Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO

Die Datenschutz-Richtlinie

Grundlagen, Grundstrukturen und typische Regelungsbereiche

Anmerkung von Nicholas Vollmer:
Die GDD hat die römische Nummerierungen der Praxishilfen leider gestoppt.
Auf der GDD-Website wird das hier vorliegende Dokument als Version 2 der alten Praxishilfe VIII genannt.
Allerdings finden sich hier völlig andere Inhalte und es stellt sich die Frage, in welchem Verhältnis die neue und alte Version zueinander stehen.

INHALT

EINLEITUNG

Organisationen - Unternehmen, Vereine oder Behörden - sind im Rahmen der Datenschutz-Grundverordnung (DS-GVO) verpflichtet, jederzeit nachweisen zu können, dass und wie sie die gesetzlichen Datenschutz-Anforderungen umsetzen (Rechenschaftspflicht oder Accountability). In der Praxis stellt sich einerseits die Frage, wie dieser Nachweis zu führen ist. Auf der anderen Seite wird gelebter Datenschutz in einer Organisation nur möglich, wenn den dort tätigen Menschen klar ist, was ihre Aufgaben und Pflichten – ihre Rollen – bei der operativen Umsetzung des Datenschutzes sind. Wofür ist jeder selbst verantwortlich?

Praxis-Tipp:

Klare, verständliche und auf das Wesentliche reduzierte Regelungen tragen dazu bei, Haftungsrisiken für die Organisation zu reduzieren und schaffen gleichzeitig (Handlungs-)Sicherheit für die Beschäftigten.

Für das weitere einheitliche Verständnis der Praxishilfe wird an dieser Stelle eine Unterscheidung zwischen Datenschutz-Management und Datenschutz-Organisation getroffen:

>> Das **Datenschutz-Management** umfasst alle Elemente, die zum Steuern/Führen, Umsetzen, Kontrollieren/Prüfen, Weiterentwickeln im Datenschutz erforderlich sind.

>> Die **Datenschutz-Organisation** umfasst die Gesamtheit aller Maßnahmen (strukturell, prozessual, regelsetzend), die der Umsetzung des Datenschutzes dienen.

In der Praxis hat sich die Erstellung und Einführung von Datenschutz-Richtlinien bewährt, um die Umsetzung des Datenschutzes (die Datenschutz-Organisation) und den kontinuierlichen Verbesserungsprozess zur Gewährleistung der Wirksamkeit (Datenschutz-Management) einer Organisation zu dokumentieren. Während Leitlinien primär die Datenschutz-Ziele einer Organisation in Grundzügen beschreiben, geben Richtlinien den Rahmen zur Umsetzung konkreter Maßnahmen zur Erreichung dieser Ziele vor.

EINLEITUNG (FORTSETZUNG)

Mit Blick auf die Accountability erscheinen daher primär Datenschutz-Richtlinien als das geeignete Mittel, um den Nachweis eines aktiven Datenschutz-Managements innerhalb einer Organisation erbringen zu können. Diesen Datenschutz-Richtlinien kann sinnvoll eine Datenschutz-Leitlinie vorangestellt werden, in der

- die Bedeutung des Datenschutzes unterstrichen wird,
- Ziele definiert werden und
- vor allem die gesamte Organisation auf die Einhaltung sämtlicher interner Vorgaben und Regelungen zum Datenschutz sensibilisiert wird.

Den Autoren ist klar, dass in überschaubaren Strukturen vielleicht eine einzige Datenschutz-Richtlinie ausreicht, um die Datenschutz-Organisation zu dokumentieren und den Nachweis eines Datenschutz-Managements zu erbringen. In vielen Fällen wird es aber unterschiedliche Datenschutz-Richtlinien geben, um komplexeren Strukturen und Anforderungen gerecht zu werden. Im Weiteren wird daher von Datenschutz-Richtlinien die Rede sein.

Die vorliegende Praxishilfe wurde im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt durch:

RA Levent Ferik, LL.M. (Datenschutzbeauftragter, HIL Heeresinstandsetzungslogistik GmbH)
Stefan Hardelt (Fachberatung Datenschutz)
Dirk Niedernhöfer (dn Datenschutz UG)
Uwe Bargmann (Berater Datenschutzmanagement)
Thomas Müthlein (DMC - Datenschutz Management & Consulting, GDD-Vorstand)

Die GDD-Geschäftsstelle dankt den Genannten herzlich für ihr Engagement!

1. Zweck und Motivation der Praxishilfe

Diese Praxishilfe leistet Überzeugungsarbeit für das Erstellen, die regelmäßige Anpassung und Aktualisierung der Datenschutz-Organisation mittels Leit- und Richtlinien zum Datenschutz (Datenschutz-Leitlinie/Datenschutz-Richtlinien).

Sie soll dabei unterstützen, einen verbindlichen Standard für die Erstellung von Datenschutz-Richtlinien innerhalb der Organisation zu etablieren. Die Praxishilfe soll Hilfestellung für die grundsätzlichen Zuständigkeiten im Erstellungs- und Freigabeprozess geben. Sie soll die Grundlagen vermitteln, um individuelle Datenschutz-Richtlinien für ein Unternehmen, einen Verein oder eine Behörde umzusetzen. Sie zeigt typische Regelungsbereiche auf und liefert Erfahrungswerte aus der Praxis.

