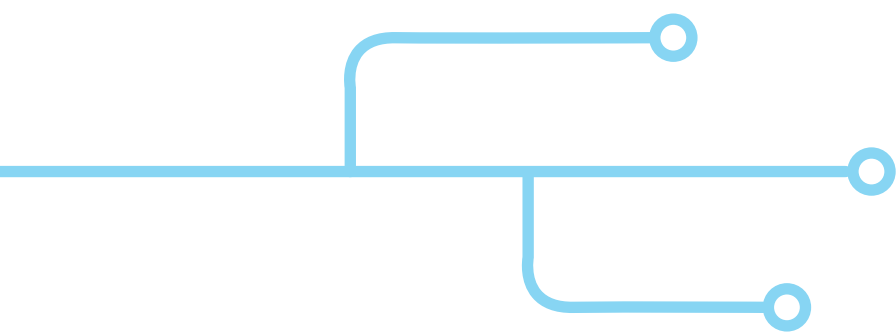




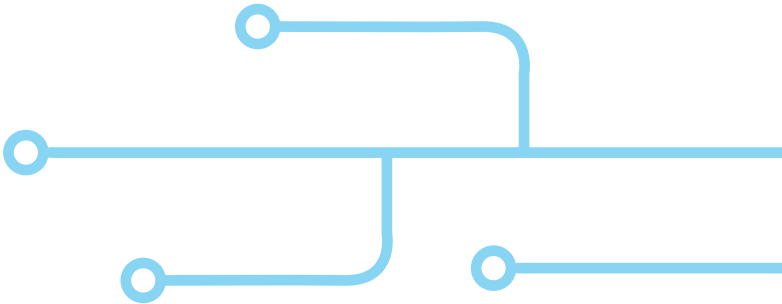
In 10 Schritten ein DSMS aufbauen

Inhalt

1. Organisation abbilden	6
2. Verarbeitungstätigkeiten erfassen	8
3. Dienstleister und Lieferanten managen	10
4. Informationspflichten erfüllen	12
5. Maßnahmen (TOM) dokumentieren	13
6. Betroffenenrechte erfüllen	14
7. Datenschutzverletzungen erkennen	17
8. Interne Richtlinien veröffentlichen	18
9. Mitarbeitende schulen und sensibilisieren	19
10. Managementsystem bewerten und verbessern	20



„Entdecken Sie, wie Sie mit moderner Software Schritt für Schritt ein Datenschutzmanagementsystem aufbauen.“



In 10 Schritten ein DSMS aufbauen

Unsere Softwarelösung unterstützt Sie dabei, datenschutzrechtliche Anforderungen systematisch zu erfüllen, Risiken zu minimieren und Ihrer Rechenschaftspflicht zuverlässig nachzukommen. In diesem Leitfaden zeigen wir in 10 praxisorientierten Schritten, wie Sie mit unserer Software ein Datenschutzmanagementsystem (DSMS) aufbauen und laufend weiterentwickeln.

Was ist ein Datenschutzmanagementsystem?

Ein Datenschutzmanagementsystem ist der strukturierte organisatorische Rahmen, mit dem eine Organisation den Schutz personenbezogener Daten plant, umsetzt, überwacht und fortlaufend verbessert. Es übersetzt die gesetzlichen Anforderungen – insbesondere der DSGVO – in gelebte Prozesse, Verantwortlichkeiten und klare Nachweisketten. Außerdem unterstützt es dabei, Datenschutzrisiken zu erkennen und zu minimieren.

