Datenschutzberichte
- Verbesserungsprogramme

Deshalb sollten Audits vollständig dokumentiert werden.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen eines Audit-Eintrags erscheint eine Sicherheitsabfrage.

Aus Gründen der Nachvollziehbarkeit sollte geprüft werden, ob eine Löschung tatsächlich erforderlich ist.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 9 – Maßnahmen

Zweck des Moduls

Das Modul **Maßnahmen** dient der Planung, Steuerung und Nachverfolgung von Verbesserungsmaßnahmen.

Maßnahmen entstehen häufig aus:

- Audits
- Datenschutzvorfällen
- Datenschutzfolgenabschätzungen (DSFA)
- PIMS-Kontrollen
- Managementbewertungen
- internen Verbesserungsprojekten

Das Modul unterstützt die kontinuierliche Verbesserung des Datenschutzmanagementsystems.

Was ist eine Maßnahme?

Eine Maßnahme beschreibt eine konkrete Aufgabe, die umgesetzt werden soll.

Beispiele:

- Richtlinie erstellen
- Dienstleister prüfen
- Multi-Faktor-Authentifizierung einführen
- Löschkonzept überarbeiten
- Datenschutzhinweise aktualisieren
- Mitarbeiter schulen

Neue Maßnahme anlegen

Öffnen Sie das Modul:

Maßnahmen

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Pflegen Sie mindestens:

- Titel
- Beschreibung
- Priorität
- Status
- Verantwortlicher
- Frist

Diese Angaben ermöglichen eine strukturierte Nachverfolgung.

Priorität festlegen

Die Priorität unterstützt die Reihenfolge der Umsetzung.

Niedrig

Verbesserung sinnvoll, aber nicht dringend.

Mittel

Soll zeitnah umgesetzt werden.

Hoch

Dringende Maßnahme mit erhöhtem Risiko.

Verantwortliche Person

Jede Maßnahme sollte einer verantwortlichen Person zugeordnet werden.

Beispiele:

- Datenschutzbeauftragter
- IT-Leitung
- Personalabteilung
- Fachbereich

Dadurch ist jederzeit nachvollziehbar, wer für die Umsetzung zuständig ist.

Fristen

Für jede Maßnahme kann eine Frist definiert werden.

Beispiele:

- kurzfristig
- mittelfristig
- langfristig

Empfehlung:

Fristen möglichst konkret mit Datum hinterlegen.

Statusverwaltung

Empfohlene Statuswerte:

Offen

Maßnahme wurde erfasst.

In Bearbeitung

Umsetzung läuft.

Wartet auf Rückmeldung

Umsetzung hängt von externen Faktoren ab.

Abgeschlossen

Maßnahme wurde vollständig umgesetzt.

Herkunft der Maßnahme

Maßnahmen können aus verschiedenen Quellen entstehen.

Beispiele:

Audit

Feststellung aus einem Audit.

Datenschutzvorfall

Korrekturmaßnahme nach einem Vorfall.

DSFA

Risikomindernde Maßnahme aus einer Datenschutzfolgenabschätzung.

PIMS-Kontrolle

Verbesserungsmaßnahme aus einer PIMS-Bewertung.

Freie Maßnahme

Unabhängig von anderen Modulen erfasste Verbesserung.

Wirksamkeitsprüfung

Nach Umsetzung sollte geprüft werden, ob die Maßnahme tatsächlich wirksam ist.

Beispiele:

- Nachaudit
- technische Prüfung
- Dokumentenprüfung
- Stichprobe

Die Ergebnisse können direkt in der Maßnahme dokumentiert werden.

Nachweise hinterlegen

Zu einer Maßnahme können Nachweise gespeichert werden.

Beispiele:

- Richtlinien
- Screenshots
- Auditberichte
- Schulungsunterlagen
- technische Dokumentationen

Empfehlung:

Nachweise möglichst zentral über Steuerungsdokumente verwalten.

Zusammenhang mit Audits

Maßnahmen bilden häufig die Reaktion auf Auditfeststellungen.

Dadurch entsteht ein nachvollziehbarer Verbesserungsprozess.

Zusammenhang mit Managementbewertungen

Offene und abgeschlossene Maßnahmen fließen regelmäßig in:

- Managementbewertungen
- Jahresberichte
- Datenschutzberichte

ein.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen einer Maßnahme erscheint eine Sicherheitsabfrage.

Bereits dokumentierte Nachweise und Zusammenhänge sollten vor dem Löschen geprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 10 – Steuerungsdokumente

Zweck des Moduls

Das Modul **Steuerungsdokumente** bildet die zentrale Nachweis- und Dokumentationsplattform des DatenschutzManagers.

Hier werden die wesentlichen Dokumente des Datenschutzmanagementsystems verwaltet.

Empfehlung:

Steuerungsdokumente sollten als zentrale Nachweisquelle genutzt werden. Dokumente sollten möglichst nicht mehrfach in verschiedenen Modulen hochgeladen werden.

Was sind Steuerungsdokumente?

Steuerungsdokumente beschreiben Vorgaben, Regeln, Verfahren und Nachweise innerhalb des Datenschutzmanagementsystems.

Beispiele:

- Datenschutzrichtlinien
- Verfahrensanweisungen
- Arbeitsanweisungen
- TOM-Dokumentationen
- Schulungsnachweise
- Löschkonzepte
- Notfallkonzepte
- Richtlinie Sichere Softwareentwicklung
- Berechtigungskonzepte

Neues Steuerungsdokument anlegen

Öffnen Sie das Modul:

Steuerungsdokumente

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Pflegen Sie mindestens:

- Titel
- Dokumenttyp
- Version
- Dokumentdatum
- Status

Dadurch entsteht eine nachvollziehbare Dokumentation.

Dokumenttypen

Beispiele für Dokumenttypen:

Richtlinie

Übergeordnete Regelungen.

Beispiele:

Datenschutzrichtlinie

Informationssicherheitsrichtlinie

Verfahrensanweisung

Beschreibt konkrete Abläufe.

Beispiele:

- Umgang mit Betroffenenersuchen
- Meldung von Datenschutzvorfällen

Arbeitsanweisung

Detaillierte Beschreibung einzelner Tätigkeiten.

Nachweis

Dokumentiert die Umsetzung von Anforderungen.

Beispiele:

- Schulungsnachweise
- Auditberichte
- Prüfprotokolle

Versionierung

Jedes Dokument kann versioniert werden.

Beispiel:

```
Version 1.0

Version 1.1

Version 2.0
```

Dadurch bleibt nachvollziehbar, welche Dokumentversion aktuell gültig ist.

Dokumentdateien hinterlegen

Zu jedem Steuerungsdokument können Dateien hinterlegt werden.

Beispiele:

- PDF
- Word-Dokumente
- Excel-Dateien
- Bilder
- Präsentationen

Ausgabe und Freigabe

Dokumentieren Sie:

- Freigabedatum
- Herausgeber
- Verantwortliche Stelle

Dadurch wird die Nachvollziehbarkeit verbessert.

Verknüpfung mit anderen Modulen

Steuerungsdokumente können mit verschiedenen Modulen verknüpft werden.

Beispiele:

Verarbeitungstätigkeiten

Nachweis der Umsetzung einer Verarbeitung.

TOM

Nachweis technischer und organisatorischer Maßnahmen.

PIMS-Kontrollen

Nachweis der Umsetzung von ISO-27701-Anforderungen.

Maßnahmen

Dokumentation umgesetzter Verbesserungen.

Audits

Auditberichte und Auditnachweise.

Nachweisstrategie

Empfohlene Vorgehensweise:

Dokumente möglichst nur einmal zentral als Steuerungsdokument pflegen und anschließend mit anderen Modulen verknüpfen.

Dadurch wird vermieden:

- doppelte Dokumentpflege
- unterschiedliche Versionen
- Inkonsistenzen

Dokumentenüberwachung

Das Modul unterstützt die regelmäßige Überprüfung von Dokumenten.

Empfehlung:

Prüfen Sie Richtlinien und Konzepte mindestens einmal jährlich.