Die Praxishilfe soll:

1. die Erstellung von Datenschutz-Leit- und -Richtlinien vereinfachen;
2. die Interessen aller Beteiligten im Entstehungsprozess von Datenschutz-Leit- und -Richtlinien angemessen berücksichtigen;
3. die Verständlichkeit, Eindeutigkeit und Nachvollziehbarkeit von Festlegungen in einer Richtlinie erhöhen.

Diese Praxishilfe liefert eine Begriffsdefinition, formuliert anschließend Anforderungen an Inhalt und Form von Datenschutz-Richtlinien und beschreibt Zuständigkeiten für Erstellungs-, Prüfungs- und Freigabeprozesse.

Sie kann keine konkreten Beispiele für Datenschutz-Richtlinien liefern. Sie gibt vielmehr Hilfe zur Selbsthilfe und ist eine Anleitung zur Erstellung individueller Datenschutz-Richtlinien.

2. Begriffsklärung und Grundlagen

2.1 Definition und Abgrenzung von Datenschutz-Richtlinien und Datenschutz-Leitlinien

Im Gegensatz zur Datenschutz-Richtlinie sind Datenschutz-Leitlinien Grundsatzdokumente der Leitung, die Aussagen zum Stellenwert, den verbindlichen Prinzipien und dem anzustrebenden Niveau des Datenschutzes innerhalb einer Organisation treffen. Eine Leitlinie enthält in der Regel daher keine konkreten operativen Beschreibungen und Umsetzungsmaßnahmen. Um es plastisch auszudrücken: Sie ist mehr als Gerüst oder Leitpfosten zu verstehen, an dem sich die Mitarbeiter der Organisation orientieren sollen und nicht als Korsett zu verstehen.

Datenschutz-Richtlinien sind schriftlich dokumentierte, je nach Organisationsstruktur des Verantwortlichen bereichsübergreifend geltende, organisatorische Regelungen. Sie werden von der Leitung in Kraft gesetzt und gelten grundsätzlich für alle Mitglieder der Organisation beziehungsweise die Beschäftigten. Sie liefern sachlich richtige, eindeutig nachvollziehbare Informationen und klare Vorgaben. In Behörden und Dienststellen werden Richtlinien häufig Dienstanweisungen genannt.

Die Datenschutz-Richtlinien einer Organisation sind zu behandeln wie - eventuell - bereits zu anderen Sachverhalten existierende Richtlinien: sie reihen sich nahtlos ein. Bei der Erstellung unterliegen sie - soweit vorhanden - den gleichen Vorgaben wie andere Richtlinien der Organisation.

Eine Grafik zur Normenpyramide finden Sie nachstehend (**auf Seite 6**).