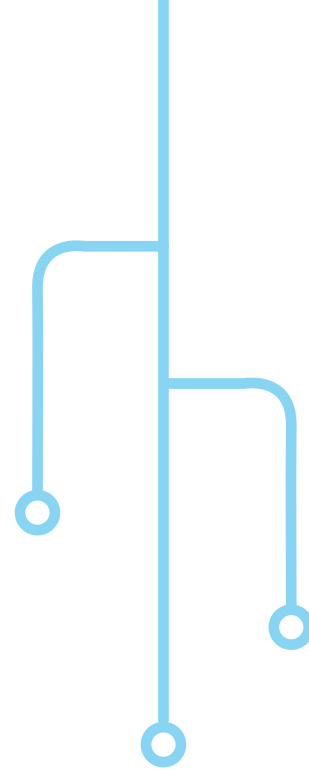
Gleichzeitig wird die Organisation in die Lage versetzt, nachvollziehbar belegen zu können, dass die datenschutzrechtlichen Vorschriften eingehalten werden – sei es gegenüber Kundinnen und Kunden, betroffenen Personen oder Behörden.

Im Folgenden erfahren Sie, wie Sie mit unserer Compliance-Software den Datenschutz in Ihrer Organisation effizient und nachvollziehbar steuern.

Hinweis zur Reihenfolge der Schritte: Dieser Leitfaden bietet Ihnen eine erste Orientierung beim Aufbau eines Datenschutzmanagementsystems. Die Bearbeitung der einzelnen Schritte muss nicht zwingend linear erfolgen – je nach Struktur und Reifegrad Ihrer Organisation können Sie die Module der Software flexibel nutzen und insbesondere auch in einer anderen Reihenfolge bearbeiten. Außerdem können Datensätze aus verschiedenen Modulen an vielen Stellen miteinander verknüpft werden.



„Die Software unterstützt Sie dabei, sowohl Ihren Dokumentationspflichten nachzukommen als auch funktionierende Prozesse zu implementieren.“



1. Organisation abbilden

Zu Beginn legen Sie fest, welche Organisation und welche organisatorischen Einheiten Ihr Datenschutzmanagementsystem abdecken soll. Nutzen Sie zum Beispiel ein bestehendes Organigramm als Grundlage, um Ihre Fachabteilungen anzulegen.

Umsetzung mit dem Modul „Organisation“

- Hinterlegen Sie Stammdaten, Kontaktdaten Ihrer/Ihres Datenschutzbeauftragten, die für Sie zuständige Aufsichtsbehörde sowie Ihr Corporate Design für Berichte.
- Legen Sie Benutzer an, die Sie beim Aufbau und der Pflege Ihres Managementsystems unterstützen.

Umsetzung mit dem Modul „Beschäftigte“

- Legen Sie die Abteilungen an, die in Ihrer Organisation personenbezogene Daten verarbeiten (z. B. HR, Vertrieb, IT, Finanzen, Einkauf, Produktion, Kundenservice).
- Ergänzen Sie optional eine kurze Beschreibung pro Abteilung, um spätere Zuordnungen zu Verarbeitungstätigkeiten, Prozessen oder Systemen zu erleichtern.
- Pflegen Sie Beschäftigtendaten inkl. Abteilungszuordnung per manueller Importfunktion oder binden Sie sie automatisiert über eine Schnittstelle ein.



2. Verarbeitungstätigkeiten erfassen

Das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO ist das Herzstück Ihres DSMS. Es dokumentiert, welche personenbezogenen Daten verarbeitet werden – durch wen, auf welcher rechtlichen Grundlage, zu welchem Zweck und mit welchen Schutzmaßnahmen.

Praxistipp: Beginnen Sie mit den für Ihr Unternehmen relevantesten Prozesse wie Kundenverwaltung, Lohnabrechnung oder Kommunikationswege. Wichtig ist der Fokus auf den Zweck, nicht auf das eingesetzte System.