Zusammenhang mit ISO 27701

Steuerungsdokumente bilden die wichtigste Nachweisquelle für:

- DSGVO
- ISO 27001
- ISO 27701

Viele Kontrollen und Auditfragen lassen sich direkt über hinterlegte Steuerungsdokumente beantworten.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen eines Steuerungsdokuments erscheint eine Sicherheitsabfrage.

Vorhandene Verknüpfungen zu anderen Modulen sollten vor dem Löschen geprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 11 – Informationspflichten

Zweck des Moduls

Das Modul **Informationspflichten** dient der Verwaltung und Dokumentation von Datenschutzhinweisen.

Die Informationspflichten ergeben sich insbesondere aus:

- Art. 13 DSGVO
- Art. 14 DSGVO

Betroffene Personen müssen darüber informiert werden, wie ihre personenbezogenen Daten verarbeitet werden.

Was sind Informationspflichten?

Informationspflichten beschreiben die Datenschutzhinweise, die betroffenen Personen zur Verfügung gestellt werden.

Beispiele:

- Datenschutzhinweise für Bewerber
- Datenschutzhinweise für Beschäftigte
- Datenschutzhinweise für Kunden
- Datenschutzhinweise für Lieferanten
- Datenschutzhinweise für Besucher
- Datenschutzhinweise für Webseiten

Neue Informationspflicht anlegen

Öffnen Sie das Modul:

Informationspflichten

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Pflegen Sie mindestens:

- Bezeichnung
- Zielgruppe
- Version
- Standdatum
- Verantwortlicher
- Status

Diese Angaben unterstützen die Nachvollziehbarkeit der Datenschutzhinweise.

Zielgruppe festlegen

Die Zielgruppe beschreibt, für wen die Information bestimmt ist.

Beispiele:

Bewerber

Informationen zum Bewerbungsverfahren.

Beschäftigte

Informationen zur Personalverwaltung.

Kunden

Informationen zur Kundenbetreuung und Vertragsabwicklung.

Lieferanten

Informationen zur Lieferantenverwaltung.

Besucher

Informationen zu Besucherverwaltung oder Videoüberwachung.

Versionierung

Informationspflichten sollten versioniert werden.

Beispiel:

```
Version 1.0

Version 1.1

Version 2.0
```

Dadurch bleibt nachvollziehbar, welche Version aktuell verwendet wird.

Dokument hinterlegen

Zu jeder Informationspflicht kann ein Dokument hinterlegt werden.

Beispiele:

- PDF-Datenschutzhinweis
- Word-Dokument
- veröffentlichte Datenschutzerklärung

Verantwortlicher

Dokumentieren Sie die verantwortliche Stelle.

Beispiele:

- Datenschutzbeauftragter
- Geschäftsführung
- Personalabteilung
- Marketingabteilung

Nächste Prüfung

Datenschutzhinweise sollten regelmäßig überprüft werden.

Empfehlung:

Mindestens einmal jährlich oder bei:

- Gesetzesänderungen
- neuen Verarbeitungstätigkeiten

- Einführung neuer Systeme
- organisatorischen Änderungen

Verknüpfung mit Verarbeitungstätigkeiten

Informationspflichten können direkt mit Verarbeitungstätigkeiten verknüpft werden.

Beispiel:

Verarbeitung

Bewerbermanagement

Zugeordnete Informationspflicht

Datenschutzhinweise für Bewerber

Dadurch wird nachvollziehbar, welche Datenschutzhinweise zu welcher Verarbeitung gehören.

Zusammenhang mit Betroffenenrechten

Informationspflichten bilden häufig die Grundlage für:

- Auskunftsersuchen
- Berichtigungsersuchen
- Löschersuchen
- Widersprüche

Eine aktuelle und vollständige Information reduziert häufig Rückfragen betroffener Personen.

Zusammenhang mit Audits

Informationspflichten gehören regelmäßig zu den Prüfgegenständen von:

- Datenschutz-Audits
- ISO-27701-Audits
- internen Kontrollen

Eine gepflegte Dokumentation erleichtert die Nachweisführung erheblich.

Statusverwaltung

Empfohlene Statuswerte:

Entwurf

Dokument wird erstellt oder überarbeitet.

Freigegeben

Dokument ist gültig und wird verwendet.

Archiviert

Dokument wird nicht mehr verwendet, bleibt aber aus Nachweisgründen erhalten.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen einer Informationspflicht erscheint eine Sicherheitsabfrage.

Vorhandene Verknüpfungen zu Verarbeitungstätigkeiten sollten vor dem Löschen geprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 12 – Sensibilisierung und Schulungen

Zweck des Moduls

Das Modul **Sensibilisierung** dient der Dokumentation von Datenschutz- und Informationssicherheits-Schulungen.

Mitarbeiter stellen einen wesentlichen Erfolgsfaktor für Datenschutz und Informationssicherheit dar.

Regelmäßige Sensibilisierungsmaßnahmen helfen dabei:

Datenschutzverstöße zu vermeiden

Sicherheitsvorfälle zu reduzieren

gesetzliche Anforderungen zu erfüllen

das Datenschutzbewusstsein zu stärken

Warum sind Schulungen wichtig?

Viele Datenschutzvorfälle entstehen nicht durch technische Fehler, sondern durch menschliche Fehlhandlungen.

Beispiele:

- Versand von E-Mails an falsche Empfänger
- Nutzung unsicherer Passwörter
- Phishing-Angriffe
- Verlust mobiler Geräte
- Fehlkonfigurationen
- Regelmäßige Schulungen reduzieren diese Risiken erheblich.

Neue Sensibilisierungsmaßnahme anlegen

Öffnen Sie das Modul:

Sensibilisierung

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Pflegen Sie mindestens:

- Titel
- Datum
- Zielgruppe
- Verantwortlicher

Status

Beispiele:

```
Datenschutzschulung 2026

Phishing Awareness Training

Einführung DSGVO für neue Mitarbeiter

Microsoft 365 Security Workshop
```

Zielgruppe festlegen

Dokumentieren Sie, wer an der Maßnahme teilnehmen soll.

Beispiele:

Alle Mitarbeiter

Unternehmensweite Schulung.

Führungskräfte

Schulung für Verantwortliche.

Personalabteilung

Spezielle Schulung zu Bewerber- und Beschäftigtendaten.

IT-Abteilung

Technische Datenschutz- und Sicherheitsmaßnahmen.

Inhalte dokumentieren

Beschreiben Sie die behandelten Themen.

Beispiele:

- DSGVO-Grundlagen
- Betroffenenrechte
- Umgang mit Datenschutzvorfällen
- Passwortsicherheit
- Phishing-Erkennung
- Mobile Geräte
- Clean-Desk-Policy
- Homeoffice-Sicherheit

Nachweise hinterlegen

Zu jeder Schulungsmaßnahme können Nachweise hinterlegt werden.

Beispiele:

- Teilnehmerlisten
- Präsentationen
- Schulungsunterlagen
- Zertifikate
- Screenshots
- Lernnachweise

Wiederkehrende Schulungen

Empfehlung:

Datenschutzschulungen sollten regelmäßig durchgeführt werden.

Typische Intervalle:

Jährlich

Standard für Datenschutzschulungen.

Halbjährlich

Bei erhöhtem Risiko oder sensiblen Daten.

Anlassbezogen

Bei:

- neuen Prozessen
- neuen Systemen
- Datenschutzvorfällen
- Gesetzesänderungen

Zusammenhang mit Audits

Sensibilisierungsmaßnahmen werden häufig in Audits geprüft.

Typische Auditfragen:

- Wurden Mitarbeiter geschult?
- Wann fand die letzte Schulung statt?
- Gibt es Nachweise?
- Welche Inhalte wurden vermittelt?

Eine vollständige Dokumentation erleichtert die Nachweisführung erheblich.

Zusammenhang mit PIMS und ISO 27701

Schulungen und Sensibilisierung sind wichtige Bestandteile eines Privacy Information Management Systems (PIMS).

Sie unterstützen:

- Datenschutzbewusstsein
- Verantwortlichkeiten
- kontinuierliche Verbesserung
- Compliance-Nachweise

Statusverwaltung

Empfohlene Statuswerte:

Geplant

Schulung wurde vorbereitet.

In Durchführung

Maßnahme läuft aktuell.

Abgeschlossen

Schulung wurde erfolgreich durchgeführt.