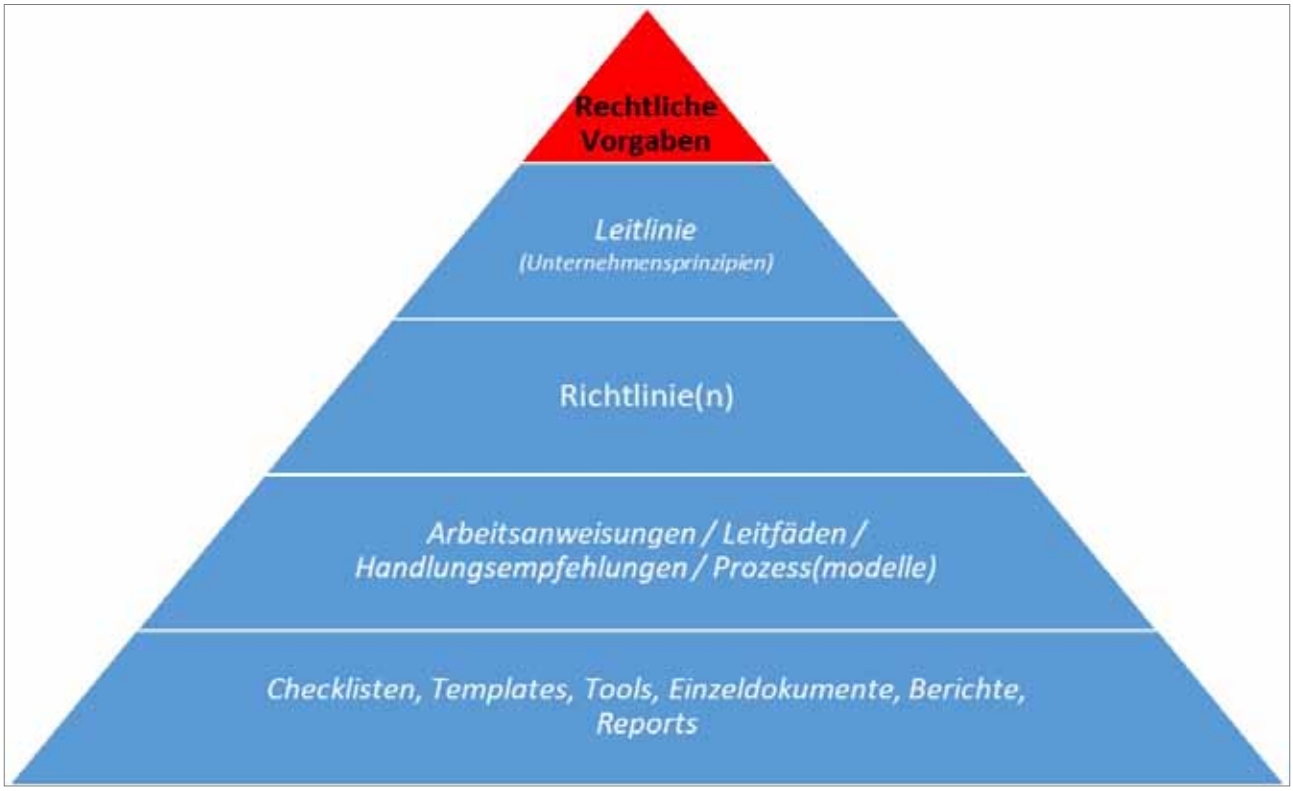

Abb. Normenpyramide

Während eine Leitlinie übergeordnete Zielsetzungen beschreibt, die ein Unternehmen, eine Behörde oder ein Verein im Datenschutz verfolgen, werden Datenschutz-Richtlinien konkret regelsetzend. Richtlinien geben einen konkreten Rahmen vor, der wiederum, falls erforderlich, in Arbeitsanweisungen oder Prozessbeschreibungen detailliert werden kann.

2.2 Rechtliche Einordnung von Datenschutz-Richtlinien

Datenschutz-Richtlinien stellen nach Innen eine allgemeinverbindliche betriebliche Anweisung dar und sollten grundsätzlich für alle Beschäftigten der Organisation gelten. Richtlinien konkretisieren das Recht der Leitung, die Leistungspflicht des Beschäftigten nach Zeit, Inhalt und Ort sowie dessen Beschäftigtenpflichten näher zu bestimmen und bringen konkret die spezifischen Anforderungen der Organisation mit den sich aus dem Datenschutzrecht ergebenden Anforderungen in Einklang.

Nach Außen muss im Fall von Auftragsverarbeitungen geprüft werden, ob der Vertrag zur Auftragsverarbeitung den Vorgaben der Datenschutz-Richtlinien entspricht. Bei in gemeinsamer Verantwortung betriebenen Verarbeitungen müssen die Verantwortlichen im Vorfeld prüfen, wie die jeweiligen Regelungen aus den Datenschutz-Richtlinien harmonieren und Anwendung in der Verarbeitung finden.

Datenschutz-Richtlinien treten mit Unterzeichnung durch die Leitung bzw. nach geltender Unterschriftenregelung in Kraft und sind ab dem Zeitpunkt ihrer Inkraftsetzung durch sämtliche Beschäftigten einzuhalten. Wichtig ist, dass die Datenschutz-Richtlinien wirksam kommuniziert und die Inhalte durch anschließende Schulungen weiter vermittelt werden. Für die notwendige Schlagkraft und Verbindlichkeit der Richtlinien sollte klargestellt werden, dass Zuwiderhandlungen einen Verstoß gegen arbeitsrechtliche Regelungen darstellen und entsprechend sanktioniert werden können. Weiterhin sollten Richtlinien regeln, wie die regelmäßige Überprüfung und Außerkraftsetzung erfolgen soll. Stringent dürfte es sein, an die Außerkraftsetzung dieselben Formvorschriften zu stellen, wie an die Inkraftsetzung.

In Entsprechung an die Normenpyramide (**siehe Seite 6**) sollte festgehalten werden, dass in Richtlinien getroffene Regelungen, die gegen geltendes Recht verstoßen, als nichtig zu bewerten sind. Um sicherzustellen, dass Richtlinien bereichsübergreifende und grundlegende Rahmenbedingungen schaffen, sollten diese bereichs- oder abteilungsinternen Anordnungen sowie Handlungs- und Arbeitsanweisungen, Prozessdarstellungen stets übergeordnet behandelt werden. Dabei sollte ein Augenmerk daraufgelegt werden, dass diese weiterführenden Dokumente im Einklang mit den Regelungen einer jeweils geltenden Richtlinie stehen und widerspruchsfrei bleiben.

2.3 Zweck einer Datenschutz-Richtlinie

Datenschutz-Richtlinien vereinheitlichen und dokumentieren die wichtigsten Prozesse im Rahmen des Datenschutz-Managements. Sie stellen so Rechtskonformität her. Richtlinien sollen den zu regelnden Gegenstand so weit wie möglich konkretisieren.

Datenschutz-Richtlinien:

- >> beschreiben und regeln die Datenschutz-Anforderungen und -Verantwortlichkeiten innerhalb einer Organisation;
- >> bilden den Rahmen, an dem betriebsinterne Datenschutzprozesse und Arbeitsabläufe auszurichten sind;
- >> geben klare Vorgaben zur Umsetzung;
- >> regeln die Anforderungen an Beschäftigte oder Dritte (Auftragsverarbeiter/Joint Controller), so dass diese den unternehmensspezifischen Datenschutzanforderungen entsprechen;
- >> können jederzeit zu Rate gezogen werden.