Umsetzung mit dem Modul „Verarbeitungstätigkeiten“

- Legen Sie neue Verarbeitungen an oder nutzen Sie systemseitige Vorlagen zur Erstellung Ihres Verzeichnisses.
- Automatische Prüfmechanismen zeigen an, wenn Pflichtangaben fehlen.
- Führen Sie eine geführte Erforderlichkeitsprüfung durch, bei der Sie Risiken identifizieren und beurteilen, ob eine Datenschutzfolgenabschätzung erforderlich ist.
- Für Auftragsverarbeiter nach Art. 28 DSGVO: Wählen Sie aus, ob Sie die Verarbeitung im Auftrag eines Kunden durchführen. So erstellen Sie gleichzeitig Ihr Verzeichnis für Auftragsverarbeitungen.
- Für Auftragnehmer: Fügen Sie Dienstleister hinzu, die bei der Verarbeitungstätigkeit eine Rolle spielen.



„Einmal angelegt, können Sie an vielen Stellen auf Ihr Verarbeitungsverzeichnis zurückgreifen.“





3. Dienstleister und Lieferanten managen

Sobald personenbezogene Daten von externen Partnern verarbeitet werden, entsteht ein erhöhter Prüf- und Dokumentationsbedarf – insbesondere bei Auftragsverarbeitungen oder Drittlandtransfers. Sie müssen Ihre Dienstleister vor der Beauftragung prüfen und vertraglich verpflichten, um sicherzustellen, dass sie mit den übermittelten Daten datenschutzkonform umgehen.

Umsetzung mit dem Modul „Dienstleister/Lieferanten“

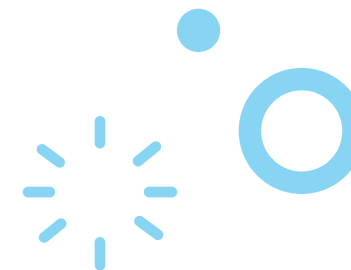
Pflegen Sie alle Ihre Dienstleister auf einer zentralen Oberfläche:

- Hinterlegen Sie Zertifikate und Sicherheitsnachweise von Ihren Lieferanten.
- Fügen Sie verbundene Organisationen (z. B. Muttergesellschaften) oder Unterauftragnehmer Ihrer Lieferanten hinzu und dokumentieren Sie, wie mögliche Drittland-Übermittlungen abgesichert werden.
- Führen Sie eine Dienstleister- bzw. Lieferantenbewertung durch.
- Holen Sie anhand von Online-Fragebögen Informationen über aktuelle Sicherheitsmaßnahmen Ihrer Dienstleister ein.
- Managen Sie den internen Freigabeprozess und halten Sie die verantwortlichen Personen bei Änderungen auf dem Laufenden.

Umsetzung mit dem Modul „Datenschutzverträge“

Schließen Sie Datenschutzverträge wie AV-Verträge und Verträge zur gemeinsamen Verantwortlichkeit digital ab:

- Legen Sie eigene Vertragstemplates an oder nutzen Sie eine Vorlage.
- Als Auftragsverarbeiter verknüpfen Sie Ihre TOM-Übersicht und Verarbeitungstätigkeiten im Auftrag mit Ihren Datenschutzverträgen.



„Prüfen und dokumentieren Sie mit Hilfe von Checklisten die Vollständigkeit von Datenschutzverträgen.“

4. Informationspflichten gemäß Art. 13 und 14 DSGVO erfüllen

Nach Artikel 13 und 14 DSGVO müssen Sie betroffene Personen – zum Beispiel Beschäftigte, Kundinnen und Kunden oder Interessenten, transparent darüber aufklären, inwiefern Ihre Organisation und ggf. weitere Stellen ihre Daten verarbeiten.

Praxistipp: Erstellen Sie modulare Textbausteine für wiederkehrende Anforderungen (Rechtsgrundlagen, Speicherfristen, Kontakt für Auskünfte usw.).



Umsetzung mit den Modulen „Verarbeitungstätigkeiten“ & „DS-Informationen“

- Erstellen Sie Datenschutzhinweise automatisch auf Basis Ihrer erfassten Verarbeitungstätigkeiten.
- Nutzen Sie vorgefertigte Formulierungen als Ausgangspunkt.
- Individualisieren Sie Ihre Informationen nach Bedarf.
- Veröffentlichen Sie Ihre Datenschutzinformationen als PDF, per Direktlink oder Website-Integration.