Wiederholung erforderlich

Neue Schulung ist notwendig.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen einer Sensibilisierungsmaßnahme erscheint eine Sicherheitsabfrage.

Bereits hinterlegte Nachweise und Teilnehmerinformationen sollten vor dem Löschen geprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 13 – PIMS-Kontrollen (ISO 27701)

Zweck des Moduls

Das Modul **PIMS-Kontrollen** unterstützt die Umsetzung und Dokumentation eines Privacy Information Management Systems (PIMS) nach ISO 27701.

Es dient dazu, Datenschutzanforderungen systematisch zu bewerten, nachzuweisen und kontinuierlich zu verbessern.

Die Kontrollen bilden die Grundlage für:

- Datenschutzmanagement
- Privacy Governance
- Managementbewertungen
- Audits
- Reifegradbewertungen
- Nachweisführung gegenüber Kunden und Auditoren

Was ist eine PIMS-Kontrolle?

Eine PIMS-Kontrolle beschreibt eine konkrete Anforderung aus dem Datenschutzmanagement.

Beispiele:

- Verantwortlichkeiten definiert
- Verfahren für Betroffenenrechte vorhanden
- Datenschutzvorfälle dokumentiert
- Dienstleister überprüft
- Löschkonzept umgesetzt
- Schulungen durchgeführt
- Informationspflichten vorhanden

Neue PIMS-Kontrolle anlegen

Öffnen Sie das Modul:

PIMS-Kontrollen

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Pflegen Sie mindestens:

- Titel
- Kontrollbeschreibung
- Status
- Reifegrad
- Verantwortlicher

Beispiel:

```
Informationspflichten dokumentiert
```

oder

```
Verfahren für Betroffenenrechte vorhanden
```

Reifegradbewertung

Jede Kontrolle kann bewertet werden.

Empfohlene Bewertung:

0 – Nicht vorhanden

Die Anforderung wurde bisher nicht umgesetzt.

---

1 – Geplant

Die Umsetzung wurde geplant.

---

2 – Teilweise umgesetzt

Einzelne Bestandteile sind vorhanden.

---

3 – Weitgehend umgesetzt

Die Kontrolle wird bereits genutzt.

---

4 – Vollständig umgesetzt

Die Kontrolle ist vollständig eingeführt.

---

5 – Optimiert

Die Kontrolle wird regelmäßig überprüft und verbessert.

Nachweise hinterlegen

Zu jeder Kontrolle können Nachweise hinterlegt werden.

Beispiele:

- Richtlinien
- Verfahrensanweisungen
- Auditberichte
- Schulungsnachweise
- Protokolle
- Dokumentationen

Empfehlung:

Steuerungsdokumente als zentrale Nachweisquelle verwenden.

Verknüpfung mit Verarbeitungstätigkeiten

PIMS-Kontrollen können direkt mit Verarbeitungstätigkeiten verknüpft werden.

Beispiel:

Verarbeitung

Bewerbermanagement

PIMS-Kontrolle

Informationspflichten dokumentiert

Dadurch wird nachvollziehbar, welche Datenschutzanforderungen für welche Verarbeitung umgesetzt wurden.

Zusammenhang mit Maßnahmen

Werden Defizite festgestellt, können daraus Maßnahmen entstehen.

Beispiele:

- Datenschutzhinweise erstellen
- Löschkonzept ergänzen
- Dienstleister überprüfen
- Schulungen durchführen

Diese Maßnahmen können im Modul:

Maßnahmen

weiter verfolgt werden.

Zusammenhang mit Audits

PIMS-Kontrollen bilden einen wichtigen Bestandteil interner und externer Audits.

Typische Fragestellungen:

- Ist die Kontrolle umgesetzt?
- Gibt es Nachweise?
- Ist die Kontrolle wirksam?
- Wird sie regelmäßig überprüft?

Zusammenhang mit Managementbewertungen

Die Ergebnisse der PIMS-Kontrollen fließen häufig in:

- Managementbewertungen
- Datenschutzberichte
- Jahresberichte
- Reifegradanalysen

ein.

Dadurch entsteht ein kontinuierlicher Verbesserungsprozess.

Statusverwaltung

Empfohlene Statuswerte:

Offen

Kontrolle noch nicht umgesetzt.

In Bearbeitung

Umsetzung läuft.

Umgesetzt

Kontrolle vollständig umgesetzt.

Überprüfung erforderlich

Regelmäßige Neubewertung notwendig.

ISO-27701-Nachweis

Die dokumentierten Kontrollen können als Nachweis für die Umsetzung von Anforderungen aus ISO 27701 dienen.

Dies erleichtert:

- Zertifizierungen
- Audits
- Kundenanfragen
- interne Bewertungen

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen einer PIMS-Kontrolle erscheint eine Sicherheitsabfrage.

Vorhandene Nachweise und Verknüpfungen sollten vor dem Löschen geprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 14 – Applikationsprüfung

Zweck des Moduls

Das Modul **Applikationsprüfung** dient der datenschutzrechtlichen und organisatorischen Bewertung von Anwendungen, Softwarelösungen und Cloud-Diensten.

Vor der Einführung neuer Systeme sollte geprüft werden, ob die Anwendung die Anforderungen an Datenschutz und Informationssicherheit erfüllt.

Die Applikationsprüfung unterstützt insbesondere:

- Datenschutz-Folgenabschätzungen
- Lieferantenbewertungen
- Softwarefreigaben
- Risikoanalysen
- PIMS-Anforderungen nach ISO 27701

Wann sollte eine Applikationsprüfung durchgeführt werden?

Eine Prüfung empfiehlt sich insbesondere bei:

- neuer Software
- Cloud-Diensten
- SaaS-Lösungen
- KI-Anwendungen
- mobilen Apps
- Fachanwendungen
- Collaboration-Plattformen
- Beispiele:
- Microsoft 365
- Teams
- Copilot
- DATEV
- SAP
- Jira
- Confluence
- Synthesia
- ChatGPT Enterprise

Neue Applikationsprüfung anlegen

Öffnen Sie das Modul:

Applikationsprüfung

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Pflegen Sie mindestens:

- Name der Anwendung
- Hersteller
- Version

Zweck der Anwendung

Status

Beispiele:

```
Microsoft Teams

Microsoft Corporation

ChatGPT Enterprise

OpenAI
```

Hersteller bewerten

Dokumentieren Sie:

- Hersteller
- Sitz des Unternehmens
- Ansprechpartner
- Supportinformationen

Diese Informationen unterstützen spätere Audits und Bewertungen.

Datenschutzbewertung

Prüfen Sie insbesondere:

Personenbezogene Daten

Werden personenbezogene Daten verarbeitet?

Besondere Kategorien personenbezogener Daten

Werden sensible Daten verarbeitet?

Beispiele:

- Gesundheitsdaten
- Religionsdaten
- biometrische Daten

Drittlandtransfer

Werden Daten außerhalb der EU bzw. des EWR verarbeitet?

Falls ja:

- Zielland dokumentieren
- Rechtsgrundlage dokumentieren
- Schutzmaßnahmen bewerten

Technische Bewertung

Prüfen Sie beispielsweise:

Authentifizierung

MFA vorhanden?

Rollenmodell vorhanden?

Verschlüsselung

Datenübertragung verschlüsselt?

Datenspeicherung verschlüsselt?

Protokollierung

Audit-Logs vorhanden?

Nachvollziehbarkeit gewährleistet?

Backup und Wiederherstellung

Backup-Konzept vorhanden?

Wiederherstellung dokumentiert?

Auftragsverarbeitung

Prüfen Sie:

- Liegt ein AVV vor?
- Ist der Vertrag aktuell?
- Sind TOM dokumentiert?

Falls vorhanden, können Dienstleister und AVV separat dokumentiert und verknüpft werden.

Risikobewertung

Bewerten Sie die Anwendung.

Empfohlene Einstufungen:

Niedrig

Geringe Risiken.

Mittel

Normale Geschäftsanwendung.

Hoch

Erhöhte Risiken oder kritische Daten.

Verknüpfung mit Verarbeitungstätigkeiten

Eine Applikation kann mehreren Verarbeitungstätigkeiten zugeordnet werden.