Gegenüber Dritten stärken Datenschutz-Richtlinien die Nachweisbarkeit der Umsetzung gesetzlicher Anforderungen.

2.4 Initiierung von Datenschutz-Richtlinien

Der Ursprung jeder Datenschutz-Richtlinie wird das Erkennen eines Regelungsdefizits sein. Ein Regelungsdefizit kann überall in der Organisation erkannt werden: aus einer Fachabteilung heraus, durch die Leitung der Organisation selbst, soweit vorhanden durch Datenschutz-Manager (DSMgr), Datenschutz-Koordinatoren (DSK), einem Datenschutzteam oder den Datenschutzbeauftragten (DSB), die die Gesamtheit der Verarbeitungstätigkeiten und die Schnittmenge der Prozesse der Organisation zum Datenschutz am besten überblicken dürften. Soweit der Bedarf erkannt ist, sollte die Entstehung einer erforderlichen Datenschutz-Richtlinie durch die Leitung initiiert werden. Sie kann dies aber auch auf ggf. vorhandene Datenschutz-Manager bzw. das Datenschutzteam delegieren[1].

Um die Anzahl der regelungsrelevanten Sachverhalte zum Datenschutz auf ein sinnvolles Maß zu begrenzen, kann es empfehlenswert sein, (harte) Kriterien für eine Erheblichkeitsschwelle zu definieren. Darin kann festgelegt werden, welche Kriterien eine Thematik erfüllen muss, damit die Regelungsbedürftigkeit im Rahmen einer Richtlinie bejaht werden kann. Diese Kriterien könnten bspw. sein:

- >> Auswirkungen des zu regelnden Sachverhalts auf das gesamte Unternehmen bzw. die gesamte Unternehmensgruppe;
- >> Die gesetzlichen Anforderungen sind zu abstrakt und komplex, um diese in der Organisation unmittelbar umzusetzen;
- >> Es bedarf einer strategischen Ausrichtung und Aktivierung durch die Organisationsleitung;
- >> Beschäftigte sind im Hinblick auf die zu beachtenden (gesetzlichen) Anforderungen überfordert;
- >> Es gibt keine klaren Abgrenzungen im Hinblick auf die Zuständigkeiten für den Umgang mit dem zu regelnden Sachverhalt;

1 S. hierzu auch GDD-Praxishilfe DS-GVO - Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung, Version 2.0, Stand August 2021.

>> Mangelnde Regelung könnte bei rechtlichen Auseinandersetzungen und insbes. bei einer aufsichtsbehördlichen Prüfung als strukturelles Organisationsverschulden (Anweisungsverschulden[2]) und nicht als individueller „Fehler" eines/einer Beschäftigten gewertet werden und zu erheblichen materiellen und ggf. auch immateriellen Risiken für die Organisation führen;
>> Aktivierung und aktive Nutzung der Richtlinie hat positive Auswirkungen auf die Nachweisbarkeit der organisationsspezifischen Umsetzung einer gesetzlichen Anforderung, die auf anderem Wege schwierig zu erzielen ist.

Daneben sind auch Verweise auf mögliche andere Arten von Dokumenten notwendig, sofern (weitergehende) Regelungen dort getroffen werden. Nutzer sollten Hinweise erhalten, nach welchen Kriterien Sachverhalte im Rahmen von Arbeitsanweisungen/Leitfäden/Handlungsempfehlungen oder niederschwelligen Checklisten/Tools/Dokumenten geregelt oder erläutert werden können.

2.5 Vorfragen

Klärungsbedürftig ist, wer für die Vorprüfung des als regelungsbedürftig eingebrachten Sachverhalts zuständig sein soll. Sofern in der Organisation eine generelle Verantwortlichkeit für die Erstellung und (Weiter-)Entwicklung von Richtlinien etabliert ist, dürfte diese prädestiniert für eine solche Vorprüfung sein. Dies sollte aber in enger Abstimmung mit der für die (Weiter-)Entwicklung und Führung der Datenschutz-Organisation verantwortlichen Stelle erfolgen. Teil dieser Betrachtung kann auch die Prüfung sein, ob die zu regelnden Inhalte oder die Art und Weise der Regelung die Berücksichtigung von betrieblichen Mitbestimmungs-, Mitwirkungs- bzw. Informationsrechten der Mitbestimmungsgremien mit sich bringt.

3. Grundstruktur einer Datenschutz-Richtlinie

3.1 Regelungszweck und Regelungsgegenstand

Neben einem übergeordneten Zweck, der für das Erstellen einer Richtlinie ins Feld geführt werden kann, sollte für jeden Einzelbereich einer Richtlinie ein konkreter Zweck formuliert werden. Die Formulierung des Zwecks verdeutlicht die Regulierungsbedürftigkeit der Thematik. Der Zweck einer Richtlinie zum Umgang mit Datenschutzverletzungen nach Artt. 33, 34 DS-GVO ist bspw. den Ablauf der internen und externen Meldewege im Falle einer Datenpanne vorab so konkret festzulegen, dass eine fristgerechte und gesetzeskonforme Meldung möglich ist.