5. Technische und organisatorische Maßnahmen (TOM) dokumentieren

Die DSGVO schreibt vor, dass personenbezogene Daten risikobasiert zu schützen sind. Das bedeutet, Sie müssen zunächst während einer Risikoanalyse beurteilen, welchen Schutzbedarf die Daten haben, die Sie verarbeiten. Die Schutzziele umfassen die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Je nachdem, wie sensibel die personenbezogenen Daten sind, desto besser müssen sie geschützt werden.

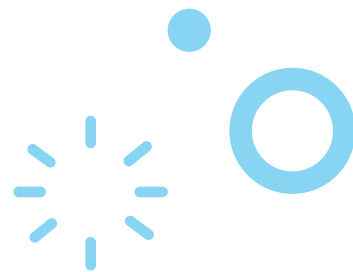
In einem Sicherheitskonzept dokumentieren Sie die implementierten und geplanten Schutzmaßnahmen, die sowohl aus technischen Maßnahmen bestehen (zum Beispiel Firewall, Virenschutz, Backup-Lösung) als auch aus organisatorischen Maßnahmen (zum Beispiel Mitarbeiterrichtlinien, Schulungen).

Die Bewertung von Risiken ist regelmäßig zu wiederholen, insbesondere bei erheblichen Veränderungen der Datenverarbeitung oder einer neuen Bedrohungslage. Um neuen Risiken zu begegnen, müssen Sie im Zuge der Risikobehandlung womöglich weitere Sicherheitsmaßnahmen ergreifen und dokumentieren.



Umsetzung mit dem Modul „TOM“

- Greifen Sie auf eine umfangreiche Maßnahmenbibliothek zurück.
- Dokumentieren Sie spezielle TOM bei einzelnen Standorten oder Verarbeitungstätigkeiten.
- Generieren Sie mit einem Klick Ihre TOM-Übersicht – zum Beispiel für Verträge zur Auftragsverarbeitung oder Lieferantenaudits.
- Greifen Sie bei einer Datenschutzfolgenabschätzung auf Ihre bereits dokumentierten technischen und organisatorischen Maßnahmen zurück.



6. Betroffenenrechte erfüllen

Die Artikel 15 bis 22 DSGVO führen verschiedene Rechte auf, die den Betroffenen zustehen. Sie haben unter anderem ein Recht auf Auskunft, Berichtigung und Löschung ihrer personenbezogenen Daten.

In Ihrer Organisation müssen Sie sicherstellen, dass Betroffenenanfragen strukturiert, fristgerecht und nachvollziehbar bearbeitet werden. Modellieren Sie hierfür entsprechende Prozesse.

Praxistipp: Gehen Sie zweistufig vor, um den Betroffenen zu signalisieren, dass Sie ihre Anfragen ernst nehmen. Das heißt: Verschicken Sie zunächst eine kurze Eingangsbestätigung und danach eine vollständige Antwort.

Achten Sie ebenfalls darauf, auch Dienstleister oder andere externe Partner einzubinden – insbesondere, wenn es um Lös- und Korrekturanfragen geht.

Umsetzung mit dem Modul „Anfragen“

- Richten Sie ein Online-Formular ein, über das Betroffenenanfragen direkt ins System fließen.
- Je nach Betroffenenkategorie unterstützt Sie das System mit den passenden Verarbeitungstätigkeiten – das erleichtert die Datenrecherche.
- Pflegen Sie Anfragen aus anderen Kanälen manuell ein, um Ihre Anfragen lückenlos zu dokumentieren.
- Generieren Sie einen Report Ihrer Dokumentation, um Betroffenen Informationen nach Art. 15 DSGVO strukturiert mitzuteilen.