Beispiel:

Anwendung

Microsoft Teams

Verarbeitungen

- Personalverwaltung
- Bewerbermanagement
- Kundenkommunikation

Dadurch entsteht Transparenz über die eingesetzten Systeme.

Nachweise hinterlegen

Zu jeder Applikationsprüfung können Nachweise gespeichert werden.

Beispiele:

- Datenschutzerklärungen
- Zertifikate
- AVV
- TOM
- Auditberichte
- Herstellerinformationen

Zusammenhang mit DSFA

Eine Applikationsprüfung ersetzt keine Datenschutzfolgenabschätzung.

Die Ergebnisse können jedoch wichtige Informationen für eine DSFA liefern.

Zusammenhang mit Audits

Applikationsprüfungen werden häufig im Rahmen von:

- Datenschutz-Audits
- ISO-27001-Audits
- ISO-27701-Audits

als Nachweis herangezogen.

Statusverwaltung

Empfohlene Statuswerte:

In Prüfung

Bewertung läuft.

Freigegeben

Anwendung kann eingesetzt werden.

Freigegeben mit Auflagen

Einsatz nur unter bestimmten Bedingungen.

Abgelehnt

Anwendung erfüllt die Anforderungen nicht.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen einer Applikationsprüfung erscheint eine Sicherheitsabfrage.

Vorhandene Nachweise und Verknüpfungen sollten vor dem Löschen geprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 15 – Fristenverwaltung

Zweck des Moduls

Das Modul **Fristenverwaltung** unterstützt die zentrale Verwaltung von Aufbewahrungs- und Löschfristen.

- Die Fristenverwaltung dient dazu:
- gesetzliche Aufbewahrungspflichten zu dokumentieren
- Löschkonzepte umzusetzen
- Verarbeitungstätigkeiten einheitlich zu bewerten
- Nachweise für Audits bereitzustellen

Die Fristen werden zentral gepflegt und können anschließend in mehreren Verarbeitungstätigkeiten verwendet werden.

Warum eine zentrale Fristenverwaltung?

In vielen Unternehmen werden dieselben Fristen mehrfach dokumentiert.

Beispiele:

- Handelsrechtliche Aufbewahrungsfristen
- Steuerrechtliche Aufbewahrungsfristen
- Personalunterlagen
- Vertragsunterlagen
- Durch die zentrale Fristenverwaltung werden Doppelarbeiten vermieden.
- Eine Änderung an einer Frist muss nur einmal vorgenommen werden.

Neue Frist anlegen

Öffnen Sie das Modul:

Fristen

und klicken Sie auf:

Neu

Der Datensatz wird sofort angelegt und kann anschließend bearbeitet werden.

Allgemeine Angaben

Pflegen Sie mindestens:

- Bezeichnung
- Kategorie
- Rechtsgrundlage
- Fristdauer
- Behandlung nach Fristablauf

Bezeichnung

Die Bezeichnung sollte eindeutig sein.

Beispiele:

```
Handelsbriefe

Steuerunterlagen

Personalakten

Bewerbungsunterlagen

Vertragsunterlagen
```

Kategorie

Die Kategorie dient der besseren Übersicht.

Beispiele:

- Personal
- Vertrieb
- Finanzen
- Datenschutz
- Allgemeine Verwaltung

Rechtsgrundlage

Dokumentieren Sie die gesetzliche Grundlage.

Beispiele:

```
HGB

AO
```

DSGVO

BGB

Diese Information erleichtert spätere Audits und Nachweise.

Fristdauer

Legen Sie die Dauer der Aufbewahrung fest.

Beispiele:

6 Jahre

10 Jahre

3 Monate

2 Jahre

Behandlung nach Fristablauf

Dokumentieren Sie, was nach Ablauf der Frist erfolgen soll.

Beispiele:

Löschen

Daten werden vollständig gelöscht.

Vernichten

Physische Unterlagen werden vernichtet.

Archivieren

Dokumente werden dauerhaft archiviert.

Prüfen

Manuelle Entscheidung erforderlich.

Import bestehender Fristen

Der DatenschutzManager unterstützt den Import von Fristen.

Dadurch können vorhandene Fristenkataloge übernommen werden.

Empfehlung:

Nach einem Import die Fristen kurz prüfen und bei Bedarf anpassen.

Verknüpfung mit Verarbeitungstätigkeiten

Fristen können direkt in Verarbeitungstätigkeiten verwendet werden.

Beispiel:

Verarbeitung

Personalverwaltung

Verwendete Frist

Personalakten – 10 Jahre

Dadurch wird die Frist automatisch innerhalb der Verarbeitung dokumentiert.

Zusammenhang mit Löschkonzepten

Die Fristenverwaltung bildet die Grundlage für:

- Löschkonzepte
- Aufbewahrungskonzepte
- Datenschutzberichte
- Audits

Eine zentrale Pflege reduziert Fehler und Inkonsistenzen.

Zusammenhang mit Audits

Fristen gehören regelmäßig zu den Prüffeldern interner und externer Audits.

Typische Fragen:

- Welche Frist gilt?

- Auf welcher Rechtsgrundlage basiert die Frist?
- Wie wird nach Fristablauf verfahren?

Eine gepflegte Fristenverwaltung erleichtert die Nachweisführung erheblich.

Aktualisieren

Über die Funktion:

Aktualisieren

werden Listen und Zuordnungen neu geladen.

Dies ist insbesondere nach Importen hilfreich.

Speichern

Änderungen werden über:

- Speichern in der Symbolleiste
- Tastenkombination ⌘S

gespeichert.

Löschen

Vor dem Löschen einer Frist erscheint eine Sicherheitsabfrage.

Vorhandene Zuordnungen zu Verarbeitungstätigkeiten sollten vor dem Löschen geprüft werden.

Es wird empfohlen, regelmäßig Backups zu erstellen.

Kapitel 16 – Berichte und Auswertungen

Zweck des Moduls

Das Modul **Berichte** dient der Erstellung von Nachweisen, Übersichten und Managementinformationen.

Berichte ermöglichen es, die im DatenschutzManager gepflegten Informationen strukturiert auszuwerten und als Dokument bereitzustellen.

Die Berichte unterstützen insbesondere:

- Datenschutzbeauftragte
- Auditoren
- Geschäftsleitungen
- Managementbewertungen
- Zertifizierungen
- Kundenanfragen

Warum Berichte wichtig sind

Die Dokumentation allein reicht häufig nicht aus.

In Audits oder Managementbesprechungen werden Informationen oft in verdichteter Form benötigt.

Beispiele:

- Welche Verarbeitungstätigkeiten existieren?
- Welche Risiken wurden bewertet?
- Welche Maßnahmen sind noch offen?
- Welche PIMS-Kontrollen sind umgesetzt?
- Welche Datenschutzvorfälle wurden dokumentiert?

Das Modul Berichte stellt diese Informationen übersichtlich zusammen.

Verzeichnis der Verarbeitungstätigkeiten

Der wichtigste Bericht ist das:

```
Verzeichnis der Verarbeitungstätigkeiten
```

Dieser Bericht fasst sämtliche dokumentierten Verarbeitungstätigkeiten zusammen.

Typische Inhalte:

- Bezeichnung

- Zweck
- Rechtsgrundlage
- Betroffenengruppen
- Datenkategorien
- Empfänger
- Speicherfristen

DSFA-Berichte

Datenschutzfolgenabschätzungen können als Bericht ausgegeben werden.

Beispiele:

vollständige DSFA-Dokumentation

Risikobewertungen

Maßnahmenübersichten

Diese Berichte eignen sich insbesondere für Audits und interne Prüfungen.

Maßnahmenübersichten

Berichte können offene und abgeschlossene Maßnahmen darstellen.

Beispiele:

Offene Maßnahmen

Verantwortlicher

Frist

Priorität

Status

Abgeschlossene Maßnahmen

Umsetzungsdatum

Wirksamkeitsprüfung

Nachweise

Audit-Berichte

Auditinformationen können strukturiert ausgegeben werden.

Beispiele:

- Feststellungen
- Abweichungen
- Risiken
- offene Punkte
- abgeschlossene Punkte

PIMS-Berichte

Für ein Privacy Information Management System können Berichte erzeugt werden.

Beispiele:

- PIMS-Kontrollen
- Reifegradbewertungen
- Umsetzungsstatus
- Nachweise

Diese Berichte unterstützen insbesondere ISO-27701-Audits.