3.2 Begriffsbestimmungen

Bevor das verbindliche Vorgehen, welches eine Richtlinie festlegen soll, erläutert werden kann, sollte eine Festlegung der für das Verständnis bedeutsamen Begriffe erfolgen. So kann bspw. das verbindliche Vorgehen bei Datenschutzverletzungen und das Zusammenspiel der verschiedenen Melde- und Benachrichtigungspflichten erst dann sinnvoll erläutert werden, wenn zuvor die Bedeutung der Begriffe wie z.B. Datenschutzverletzung, Vertraulichkeit, Verfügbarkeit und Integrität erläutert wurden. Eine Veranschaulichung der Legaldefinitionen anhand von kurzen Praxisbeispielen, die idealerweise spezifische Bezüge zur Organisation aufweisen, ist empfehlenswert.

3.3 Anwendungsbereiche (räumlich, zeitlich, personell)

Jede Richtlinie sollte eine genaue Beschreibung enthalten, an wen sie sich richtet. Dabei sollte beachtet werden, dass die adressierten Personenkreise

2 S. GDD-Praxishilfe DS-GVO - Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung, Version 2.0, Stand August 2021.

anhand ihrer ausgeübten Funktionen beschrieben werden und nicht namentlich. So wird der adressierte Personenkreis einer Richtlinie zum Umgang mit Datenschutzvorfällen die gesamte Belegschaft sein, wenn es um die interne Meldung eines Vorfalls aus der operativen Tätigkeit heraus angeht.

Der angesprochene Personenkreis bei einer Betroffenenanfrage innerhalb einer zu dieser Thematik erstellten Richtlinie dürften z.B. hinsichtlich der Weiterleitung alle Mitarbeiter, für die Bearbeitung jedoch im Falle von Kunden primär der Kundenservice bzw. der/die DSK im Vertriebsbereich und hinsichtlich der Beschäftigten der zuständige Personalbereich bzw. der/die dortigen DSK sein.

Die Zuständigkeiten sind klar zu definieren, wobei einzelne vorhandene Funktionen bei Bedarf zu einer neuen Funktion zusammengefasst werden können („Task Force Datenpanne", „Databreach-Team" etc.).

3.4 Schulungen und kontinuierliche Verbesserung

Für Richtlinien wie auch für andere Organisationsanweisungen wie z.B. Arbeitsanweisungen, Prozessbeschreibungen müssen verbindliche Vorgaben bestehen, wie mit Schulungsbedarf umzugehen ist, der sich aus der Schaffung der „neuen" Richtlinien-Vorgaben ergibt. Für etwaige Schulungsbedarfe sollten Verantwortlichkeiten/Zuständigkeiten, was die Konzeption, Durchführung, Dokumentation und auch die Überwachung angeht, festgelegt werden. Um den Anforderungen der Artt. 5 und 24 DS-GVO gerecht zu werden, sollte festgelegt werden, wie - unterstützt durch Schulungen - ein kontinuierlicher Verbesserungsprozess etabliert werden kann („lessons learned"), der die Erfahrungen aus der Anwendung der Richtlinie sowohl dokumentiert als auch für die Fortentwicklung der organisationsinternen Prozesse nutzt.

3.5 Mitgeltende Dokumente/Anlagen

Zur weiteren Veranschaulichung und Operationalisierung einer Richtlinie kann es sinnvoll sein, detailliertere Erläuterungen in mitgeltende Dokumente oder Anlagen auszulagern, um die Richtlinie selbst übersichtlich und schlank zu halten. Als mitgeltende Unterlagen kommen detaillierte Prozessdarstellungen, Checklisten, Templates/Formulare oder Schaubilder in Betracht. Um bei ggf. häufig notwendig werdenden Anpassungen der mitgeltenden Unterlagen keine zeitraubenden und unnötigen Freigabeverfahren oder eine neue Aktivierung durch die Leitung auszulösen, kann erwogen werden, diese Unterlagen zwar als mitgeltend, aber nicht als Bestandteil der Richtlinie zu kennzeichnen und einen Prozess zu definieren, wie und durch wen Änderungen dieser Unterlagen erfolgen können.

Um die Lesbarkeit und den Revisionsprozess zu erleichtern, können Anlagen und Verweise auf andere Dokumentationen genutzt werden. Änderungen müssen dann nicht in mehreren Dokumentationen berücksichtigt werden und Aktualisierungen in Anlagen sind schneller umsetzbar.

Mit einer durchdachten Ablagestruktur sind - sofern die Dokumentation elektronisch erfolgt - alle mitgeltenden Dokumentationen per Verlinkung erreichbar.

Beispiele für mitgeltende Dokumente/Anlagen sind:

Mitgeltende Dokumente	> Betriebs-/Dienstvereinbarungen > andere Richtlinien der Organisation (z.B. Informationssicherheit, Risikomanagement)
Anhänge/ Anlagen	> Kontaktdaten der wichtigsten Rollen/Funktionen > weitergehende Prozessbeschreibungen > weitergehende Arbeitsanweisungen > verbindlich zu nutzende Tools/Templates etc.

