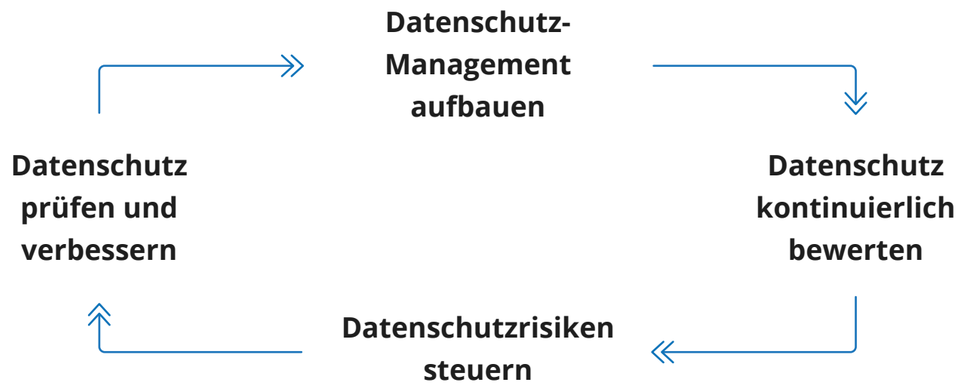
Datenschutz-Management nach der DSGVO

Frank Trautwein,
IT-Jurist, Lead Auditor ISO 27001

Philipp Heindorff,
Rechtsanwalt, DSGVO Auditor

> **Datenschutz-Management ist die Gesamtheit aller Dokumentationen, Prozesse und Maßnahmen im Datenschutz, mit dem Ziel: Datenschutz kontinuierlich zu kontrollieren und zu verbessern.**



Was ist Datenschutz-Management?

Mit der Datenschutz-Grundverordnung (DSGVO) findet am 25. Mai 2018 ein wichtiger Aspekt Einzug in den Datenschutz, der in anderen Bereichen längst üblich ist: die Verankerung eines Compliance-Bereichs in unternehmensweite Prozesse. Im Kern geht es stets darum, ein sehr spezielles Thema, in diesem Fall Datenschutz, in das kollektive Bewusstsein des Unternehmens zu bekommen. Erreicht wird dies nur durch den Anstoß der obersten Leitungsebene, die sich eine „Kultur des Datenschutzes“ zum Ziel setzen sollte. Qualitätsmanagement und Informationssicherheits-Management bieten hier bereits gute Leitfäden und Ausgangsszenarien, etwa im Bereich Risikomanagement.

Was fordert die DSGVO genau?

Die Datenschutz-Grundverordnung (DSGVO) fordert unter dem neuen Stichwort „Rechenschaftspflicht“ in Art. 5 Abs. 2 DSGVO, dass ein Unternehmen selbst nachweisen muss, dass Daten rechtmäßig verarbeitet werden. Es werden somit gänzlich neue Dokumentations- und Nachweispflichten auferlegt, die über die bisherige Datenschutzdokumentation hinausgehen. Es geht darum, analog zur Sicherheitsorganisation der ISO 27001, eine Datenschutzorganisation aufzubauen, die fortlaufend Nachweise über das eigene (rechtskonforme) Handeln generiert. Verantwortlich dafür ist übrigens nicht der Datenschutzbeauftragte, sondern die Leitungsebene.

Welche Schritte müssen unternommen werden?