Managementbewertungen

Der DatenschutzManager unterstützt die Erstellung von Managementinformationen.

Beispiele:

- Anzahl Verarbeitungstätigkeiten
- offene Maßnahmen
- offene Audits
- Datenschutzvorfälle
- Reifegradentwicklungen

Diese Informationen können für Managementbewertungen genutzt werden.

KPI-Berichte

KPIs (Key Performance Indicators) ermöglichen eine Messung der Datenschutzorganisation.

Beispiele:

- Anzahl offener Maßnahmen
- Anzahl abgeschlossener Maßnahmen
- Anzahl Datenschutzvorfälle
- Anzahl Audits
- Anzahl Schulungen

PDF-Ausgabe

Berichte werden als PDF-Dokumente erzeugt.

Vorteile:

- einfache Weitergabe
- revisionssichere Archivierung
- Auditnachweise
- Managementberichte

Verwendung in Audits

Berichte werden häufig verwendet für:

- interne Audits
- externe Audits
- Zertifizierungen
- Kundenprüfungen

Eine aktuelle Datenpflege verbessert die Qualität der Berichte erheblich.

Empfehlungen

Für aussagekräftige Berichte sollten insbesondere folgende Module gepflegt werden:

- Verarbeitungstätigkeiten
- Dienstleister
- TOM
- DSFA
- Maßnahmen
- PIMS-Kontrollen
- Audits
- Datenschutzvorfälle

Je vollständiger die Datenbasis, desto aussagekräftiger die Berichte.

Export und Archivierung

Berichte können:

- gespeichert
- archiviert
- versendet
- als Nachweis verwendet

werden.

Empfehlung:

Wichtige Berichte regelmäßig archivieren und in die Nachweisführung aufnehmen.

Speichern und Aktualisieren

Die Berichtsinhalte basieren auf den aktuell gespeicherten Daten.

Vor der Berichtserstellung empfiehlt es sich:

offene Änderungen zu speichern

Daten zu aktualisieren

Vollständigkeit zu prüfen

Dadurch wird sichergestellt, dass die Berichte den aktuellen Stand des Datenschutzmanagementsystems widerspiegeln.

Kapitel 17 – Dashboard

Zweck des Dashboards

Das Dashboard ist die zentrale Startseite des DatenschutzManagers.

Es bietet einen schnellen Überblick über den aktuellen Zustand des Datenschutzmanagementsystems (DSMS) und des Privacy Information Management Systems (PIMS).

Nach der Anmeldung gelangen Sie direkt auf das Dashboard.

Ziel des Dashboards

Das Dashboard soll die wichtigsten Informationen auf einen Blick bereitstellen.

Beispiele:

- offene Aufgaben
- offene Maßnahmen
- Datenschutzvorfälle
- Audits
- Betroffenenersuchen
- PIMS-Status
- wichtige Kennzahlen

Dadurch können Risiken und Handlungsbedarfe frühzeitig erkannt werden.

Kennzahlen (KPI)

Das Dashboard zeigt verschiedene Kennzahlen an.

Typische Kennzahlen sind:

Verarbeitungstätigkeiten

Anzahl dokumentierter Verarbeitungstätigkeiten.

Dienstleister

Anzahl erfasster Dienstleister und Auftragsverarbeiter.

TOM

Anzahl dokumentierter technischer und organisatorischer Maßnahmen.

Datenschutzvorfälle

Anzahl erfasster Datenschutzvorfälle.

Betroffenenersuchen

Anzahl offener und abgeschlossener Anfragen betroffener Personen.

Maßnahmen

Anzahl offener und abgeschlossener Maßnahmen.

Audits

Anzahl dokumentierter Audits.

Offene Aufgaben

Das Dashboard unterstützt die Identifikation offener Aufgaben.

Beispiele:

- offene Maßnahmen
- abgelaufene Fristen
- offene Audits
- fehlende Nachweise
- noch nicht umgesetzte PIMS-Kontrollen

Managementübersicht

Das Dashboard eignet sich als Managementübersicht.

Es ermöglicht eine schnelle Beurteilung:

- des Datenschutzstatus

- des Reifegrades
- der offenen Risiken
- der Umsetzungsstände

PIMS-Status

Sofern PIMS-Kontrollen gepflegt werden, kann das Dashboard Informationen zum Umsetzungsgrad anzeigen.

Beispiele:

- offene Kontrollen
- umgesetzte Kontrollen
- Reifegradentwicklung

Datenschutzvorfälle

Vorfälle mit erhöhtem Risiko können im Dashboard hervorgehoben werden.

Dadurch werden kritische Ereignisse schneller sichtbar.

Betroffenenersuchen

Offene Anfragen betroffener Personen können im Dashboard überwacht werden.

Insbesondere Fristen sollten regelmäßig kontrolliert werden.

Audits

Das Dashboard kann einen Überblick über:

- geplante Audits
- laufende Audits
- abgeschlossene Audits

bereitstellen.

Maßnahmen

Offene Maßnahmen stellen häufig den wichtigsten Arbeitsvorrat dar.

Das Dashboard unterstützt die Priorisierung und Nachverfolgung.

Berichte und Auswertungen

Das Dashboard dient als Einstiegspunkt für:

- Berichte
- Managementbewertungen
- KPI-Auswertungen

Empfohlene Nutzung

Empfehlung:

Öffnen Sie das Dashboard regelmäßig als erste Seite nach der Anmeldung.

Dadurch erhalten Sie einen schnellen Überblick über:

- offene Risiken
- offene Aufgaben
- anstehende Fristen
- Verbesserungsmaßnahmen

Hinweise

Das Dashboard ersetzt keine Detailprüfung einzelner Module.

Es dient ausschließlich der Übersicht und Priorisierung.

Die eigentliche Bearbeitung erfolgt in den jeweiligen Fachmodulen.

Best Practice

Eine bewährte Vorgehensweise ist:

- Dashboard prüfen
- Offene Aufgaben identifizieren
- Maßnahmen priorisieren
- Fachmodule bearbeiten
- Ergebnisse dokumentieren

Dadurch bleibt das Datenschutzmanagementsystem dauerhaft aktuell und nachvollziehbar.

Kapitel 18 – Einstellungen, Sicherheit, Backup und Wiederherstellung

Zweck des Moduls

Das Modul **Einstellungen** dient der zentralen Verwaltung systemweiter Einstellungen des DatenschutzManagers.

Hier finden Sie Funktionen für:

- Sicherheit
- Passwortschutz
- Backup
- Wiederherstellung
- Kataloge
- Systemverwaltung

Die Einstellungen gelten mandantenübergreifend für die gesamte Anwendung.

Sicherheitskonzept

Der DatenschutzManager wurde für die Verarbeitung datenschutzrelevanter Informationen entwickelt.

Daher stehen Sicherheitsfunktionen bereits standardmäßig zur Verfügung.

Beispiele:

- Passwortschutz
- verschlüsselte Datenspeicherung
- verschlüsselte Backups
- Zugriffsschutz
- lokale Datenhaltung

Passwortschutz

Beim ersten Start kann ein Kennwort eingerichtet werden.

Dieses Kennwort schützt den Zugriff auf:

- Mandanten
- Verarbeitungstätigkeiten
- Dokumente
- Nachweise
- Berichte

Ohne gültiges Kennwort kann die Anwendung nicht geöffnet werden.

Kennwort ändern

Empfehlung:

Verwenden Sie ein sicheres Kennwort mit:

- Großbuchstaben
- Kleinbuchstaben
- Zahlen
- Sonderzeichen

Ein sicheres Kennwort schützt die gespeicherten Datenschutzinformationen vor unberechtigtem Zugriff.

Backup erstellen

Öffnen Sie:

```
Einstellungen

→ Backup
```

und wählen Sie:

```
Backup erstellen
```

Der DatenschutzManager erstellt eine Sicherung der Datenbank sowie der zugehörigen Dokumente.

Optional können Backups zusätzlich verschlüsselt werden.

Verschlüsselte Backups

Für besonders schützenswerte Daten empfiehlt sich die Nutzung verschlüsselter Backups.