4. Typische Regelungsbereiche innerhalb einer Datenschutz-Richtlinie

Es gibt nicht DIE Datenschutz-Richtlinie, die für jede Organisation deren individuelle Datenschutz-Herausforderungen abdeckt und abbildet. In der Praxis zeigen sich aber typische Problemfelder, zu denen eine oder mehrere Datenschutz-Richtlinie(n) Festlegungen treffen sollte. Diese können natürlich entsprechend ergänzt werden.

Typische Regelungsbereiche von Datenschutz-Richtlinien sind:

Richtlinie regelt	Beispiele für Inhalte
Beschreibung der Rollen und Verantwortlichkeiten im Datenschutz[3]	>> Verantwortlicher (Leitung) >> Verarbeitungsverantwortliche (Fach-/ Geschäftsbereiche) >> Mitarbeiter >> Datenschutzteam >> Datenschutzmanager (DSMgr) >> Datenschutzkoordinator (DSK) >> Datenschutz-Experten/-Referenten >> *optional: Datenschutzbeauftragter (DSB)* >> *optional: Konzerndatenschutz/Konzern-datenschutzbeauftragter (KDSB)* >> *optional: Datensicherheits-Manager*
optional: Stellung und Aufgaben des Datenschutz-beauftragten[4]	>> Unterstützung des Datenschutzbeauftragten >> Abgrenzung zum Verantwortlichen und den übrigen definierten Rollen/Funktionen in der Datenschutzorganisation

3 S. GDD-Praxishilfe DS-GVO - Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung, Version 2.0, Stand August 2021.

4 S. GDD-Ratgeber: Der betriebliche Datenschutzbeauftragte nach DS-GVO und BDSG - Arbeitshilfe für die betriebliche Praxis - Version 2.1, Stand Juli 2019.

Richtlinie regelt	Beispiele für Inhalte
Generelle Beschreibung des Datenschutz-Managementsystems	>> Risikoorientierung >> Kontinuierliche Verbesserung (PDCA-Zyklus) >> Change Management >> Kontrolle/Audits >> Berichte/Reporting >> Überwachungsaufgaben
Sicherstellung der rechtmäßigen Verarbeitung/ Datenschutz-Change-Prozess	>> Verfahren zur Sicherstellung der datenschutzkonformen Verarbeitung >> Datenschutzprüfung bei Einführung oder Änderung der Verarbeitung personenbezogener Daten >> Information des DSB >> Verzahnung mit anderen Datenschutz-Prozessen
Dokumentation und Prüfung von Verarbeitungstätigkeiten/Verzeichnis Verarbeitungstätigkeiten[5]	>> Vorliegen einer Verarbeitungstätigkeit >> Planung von Verarbeitungstätigkeiten (Konzeptionsphase) >> Einführung, Durchführung, Änderung und Beendigung von Verarbeitungstätigkeiten >> Führung des Verzeichnisses der Verarbeitungstätigkeiten >> regelmäßige/anlassbezogene Überprüfungen
Datenschutz-Folgenabschätzung[6]	>> Erforderlichkeit einer Datenschutz-Folgenabschätzung >> Durchführung der Datenschutz-Folgenabschätzung >> Dokumentation der Ergebnisse einer Datenschutz-Folgenabschätzung >> Ggf. Kontaktaufnahme mit Aufsichtsbehörde
Informationspflichten[7]	>> Umsetzung der Transparenz-Anforderungen, z.B. bei Vertragsabschlüssen, auf Webseiten, bei Mailings/Katalogen

5 S. GDD-Praxishilfe DS-GVO - Verzeichnis von Verarbeitungstätigkeiten, Version 2.0, Stand März 2020; GDD-Praxishilfe DS-GVO - Verzeichnis von Verarbeitungstätigkeiten - Auftragsverarbeiter, Version 1.0, Stand Januar 2020.

6 S. GDD-Praxishilfe DS-GVO - Voraussetzungen der Datenschutz-Folgenabschätzung, Version 1.0, Stand Oktober 2017.

7 S. GDD-Praxishilfe DS-GVO - Transparenzpflichten bei der Datenverarbeitung, Version 2.1, Stand April 2018.

Richtlinie regelt	Beispiele für Inhalte
Umgang mit Betroffenenrechten innerhalb der Organisation[8]	>> Festlegen von Verantwortlichkeiten >> Kommunikationskanäle >> Eskalationsstufen (Einbeziehung von DSMgr, DSK und DSB) >> Fristen >> Schnittstellen und Ausgabeformate für Datenexporte (Kopie der verarbeiteten Daten) >> Mustervorlagen als Anhang >> Testprozeduren
Verletzung des Schutzes personenbezogener Daten und Meldeverfahren intern und extern[9]	>> Definition einer Verletzung des Schutzes personenbezogener Daten >> Meldeformular intern als Anlage >> Wer meldet an wen/wer wird informiert >> Fristen >> Wer entscheidet über eine Meldung an die Aufsichtsbehörde und die betroffene Person(en) >> Dokumentation der Meldung/Nicht-Meldung >> Dokumentation der externen Meldung sowie ggf. erfolgender Kommunikation mit Aufsichtsbehörden und/oder betroffenen Person(en) im Zusammenhang mit einer Meldung
Datenlöschung/Löschkonzept	>> Grundsätzliche Vorgaben zum Aufbau und der Struktur eines Löschkonzepts >> Verweis auf Löschkonzept/Löschkonzept als Anhang >> Löschung strukturierter und unstrukturierter elektronischer Daten sowie manueller Daten >> Ggf. Löschbestätigung
Technische und organisatorische Maßnahmen	>> Pseudonymisierung/Anonymisierung >> Vorgaben zu Privacy by Design >> Vorgaben zu Privacy by Default

8 S. zu möglichen Inhalten auch das **Praxis-Beispiel in Anlage 1:** Möglicher Aufbau einer Datenschutz-Richtlinie Betroffenenrechte.