Umsetzung mit dem Modul „Prozesse“

- Beschreiben und modellieren Sie Ihre Prozesse, um die Schritte für die Beantwortung der Betroffenenanfrage für alle Beteiligten verständlich zu machen (BPMN-Format).
- Legen Sie Zuständigkeiten fest und kommunizieren Sie Ihre Prozesse an alle Beteiligten.



„Denken Sie daran, bei Auskünften auch Informationen nach Art. 13 DSGVO mitzuliefern, wie Sie Betroffenenanfragen verarbeiten und wie lange Sie sie speichern.“

„Ein klarer Prozess verschafft Ihnen Zeit“.

7. Datenschutzverletzungen erkennen & dokumentieren

Eine „Datenpanne“ besteht, wenn die Vertraulichkeit, Integrität oder Verfügbarkeit personenbezogener Daten beeinträchtigt ist – zum Beispiel durch Fehlversand von E-Mails oder in Folge eines Phishing- oder Ransomware-Angriffs.

Wenn ein Risiko für die Betroffenen vorliegt, müssen Sie die Datenschutzverletzung der für Ihre Organisation zuständigen Aufsichtsbehörde melden – binnen 72 Stunden. Entscheidend ist also eine schnelle Risikobewertung. Wenn ein hohes Risiko vorliegt, müssen Sie ebenfalls die betroffenen Personen informieren.

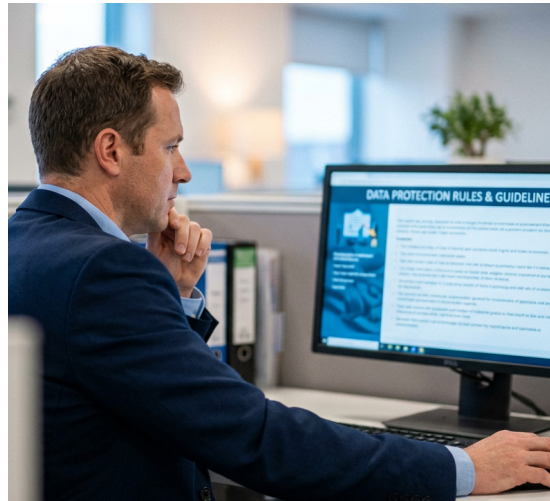
Praxistipp für Auftragsverarbeiter:

Informieren Sie Auftraggeber, deren Daten Sie verarbeiten, unverzüglich über einen Datenschutzvorfall. Nur so können die Verantwortlichen den Vorfall zeitnah bewerten und fristgerecht melden.



Umsetzung mit dem Modul „Datenschutzverletzungen“

- Beschreiben Sie Zeitpunkt der Datenschutzverletzung, Art, Ursache, Umfang und getroffene Sofortmaßnahmen.
- Wählen Sie die betroffenen Verarbeitungstätigkeiten aus, um die betroffenen Datenarten und Personengruppen abzuleiten.
- Dokumentieren Sie Ihre durchgeführte Risikobewertung anhand einer Risikomatrix.
- Behalten Sie die 72-Stunden-Frist im Blick: Die Software unterstützt Sie bei der Einhaltung der Meldefrist an die Aufsichtsbehörde.



8. Interne Richtlinien veröffentlichen

Datenschutz lebt vom Bewusstsein der Mitarbeitenden. Klare Vorgaben, leicht verfügbare Informationen und eine saubere Dokumentation der Kenntnisnahme sind zentrale Komponenten eines belastbaren DSMS. Mit einer zentralen Intranet-Oberfläche können Sie Vorgaben, Kontaktwege und Meldeprozesse sichtbar und aktuell halten.