Vorteile:

- Schutz bei Verlust des Datenträgers
- Schutz bei Diebstahl
- sichere Archivierung

Wichtig:

Das Backup-Kennwort sollte sicher dokumentiert werden.

Ohne Kennwort kann ein verschlüsseltes Backup nicht wiederhergestellt werden.

Backup wiederherstellen

Öffnen Sie:

```
Einstellungen
```

```
→ Backup
```

und wählen Sie:

```
Backup wiederherstellen
```

Anschließend wählen Sie die gewünschte Sicherungsdatei aus.

Bei verschlüsselten Backups wird zusätzlich das Backup-Kennwort abgefragt.

Wiederherstellung nach Systemwechsel

Die Wiederherstellung eignet sich insbesondere für:

- neue Macs
- Hardwarewechsel
- Notfallwiederherstellung
- Testsysteme

Nach erfolgreicher Wiederherstellung stehen sämtliche Daten und Dokumente wieder zur Verfügung.

Kataloge

Über die Einstellungen können zentrale Kataloge gepflegt werden.

- Dazu gehören:
- Betroffenengruppen
- Datenkategorien
- Risikoeinstufungen

Diese Kataloge werden in verschiedenen Modulen verwendet.

Warum sind Kataloge wichtig?

Kataloge sorgen für:

- einheitliche Bezeichnungen
- konsistente Auswertungen
- bessere Berichte
- weniger Eingabefehler

Empfehlung:

Kataloge möglichst zentral pflegen und regelmäßig überprüfen.

Aufbewahrungsfristen

Aufbewahrungsfristen werden ebenfalls zentral verwaltet.

Sie können später in Verarbeitungstätigkeiten verwendet werden.

Dadurch werden gesetzliche Fristen einheitlich dokumentiert.

Lizenzierung

Der DatenschutzManager verwendet eine Arbeitsplatzlizenz.

Grundsatz:

```
1 Arbeitsplatz = 1 Lizenz
```

Die Anwendung ist vollständig offline nutzbar.

Es erfolgt keine permanente Online-Lizenzprüfung.

Datenschutz

Die Anwendung wurde für eine datenschutzfreundliche Nutzung entwickelt.

Grundsätze:

- lokale Datenhaltung
- keine Cloud-Pflicht
- keine dauerhafte Internetverbindung erforderlich
- keine automatische Datenübertragung an Dritte

Empfehlungen

Empfohlen wird:

- regelmäßige Backups
- sichere Kennwörter
- jährliche Überprüfung der Kataloge
- regelmäßige Aktualisierung der Datenschutzdokumentation

Best Practice

Nach größeren Änderungen sollte immer:

- gespeichert werden
- ein Backup erstellt werden
- die Wiederherstellbarkeit getestet werden

Dadurch wird sichergestellt, dass das Datenschutzmanagementsystem jederzeit wiederhergestellt werden kann.

Kapitel 19 – KI-Unterstützung (Optional)

Zweck der KI-Unterstützung

Der DatenschutzManager kann optional mit einer lokalen oder unternehmensintern betriebenen KI-Lösung verbunden werden.

Die KI dient als Assistenzsystem zur Analyse, Plausibilitätsprüfung, Dokumentationsunterstützung und Erstellung von Formulierungsvorschlägen.

Die Nutzung der KI ist vollständig optional. Der DatenschutzManager kann ohne KI-Unterstützung uneingeschränkt betrieben werden.

Die KI ersetzt keine rechtliche Beratung, keine fachliche Bewertung durch einen Datenschutzbeauftragten und keine Managemententscheidung.

Grundprinzip

Die KI ist direkt in verschiedene Fachmodule integriert.

Anwender arbeiten weiterhin in den jeweiligen Modulen. Die KI analysiert die bereits dokumentierten Informationen und erstellt strukturierte Hinweise, Empfehlungen und Formulierungsvorschläge.

Alle Ergebnisse dienen ausschließlich als Unterstützung und müssen fachlich überprüft werden.

Einrichtung der KI-Unterstützung

Die KI-Unterstützung muss zunächst eingerichtet werden.

Öffnen Sie hierzu:

Einstellungen
→ KI-Konfiguration

Folgende Betriebsarten werden unterstützt:

Lokales KI-Modell

Bei dieser Betriebsart kommuniziert der DatenschutzManager direkt mit einer lokalen oder unternehmensintern betriebenen KI-Lösung.

Beispiele:

- Ollama
- Open WebUI
- Unternehmensinterne KI-Systeme

Konfiguriert werden:

- Serveradresse (IP-Adresse oder Hostname)
- Port
- Modellname
- Verbindungsprüfung

RAG-System (Retrieval Augmented Generation)

Alternativ kann ein RAG-System angebunden werden.

Dabei werden KI-Antworten mit einer Wissensbasis kombiniert.

Typische Wissensquellen:

- DSGVO
- BDSG
- DSG (Österreich)
- ISO 27001
- ISO 27701
- EU AI Act
- interne Richtlinien
- Steuerungsdokumente
- Unternehmenswissen

Konfiguriert werden:

- Serveradresse (IP-Adresse oder Hostname)
- Port
- API-Endpunkt
- Authentifizierung (optional)

Verbindungsprüfung

Über die integrierte Verbindungsprüfung kann überprüft werden, ob die konfigurierte KI erreichbar ist.

Bei erfolgreicher Verbindung können die KI-Funktionen unmittelbar genutzt werden.

Integrierte KI-Unterstützung

Die KI ist direkt in verschiedene Fachmodule integriert.

Unterstützte Module

Verarbeitungstätigkeiten

Die KI unterstützt insbesondere bei:

- Vollständigkeitsprüfungen
- Plausibilitätsprüfungen
- Verbesserung von Formulierungen
- Identifikation möglicher fehlender Verarbeitungstätigkeiten
- Vorschlägen für ergänzende Dokumentationen
- Hinweisen auf mögliche fehlende Datenschutzanforderungen

Datenschutzfolgenabschätzungen (DSFA)

Die KI unterstützt insbesondere bei:

- Plausibilitätsprüfungen von DSFA
- Bewertung dokumentierter Risiken
- Identifikation möglicher fehlender Risiken
- Vorschlägen für zusätzliche Maßnahmen
- Bewertung des Restrisikos
- Hinweisen auf mögliche DSFA-Erforderlichkeit

Datenschutzvorfälle

Die KI unterstützt insbesondere bei:

- Ersteinschätzung von Datenschutzvorfällen
- Bewertung möglicher Risiken für betroffene Personen
- Prüfung möglicher Meldepflichten
- Prüfung möglicher Informationspflichten gegenüber Betroffenen
- Vorschlägen für Sofortmaßnahmen
- Vorschlägen für Folgemaßnahmen
- Unterstützung der Dokumentation

Betroffenenersuchen

Die KI unterstützt insbesondere bei:

- Prüfung von Fristen
- Plausibilitätsprüfung von Betroffenenersuchen
- Prüfung der Identitätsfeststellung
- Unterstützung bei Antwortentwürfen
- Berücksichtigung dokumentierter Speicherfristen
- Berücksichtigung dokumentierter Löschkonzepte
- Unterstützung bei Auskunfts-, Löschungs-, Berichtigungs- und Widerspruchsersuchen
- Applikationsprüfung

Die KI unterstützt insbesondere bei:

- Datenschutzbewertung von Anwendungen
- Plausibilitätsprüfung von Risikobewertungen
- Bewertung technischer und organisatorischer Maßnahmen
- Hinweisen auf fehlende Nachweise
- Prüfung möglicher Drittlandtransfers
- Prüfung möglicher DSFA-Erfordernisse
- Unterstützung bei Datenschutz- und Sicherheitsbewertungen

Qualität der Ergebnisse

Die Qualität der Ergebnisse hängt unmittelbar von der Qualität der dokumentierten Informationen ab.

Je vollständiger die Daten gepflegt werden, desto aussagekräftiger können die Analysen und Empfehlungen der KI ausfallen.

Empfehlung:

Pflegen Sie insbesondere:

- Verarbeitungstätigkeiten
- Dienstleister
- TOM
- DSFA
- Datenschutzvorfälle
- Betroffenenersuchen
- Applikationsprüfungen
- Steuerungsdokumente

möglichst vollständig.