9 S. GDD-Ratgeber: Datenpannen - Melde- und Benachrichtigungspflichten nach DS-GVO und BDSG - 3. vollständig neu bearbeitete Auflage, 2021.

Richtlinie regelt	Beispiele für Inhalte
Umgang mit IT-Systemen und Datenträgern	>> Verschlüsselung >> Listung von (freigegebenen) Geräten >> Lagerung von Geräten >> Vernichtung ausgemusterter Geräte und Datenträger (inkl. Papierdokumente) >> Nutzung der dienstlichen IT-Infrastruktur (insbesondere Abgrenzung der privaten Internet- und E-Mail-Nutzung) >> Homeoffice/Mobiles Arbeiten
Zusammenarbeit mit Dienstleistern, Partnern und Lieferanten mit Zugang zu personenbezogenen Daten: > Auftragsverarbeitungen[10] > Joint Controllership[11] > Übermittlungen	>> Klärung der rechtlichen Voraussetzungen >> Vorgaben zur Auftragsverarbeitung >> Vorgaben zur Verpflichtung, falls keine AV >> Vorgaben bei Joint Controllership >> Aufnahme der Besucherregelung
Datenschutz-Schulung/Awareness	>> Schulungs-Konzepte z.B. für Starter >> Spezifische Schulungskonzepte für bestimmte Funktionen (z.B. Personalbereich, Einkauf, Vertrieb, IT) >> Konzept für themenspezifische Awarenessmaßnahmen (z.B. Mailings, Datenschutztag, Newsletter)

Praxis-Tipp: Diese Übersicht erhebt keinen Anspruch auf Vollständigkeit – nehmen Sie in Ihren individuellen Datenschutz-Richtlinien die Bereiche auf, die für Ihre Organisation im Sinne des risikobasierten Ansatzes der DS-GVO wichtig sind.

10 S. GDD-Praxishilfe DS-GVO - Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO, Version 2.1, Stand Juni 2021; GDD-Praxishilfe DS-GVO - Praxishinweise für Auftragsverarbeiter, Version 1.2, Stand Oktober 2018.

11 S. GDD-Praxishilfe DS-GVO - Joint Controllership, Version 1.0, Stand Dezember 2019.

5. Formale Anforderungen

Um die Erkennbarkeit als Richtlinie zu gewährleisten und um einen festgelegten Standard zu etablieren, kann die Verwendung eines einheitlichen Musters bei der Erstellung einer Richtlinie als verbindlich festgelegt werden. Sollte es bereits unternehmensweit genutzte Vorlagen geben, die bei der Formulierung von Regelwerken genutzt werden sollen oder anderweitige Vorgaben des Qualitätsmanagements existieren, so ist zu empfehlen, sich bei der Erstellung der Richtlinien an diesen zu orientieren.

Sollte es keine internen formalen Vorgaben für die Erstellung eines Dokuments geben, kann empfohlen werden, zumindest folgende Angaben auf das Deckblatt einer Richtlinie aufzunehmen:

- Den/die für die inhaltliche Erstellung der Richtlinie zuständigen Fachverantwortlichen unter Angabe der Funktion/Abteilung
- Die Erstellungs- und Änderungshistorie inkl.
  - Versionsnummer
  - Erstellungs-/Änderungsdatum
  - Inhaltliche Änderungen (Kurzbeschreibung)
  - Name des Bearbeiters
  - die Unterschriften der Zeichnungsberechtigten/Aktivierungsberechtigten

Als weitere Vorgaben für die Richtlinie selbst können folgende Gesichtspunkte sinnvoll sein:

- Die Vorgabe, ein Inhaltsverzeichnis voranzustellen
- Einfachheit der Sprache und Formulierungen
- Verständlichkeit
- Sachliche Richtigkeit, Eindeutigkeit und Klarheit
- Voranstellung von Definitionen, wenn Fachtermini verwendet werden
- Genderneutrale Formulierung

6. Geltungsdauer und Überprüfungsfristen

Empfehlenswert ist es, bei der Erstellung der Richtlinie weitere Vorgaben zur Geltungsdauer und zu etwaigen Überprüfungsfristen aufzunehmen. Der Regelfall für die Geltung einer Richtlinie wird sein, dass diese ab Aktivierung der Richtlinie durch die Leitung Geltung erlangt und so lange gelten soll, bis sie von der Leitung der Organisation außer Kraft gesetzt wird (unbefristet). Sind Änderungen einer Gesetzeslage erkennbar, die Auswirkungen auf die zu erstellende Richtlinie aufweist oder hängt die Geltung einer Richtlinie ggf. von anderen Regelungen ab, sollte dies schon bei der Erstellung der Richtlinie mitbedacht werden.