Im ersten Schritt muss sich die Leitungsebene der eigenen Verantwortung im Rahmen der neuen Anforderungen der DSGVO bewusstwerden. Es sollte eine **Datenschutzleitlinie ausgearbeitet** werden, die den Stellenwert des Datenschutzes beschreibt und was das Unternehmen unternimmt, um die Daten der Mitarbeiter und Kunden zu schützen. Im nächsten Schritt ist zu klären „wer wem wie" zuarbeitet und es müssen **Verantwortliche benannt** werden, allen voran der Datenschutzbeauftragte und je nach Organisationsgröße auch standortbezogene Datenschutzkoordinatoren. Zudem sollte eine **Risikomethodik entwickelt** werden, damit Fachabteilungen überhaupt verstehen können, was ein datenschutzrechtliches Risiko darstellt und welche Daten schützenswert sind. Sobald die Vorarbeit geleistet wurde und z.B. auch **Budget und Ressourcenfragen geklärt** sind, sollte eine Bestandsaufnahme erfolgen. Dies kann entweder durch interne oder externe Stellen erfolgen, indem ein **Datenschutzaudit** der Fachabteilungen durchgeführt wird. Es leitet sich ein Maßnahmen- oder Projektplan ab, aus dem sich konkrete Umsetzungsprojekte und zu erstellende Dokumentationen ergeben. Zugleich sollte eine Festlegung erfolgen, welche **Nachweise** die internen Ansprechpartner nachzuhalten haben. Anhand der initial entwickelten Risikomethodik sollten sodann **turnusmäßige Prüfungen** erfolgen und daraus Risiken sowie deren Behandlung abgeleitet werden. Entscheidend ist, dass ein fortlaufender Austausch zwischen fachlichen Ansprechpartnern, allen voran dem Datenschutzbeauftragten, und der Leitungsebene stattfindet. Das zeichnet das Datenschutz-Management aus, mit dem Ziel **kontinuierlicher Verbesserung**.

- Leitungsebene definiert Datenschutzleitlinien
- Leitungsebene benennt Verantwortliche der DS-Organisation
- Schutzziele und Risiken im Datenschutz sind klar zu definieren
- Datenschutzaudit oder Fit-Gap Analyse durchführen
- Maßnahmenplan entwerfen und Dokumentation erstellen
- DSB kontrolliert die Einhaltung d. DS und schult zusätzlich die MA
- Fachabteilungen generieren Nachweise zur Datenverarbeitung
- Risiken werden an die Leitungsebene kommuniziert und behandelt

Checkliste Datenschutz-Management

Um die Dokumentations- und Rechenschaftspflichten im Datenschutz-Management zu konkretisieren, findet sich nachfolgend eine beispielhafte Checkliste wichtiger Dokumente und Nachweise einer funktionierenden Datenschutzorganisation.

1 Standard- Dokumente

- Datenschutzleitlinie oder Datenschutzhandbuch (zur Beschreibung der Schutzziele im Datenschutz und Verantwortung der Leitungsebene
- Prozessbeschreibungen zu DS-Prozessen (z.B. zu Betroffenenanfragen und Umgang mit DS-Vorfällen)
- Verzeichnis der Verarbeitungstätigkeiten (zur Dokumentation der einschlägigen Anwendungen und Systeme, lokal und in der Cloud)
- Datenschutzfolgen-Abschätzung und Risikokarte (die Risikokarte ist ggf. optional und bietet eine Übersicht aller bisher identifizierten Risiken)
- Verpflichtungen und Auftragsverarbeitungsverträge (z.B. auch als Vorlage für externe Dienstleister, um diese entsprechend zu verpflichten)
- Sicherheitsdokumentation und sonstige Richtlinien (z.B. Informationssicherheits-Richtlinie, BYOD und Home Office RL)

2 Nachweise

- Rollenbeschreibungen und Benennungsurkunden (z.B. als Nachweis der Funktion des Datenschutzbeauftragten oder ISO/ISB)
- Dienstleisterübersicht mit Verweis auf Datenübermittlungen und Vorhandensein von Auftragsverarbeitungsverträgen
- Datenschutzerklärungen und Rundschreiben (z.B. als Nachweis der Information Betroffener und auch interner Mitarbeiter)
- Schulungszertifikate und Teilnehmerlisten (z.B. um nachzuweisen, dass man den Aufklärungspflichten nachgekommen ist)
- Abgeschlossene Datenschutzfolgen-Abschätzungen (z.B. um erfolgte Risikoabwägungen ggü. der Datenschutzaufsicht zu rechtfertigen)
- Screenshots aus Anwendungen und Netwrix Auditor Berichte (z.B. um Double-Opt-In bei Newsletter oder Berechtigungen in AD aufzuzeigen)

Mit Netwrix Auditor können Sie die Einhaltung des strengen EU-DSGVO Datenschutzstandards nachweisen

Netwrix Auditor hilft Unternehmen auf der ganzen Welt die wichtigsten Datenschutz-bestimmungen der EU-DSGVO zu erfüllen und nachzuweisen. Mit Netwrix Auditor erhalten Sie die Sichtbarkeit, die Sie für Ihre Kontrollen, Prozesse und Praktiken benötigen, um sicherstellen zu können, dass sie mit den Anforderungen der Verordnung in Einklang stehen.