Datenschutz und KI

Die KI verarbeitet ausschließlich die Informationen, die ihr zur Verfügung gestellt werden.

Je nach gewählter KI-Lösung können die Analysen:

- lokal auf dem eigenen System
- innerhalb der eigenen Infrastruktur
- über eine angebundene KI-Umgebung

durchgeführt werden.

Der DatenschutzManager selbst enthält keine verpflichtende Cloud-Anbindung.

Grenzen der KI-Unterstützung

Die KI:

- ersetzt keine rechtliche Beratung durch eine Fachkraft
- ersetzt keinen Datenschutzbeauftragten
- ersetzt keine Risikoentscheidung
- ersetzt keine Managemententscheidung
- ersetzt keine fachliche Prüfung

Alle Ergebnisse sind als Empfehlungen und Prüfhinweise zu verstehen.

Best Practice

Bewährte Vorgehensweise:

- Sachverhalt dokumentieren
- KI-Analyse durchführen
- Empfehlungen prüfen
- Fachliche Bewertung durchführen
- Entscheidung dokumentieren

Die KI sollte als Werkzeug zur Unterstützung, Qualitätssteigerung und Effizienzverbesserung verstanden werden.

Kapitel 20 – Datensicherung, Wiederherstellung und Notfallvorsorge

Warum Datensicherungen wichtig sind

Der DatenschutzManager enthält zentrale Informationen des Datenschutzmanagementsystems.

Dazu gehören unter anderem:

- Verarbeitungstätigkeiten
- Dienstleister
- TOM
- Datenschutzfolgenabschätzungen
- Auditberichte
- Datenschutzvorfälle
- Betroffenenersuchen
- Steuerungsdokumente
- Nachweise
- Berichte

Ein Verlust dieser Informationen kann erhebliche organisatorische und rechtliche Folgen haben.

Regelmäßige Datensicherungen sind daher ein wesentlicher Bestandteil eines funktionierenden Datenschutz- und Informationssicherheitskonzepts.

Was wird gesichert?

Eine Sicherung umfasst:

Datenbank

Alle im DatenschutzManager gespeicherten Informationen.

Beispiele:

- Stammdaten
- Verknüpfungen
- Bewertungen
- Berichte

Dokumente

Alle hinterlegten Dokumente und Nachweise.

Beispiele:

- Richtlinien
- AVV
- Auditberichte
- Schulungsnachweise
- DSFA-Dokumente

Backup erstellen

Öffnen Sie:

```
Einstellungen

→ Backup
```

und wählen Sie:

```
Backup erstellen
```

Anschließend kann die gewünschte Sicherungsart gewählt werden.

Verschlüsselte Backups

Empfohlen wird die Nutzung verschlüsselter Backups.

Vorteile:

- Schutz bei Verlust von Datenträgern
- Schutz bei Diebstahl
- Schutz bei unbefugtem Zugriff

Für verschlüsselte Backups wird ein separates Backup-Kennwort verwendet.

Backup-Kennwort

Wichtige Hinweise:

- Das Backup-Kennwort sollte sicher dokumentiert werden.
- Das Backup-Kennwort sollte nicht mit dem App-Kennwort identisch sein.

Ohne Backup-Kennwort kann ein verschlüsseltes Backup nicht wiederhergestellt werden.

Wiederherstellung

Öffnen Sie:

```
Einstellungen

→ Backup

→ Backup wiederherstellen
```

Anschließend wählen Sie die gewünschte Sicherungsdatei aus.

Bei verschlüsselten Backups erfolgt zusätzlich die Eingabe des Backup-Kennworts.

Nach der Wiederherstellung

Nach erfolgreicher Wiederherstellung sollten Sie:

- Die Anwendung neu starten.
- Eventuell Kennwort bestätigen.
- Gegenfalls Anwendung neu starten.
- Die Mandanten prüfen.
- Stichprobenartig Daten kontrollieren.
- Dokumente öffnen und testen.

Notfallvorsorge

Der DatenschutzManager sollte Bestandteil des allgemeinen Notfallkonzepts sein.

Empfehlung:

- Mindestens folgende Informationen dokumentieren:
- Speicherort der Backups
- Verantwortliche Personen
- Backup-Intervall
- Wiederherstellungsprozess

Empfohlene Backup-Strategie

Täglich

Bei intensiver Nutzung.

Wöchentlich

Für kleinere Organisationen.

Vor größeren Änderungen

Beispiele:

- Import von Daten
- Migrationen
- Software-Updates
- umfangreiche Dokumentenimporte

Aufbewahrung von Backups

Empfehlung:

Mindestens drei Generationen aufbewahren.

Beispiel:

```
Backup aktuell

Backup Vorwoche

Backup Vormonat
```

Dadurch können auch ältere Datenstände wiederhergestellt werden.

Getrennte Speicherung

Backups sollten nicht ausschließlich auf demselben Gerät gespeichert werden.

Empfehlung:

- externe Datenträger
- NAS-Systeme
- verschlüsselte Archivspeicher

Wiederherstellung testen

Eine Datensicherung ist nur dann wertvoll, wenn sie wiederhergestellt werden kann.

Empfehlung:

Mindestens einmal pro Jahr eine Testwiederherstellung durchführen.

Best Practice

Bewährte Vorgehensweise:

- Regelmäßig sichern
- Backups verschlüsseln
- Backup-Kennwort dokumentieren
- Mehrere Generationen aufbewahren
- Wiederherstellung regelmäßig testen

Dadurch wird sichergestellt, dass das Datenschutzmanagementsystem auch nach technischen Störungen oder Hardwareausfällen vollständig wiederhergestellt werden kann.

Kapitel 21 – Kataloge

Zweck der Kataloge

Die Kataloge bilden die zentrale Stammdatenbasis des DatenschutzManagers.

Viele Module greifen auf diese Informationen zurück.

Dazu gehören insbesondere:

- Verarbeitungstätigkeiten
- Betroffenenersuchen
- Datenschutzfolgenabschätzungen
- Berichte
- Auswertungen

Warum sind Kataloge wichtig?

Kataloge verhindern:

- unterschiedliche Schreibweisen
- doppelte Einträge
- fehlerhafte Auswertungen
- Inkonsistenzen

Beispiel:

Statt mehrfach:

```
Mitarbeiter

Beschäftigte

Angestellte

Personal
```

anzulegen, wird ein einheitlicher Eintrag verwendet.

Empfohlene Reihenfolge

Nach der Anlage eines Mandanten sollten zunächst die Kataloge gepflegt werden.

Empfohlene Reihenfolge:

- Betroffenengruppen
- Datenkategorien
- Risikoeinstufungen

- Aufbewahrungsfristen

Erst danach sollten Verarbeitungstätigkeiten angelegt werden.

Betroffenengruppen

Betroffenengruppen beschreiben die Personen, deren Daten verarbeitet werden.

Typische Beispiele:

- Beschäftigte
- Bewerber
- Kunden
- Lieferanten
- Besucher
- Interessenten
- Mitglieder
- Patienten

Die Betroffenengruppen werden später den Verarbeitungstätigkeiten zugeordnet.

Datenkategorien

Datenkategorien beschreiben die Art der verarbeiteten Daten.

Typische Beispiele:

- Stammdaten
- Kontaktdaten
- Vertragsdaten
- Kommunikationsdaten
- Finanzdaten
- Gesundheitsdaten
- Bewerbungsdaten

Die Datenkategorien werden später den Verarbeitungstätigkeiten zugeordnet.

Risikoeinstufungen

Risikoeinstufungen dienen der Bewertung datenschutzrechtlicher Risiken.

Typische Einstufungen:

Niedrig

Geringes Risiko für betroffene Personen.

Mittel

Normale Verarbeitung personenbezogener Daten.

Hoch

Erhöhte Risiken oder sensible Daten.

Die Einstufungen können individuell angepasst werden.

Aufbewahrungsfristen

Aufbewahrungsfristen werden zentral gepflegt und später in Verarbeitungstätigkeiten verwendet.

Beispiele:

6 Jahre

10 Jahre

3 Monate

2 Jahre

Dadurch werden Speicherfristen einheitlich dokumentiert.

Änderungen an Katalogen

Änderungen an Katalogen wirken sich auf die gesamte Anwendung aus.