Umsetzung mit dem Modul „Dokumente“

- Erstellen Sie im integrierten Editor neue Richtlinien oder laden Sie bereits erstellte Dokumente hoch.
- Definieren Sie Rollen, um Verantwortlichkeiten festzulegen.
- Lenken Sie Ihre Dokumente digital, indem Sie Freigabe, Versionierung und Review-Termine steuern.

Umsetzung mit dem Modul „Intranet“

- Veröffentlichen Sie Richtlinien, Leitlinien oder Verhaltensregeln im Intranet
- Verfolgen Sie die Kenntnisnahme digital.
- Stellen Sie ein Online-Formular zur Verfügung, über das Mitarbeitende Datenschutzverletzungen intern melden können.

///
„Die Sichtbarkeit von Dokumenten können Sie über die angelegten Abteilungen steuern.“



9. Mitarbeitende schulen und sensibilisieren

Regelmäßige Datenschutzzschulungen sind die Voraussetzung für gelebtes Datenschutzbewusstsein. Sie sind elementar, um Datenschutzverletzungen vorzubeugen. Indem Sie Ihre Mitarbeitenden involvieren, bekommen Sie außerdem neue Denkanstöße für die Weiterentwicklung Ihres Datenschutzmanagementsystems.

Umsetzung mit dem Modul „Schulungen“

- Erstellen Sie eigene Online-Mitarbeiterschulungen inkl. Abschlusstest oder nutzen Sie sofort nutzbare Datenschutzzschulungen aus unserem Schulungsangebot.
- Stellen Sie Schulungen im „Intranet“ zur Verfügung.
- Nutzen Sie die automatische Einladungs- und Erinnerungsfunktion.
- Verschicken Sie automatisiert die Teilnahmezertifikate.





10. Managementsystem bewerten und verbessern

Ein Datenschutzmanagementsystem aufzubauen ist keine einmalige Maßnahme, sondern mit einem kontinuierlichen Verbesserungsprozess verbunden. Um Ihre Datenschutzorganisation langfristig wirksam und sicher zu gestalten, sollten Sie regelmäßig überprüfen, wie gut die rechtlichen Anforderungen umgesetzt sind. Orientierung bieten standardisierte Anforderungskataloge – zum Beispiel auf Basis des

Standard-Datenschutzmodells (SDM), der VdS 10010-Richtlinie oder der ISO/IEC 27701. Anhand dieser Kataloge können Sie bewerten: Welche Anforderungen sind vollständig erfüllt? Wo bestehen Umsetzungsdefizite? Welche Maßnahmen wurden bereits umgesetzt – und welche sind noch offen? Ziel ist es, Fortschritte messbar zu machen und Verbesserungspotenziale gezielt zu identifizieren.

Umsetzung mit den Modulen „Managementsysteme“, „Maßnahmen“, „Interne Audits“

- Legen Sie eigene Kataloge an oder importieren Sie vorkonfigurierte Kataloge aus unseren Zusatzinhalten.
- Verwalten Sie Maßnahmen sowie verantwortliche Personen und Fristen zur Umsetzung.
- Erstellen Sie Online-Fragebögen (Selbst-Audits) für die Zusammenarbeit mit Kolleginnen und Kollegen oder externen Partnern.
- Führen Sie interne Audits durch und dokumentieren Sie Ihre Ergebnisse in einem ausführlichen Bericht.
- Integrieren Sie weitere Managementsysteme, zum Beispiel für den Aufbau eines Informationssicherheitsmanagementsystems.

Vielen Dank für Ihr Vertrauen!

Sollten Sie Fragen haben oder eine individuelle Beratung wünschen, stehen wir Ihnen jederzeit gerne zur Verfügung.

Kontaktieren Sie uns

LegallInnovate Technologies GmbH
Geschäftsführer: Thomas Niersmann
Adresse: Issumer Tor 45, 47608 Geldern
E-Mail: info@dpms-online.de



Management
System
ISO/IEC
27001:2022

www.tuv.com
ID 9000045316

Noch mehr Infos
finden Sie hier!