Führen Sie regelkonforme Zugriffsberechtigungen ein

Stellen Sie sicher, dass regulierte personenbezogene Daten, über eine strenge Kontrolle der Zugriffsberechtigungen, nicht für unbefugte Personen zugänglich gemacht werden können.

Bleiben Sie über anomales oder offenkundig unerlaubtes Nutzerverhalten informiert

Überwachen Sie das Benutzerverhalten nach Hinweisen auf ein potenziell böswilliges Verhalten, das zu unrechtmäßigen Datenzugriffen oder Datenänderungen führen könnte.

Aktivieren Sie die Kontrolle über strukturierte und unstrukturierte Datenkontakte

Achten Sie auf nicht autorisierte Versuche, vertrauliche Inhalte und Daten zu löschen oder zu modifizieren, um zu garantieren, dass personenbezogene Daten sicher gespeichert sind und nicht außerhalb von ordnungsgemäßen Arbeitsabläufen verarbeitet werden können.

Lassen Sie sich über wichtige Ereignisse informieren, die gegen Datenschutzrichtlinien verstoßen

Richten Sie Benachrichtigungen für kritische Ereignisse ein, damit Sie schnell auf Sicherheitsvorfälle reagieren können. Abonnieren und Prüfen Sie die Ereignisberichte, um frühzeitig Bedrohungsmuster identifizieren zu können.

Vereinfachen Sie die Untersuchungen und ermitteln Sie unkompliziert die spezifischen Auditdaten

Verwenden Sie die interaktive Suche um Nutzerinteraktionen auf mehreren IT-Systemen schnell zu finden und benutzerdefinierte Berichte zu erstellen, um die Effektivität Ihrer Kontrollmechanismen zu veranschaulichen.

Sichern Sie Ihre Prüfprotokolle für mögliche Sanierungen und Ermittlungen über mehrere Jahre

Stellen Sie sicher, dass der Nachweis Ihrer EU-DSGVO-Konformität für Jahre gesichert bleibt und gleichzeitig mit einem zuverlässigen, zweistufigen AuditArchive ™ -Speichersystem (dateibasiert + SQL-Datenbank) leicht zugänglich bleibt.

Über die Autoren

Frank Trautwein,

IT-Jurist, Lead Auditor ISO 27001

Frank Trautwein ist auf Rechtsinformatik spezialisiert und Mitgründer der Firma Fresh Compliance, die sich auf praxisnahen und innovativen Datenschutz konzentriert. Neben Veröffentlichungen in Fachzeitschriften, hält er regelmäßig Webinare und Fachvorträge. Er berät gleichermaßen Startups und Konzerne zu DSGVO, BDSG-neu, IT-SiG und der ePrivacy Verordnung. Als zertifizierter Lead Auditor (ISO 27001) begleitet er zudem den Aufbau von Informationssicherheits- sowie Datenschutz-Managementsystemen und ist GDD-zertifizierter Datenschutzbeauftragter. Er ist davon überzeugt, dass Datenschutz spätestens mit der DSGVO zu einem wichtigen Wettbewerbsfaktor wird, den es von Unternehmen auszunutzen gilt.

Philipp Heindorff,

Rechtsanwalt, DSGVO Auditor

Philipp Heindorff ist zugelassener Rechtsanwalt und spezialisiert auf Datenschutz und IT-Recht. Als Mitgründer der Firma Fresh Compliance berät er dank langjähriger Praxiserfahrung unzählige Unternehmen zu neuen Anforderungen aus den Bereichen Datenschutz und Datensicherheit. Er ist in der der Rolle des externen Datenschutzbeauftragten für Unternehmen der Digitalwirtschaft im Einsatz und hat verschiedene Verfahren der Datenschutzaufsichtsbehörden begleitet. Schwerpunkte liegen in Datenschutz-Risikoanalysen und der Implementierung von Datenschutz-Managementsystemen. Er ist sich sicher, dass es beim Datenschutz in erster Linie auf eine praxisnahe und verständliche Vermittlung ankommt, damit DSGVO & Co. so in der Wirtschaft ankommen, wie vom Gesetzgeber vorgesehen.