Empfehlung:

Kataloge möglichst sorgfältig pflegen und regelmäßig überprüfen.

Häufige Ursache leerer Auswahllisten

Wenn in einer Verarbeitungstätigkeit keine Auswahlmöglichkeiten erscheinen, liegt dies häufig daran, dass die entsprechenden Katalogeinträge noch nicht angelegt wurden.

Beispiel:

Keine Betroffenengruppen vorhanden → keine Auswahl in Verarbeitungstätigkeiten.

Keine Datenkategorien vorhanden → keine Auswahl in Verarbeitungstätigkeiten.

Best Practice

Empfohlene Vorgehensweise:

- Mandant anlegen
- Kataloge pflegen
- Dienstleister und TOM erfassen
- Verarbeitungstätigkeiten anlegen
- Weitere Module verwenden

Dadurch lassen sich die meisten Rückfragen und Konfigurationsprobleme vermeiden.

Kapitel 22 – Privacy Information Management System (PIMS) und ISO 27701

Was ist ein PIMS?

PIMS steht für:

```
Privacy Information Management System
```

Ein PIMS erweitert ein Informationssicherheitsmanagementsystem (ISMS) um Datenschutzanforderungen.

Die internationale Norm hierfür ist:

```
ISO/IEC 27701
```

Ziel eines PIMS

Ein PIMS unterstützt Organisationen dabei:

- Datenschutz systematisch umzusetzen
- Verantwortlichkeiten festzulegen
- Risiken zu bewerten
- Nachweise zu dokumentieren
- kontinuierliche Verbesserungen umzusetzen

Zusammenhang mit der DSGVO

Die DSGVO beschreibt gesetzliche Anforderungen.

Ein PIMS beschreibt die organisatorische Umsetzung dieser Anforderungen.

Vereinfacht:

```
DSGVO = Was muss getan werden?

PIMS  = Wie wird es dauerhaft umgesetzt?
```

Rolle des DatenschutzManagers

Der DatenschutzManager unterstützt den Aufbau eines PIMS durch:

- Verarbeitungstätigkeiten
- Dienstleisterverwaltung
- TOM

- Audits
- Maßnahmen
- PIMS-Kontrollen
- Managementbewertungen
- Berichte

PIMS-Kontrollen

PIMS-Kontrollen dienen der Bewertung einzelner Datenschutzanforderungen.

Beispiele:

- Informationspflichten dokumentiert
- Verfahren für Betroffenenrechte vorhanden
- Datenschutzvorfälle dokumentiert
- Schulungen durchgeführt
- Dienstleister überprüft

Reifegradmodell

Der DatenschutzManager unterstützt die Bewertung von Kontrollen über Reifegrade.

Typische Bewertung:

0 – Nicht vorhanden

Keine Umsetzung.

1 – Geplant

Umsetzung vorbereitet.

2 – Teilweise umgesetzt

Einzelne Bestandteile vorhanden.

3 – Weitgehend umgesetzt

Kontrolle funktioniert bereits.

4 – Vollständig umgesetzt

Anforderung vollständig erfüllt.

5 – Optimiert

Regelmäßige Verbesserung und Überprüfung.

Verantwortlicher und Auftragsverarbeiter

Die ISO 27701 unterscheidet zwischen:

Verantwortlicher

Entscheidet über Zweck und Mittel der Verarbeitung.

Beispiele:

- Unternehmen
- Behörden
- Vereine

Auftragsverarbeiter

Verarbeitet Daten im Auftrag.

Beispiele:

- Hostinganbieter
- Cloud-Dienstleister
- Lohnabrechnungsanbieter

Diese Rollen können im DatenschutzManager dokumentiert werden.

Managementbewertung

Ein wichtiger Bestandteil eines PIMS ist die regelmäßige Managementbewertung.

Dabei werden unter anderem bewertet:

- Auditergebnisse
- Datenschutzvorfälle
- Maßnahmen
- Risiken
- PIMS-Kontrollen
- Reifegradentwicklungen

Kontinuierliche Verbesserung

Ein PIMS ist kein einmaliges Projekt.

Es lebt von:

- regelmäßigen Audits
- Maßnahmen
- Schulungen
- Managementbewertungen
- Verbesserungen

Der DatenschutzManager unterstützt diesen kontinuierlichen Verbesserungsprozess.

Zusammenhang mit Audits

Ein PIMS erleichtert:

- interne Audits
- externe Audits
- Kundenprüfungen
- Zertifizierungen

Die dokumentierten Nachweise können direkt als Auditgrundlage verwendet werden.

Best Practice

Empfohlene Vorgehensweise:

- Verarbeitungstätigkeiten dokumentieren
- Dienstleister erfassen
- TOM pflegen
- PIMS-Kontrollen bewerten
- Audits durchführen
- Maßnahmen umsetzen
- Managementbewertungen durchführen

Dadurch entsteht ein nachhaltiges Datenschutzmanagementsystem nach den Grundsätzen der ISO 27701.

Kapitel 22 Unterstützung bei der Einführung einer KI-Lösung

Der DatenschutzManager kann in Verbindung mit einer lokalen oder unternehmensintern betriebenen KI-Lösung einen erheblichen Mehrwert schaffen.

Wissensbasis und RAG-Unterstützung

Der DatenschutzManager kann mit einer KI-gestützten Wissensbasis (Retrieval Augmented Generation – RAG) kombiniert werden.

Hierbei werden Anfragen nicht ausschließlich durch ein Sprachmodell beantwortet, sondern zusätzlich mit dokumentierten Fachinformationen abgeglichen.

Die von Digitales Erbe Fimberger eingesetzte Lösung nutzt hierzu eine speziell aufgebaute Wissensbasis mit datenschutzrechtlichen und regulatorischen Quellen.

Beispiele:

- Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- EU AI Act
- Bürgerliches Gesetzbuch (BGB)
- Entscheidungen des Europäischen Gerichtshofs (EuGH)
- Entscheidungen deutscher Gerichte
- weitere datenschutzrelevante Fachquellen

Dadurch können Auswertungen und Analysen auf Grundlage der hinterlegten Wissensbasis erfolgen.

Die KI unterstützt insbesondere bei:

- Rechercheaufgaben
- Analyse von Datenschutzdokumentationen
- Vorbereitung von Bewertungen
- Zusammenfassungen umfangreicher Dokumente
- Unterstützung bei Audits
- Unterstützung bei Managementbewertungen

Die verwendete Wissensbasis kann regelmäßig aktualisiert und erweitert werden.

Die KI dient als Unterstützungssystem und ersetzt keine rechtliche Beratung oder fachliche Bewertung durch Datenschutzbeauftragte, Auditoren oder Rechtsanwälte.

Die technischen Schnittstellen und die grundlegende Architektur für KI-gestützte Auswertungen sind bereits Bestandteil der Anwendung.

Insbesondere bei großen Datenbeständen können KI-Systeme dabei unterstützen:

- Verarbeitungstätigkeiten zu analysieren
- Audits auszuwerten
- Datenschutzvorfälle zu bewerten
- Maßnahmen zu priorisieren
- Nachweise und Dokumentationen zusammenzufassen
- Managementberichte vorzubereiten
- Zusammenhänge zwischen Datenschutzdokumentationen zu erkennen

Je vollständiger die im DatenschutzManager gepflegten Informationen sind, desto wertvoller können die durch die KI erzeugten Ergebnisse werden.

Digitales Erbe Fimberger unterstützt Unternehmen bei der Planung, Installation und Inbetriebnahme einer geeigneten KI-Umgebung.

Unsere Leistungen umfassen insbesondere:

- Beratung zur Auswahl geeigneter KI-Lösungen
- Installation und Konfiguration
- Anbindung an bestehende Datenschutzdokumentationen
- Unterstützung bei der Einführung
- Schulung und Begleitung der Anwender

Abhängig von Datenbestand und Anwendungsfall können die gewonnenen Erkenntnisse und Auswertungen einen erheblichen Mehrwert für Datenschutzbeauftragte, Auditoren und Management schaffen.

Für weitere Informationen wenden Sie sich bitte an:

datenschutzmanager@digitaleserbe.net

www.digitaleserbe.net/datenschutzmanager

Die Software wurde von Apple notarisiert und durchlief deren Prüfung.