Eine Richtlinie muss regelmäßig (bspw. alle zwei Jahre) oder anlassbezogen einer Prüfung im Hinblick auf Richtigkeit, Aktualität, Vollständigkeit und Wirksamkeit unterzogen werden. Die für die Prüfung zuständige Fachabteilung dürfte in der Regel, der/die auf dem Deckblatt genannte zuständige Fachverantwortliche sein. Sollte in der Organisation eine generelle Verantwortlichkeit für die Erstellung und (Weiter-)Entwicklung von Richtlinien bestehen, kann diese Stelle hier federführend agieren. Im Hinblick auf Datenschutz-Richtlinien bieten sich hier der/die DSMgr bzw. das Datenschutzteam an[12].

6.1 Wer erstellt und pflegt die Richtlinie?

Geht es darum, die Erstellung von Datenschutz-Richtlinien zu standardisieren und zu organisieren, stellt sich unweigerlich die Frage, welche Zuständigkeiten hier definiert werden sollten. Sobald im Rahmen der Vorprüfung die Regelungsbedürftigkeit festgestellt worden ist, stellt sich die Frage, wer für die eigentliche inhaltlich-fachliche Erstellung der Richtlinien zuständig sein soll. Naheliegend dürfte es sein, dass die Zuständigkeit bei der Funktion

12 S. a. GDD-Praxishilfe DS-GVO - Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung, Version 2.0, Stand August 2021.

liegt, die für die (Weiter-)Entwicklung und Führung der Datenschutz-Organisation verantwortlich ist (i.d.R. DSMgr bzw. das Datenschutzteam).

Die Verarbeitungsverantwortlichen in den operativen Fachabteilungen/Geschäftsbereichen sowie ggf. benannte DSK und weitere Datenschutz-Experten/innen sind bei der Erstellung von Richtlinien zum Thema Datenschutz zu beteiligen. Sofern in der Organisation ein DSB benannt wurde, berät und überwacht dieser die Fachfunktionen sowohl bei der Erstellung als auch bei der kontinuierlichen Weiterentwicklung der Richtlinien.

6.2 Bekanntmachung

Es sollte eine Festlegung erfolgen, wie eine Richtlinie bekannt gemacht wird. In aller Regel wird eine Richtlinie erst mit ihrer Bekanntmachung wirksam. Daher sollte sich die Form der Bekanntmachung danach richten, welcher Personenkreis mit der Richtlinie angesprochen werden soll. Eine Richtlinie zum Umgang mit Datenschutzverletzungen wird sich, was die interne Meldepflicht angeht, an alle Beschäftigten richten. Daher wird es in punkto Bekanntmachung erforderlich sein, alle relevanten Beschäftigten zu erreichen. Sofern alle Beschäftigten Zugriff auf das Intranet der Organisation haben, kann das Intranet ein geeignetes Medium für die Bekanntmachung sein. Alternativ kann als Medium und Art und Weise der Bekanntmachung auch ein Aushang am schwarzen Brett in Frage kommen. Zusätzlich kann der DSMgr bzw. das Datenschutzteam, die DSK und/oder die jeweils zuständige Personalabteilung für die Beschäftigten ihres Organisationsbereichs, die nicht über einen Intranetzugang verfügen, jede Richtlinie als gedrucke Version vorhalten und ggf. verteilen.

Praxis-Tipp: Die Außerkraftsetzung sowie die Aktualisierung einer Richtlinie sollten in gleicher Weise erfolgen, wie die Bekanntmachung. Geeignete Kommunikationskanäle können sein:

>> Intranet,
>> Papier, Aushang,
>> E-Mail-Versand.

6.3 Steuerung und Überwachung der Umsetzung

Unverzichtbarer Bestandteil einer Datenschutz-Richtlinie ist die Definition klarer Verantwortlichkeiten und Zuständigkeiten zu den beschriebenen Prozessen. Diese liegen nicht immer bei den Funktionsträgern der Datenschutz-Organisation wie DSMgr/DSK und erst recht nicht beim DSB. Beispiele: die Verantwortung für die Verpflichtung der Beschäftigten auf den Datenschutz liegt regelmäßig in der Personalabteilung, die für die Meldung einer Datenpanne an die zuständigen Funktionsträger in der Datenschutz-Organisation bei allen Beschäftigten, die Meldung einer Datenpanne an die Datenschutzaufsichtsbehörde kann an den DSMgr/das Datenschutzteam delegiert worden sein.

Der DSMgr bzw. das Datenschutzteam trägt/tragen die Verantwortung für die Einhaltung der externen und internen Datenschutzvorgaben sowie für die laufende Pflege und Weiterentwicklung des gesamten Regelwerks in der Organisation. Hierzu ist ein kontinuierlicher Verbesserungsprozess zu implementieren. Intensität und Regelmäßigkeit von Kontrollen und Überwachungsmaßnahmen sind entsprechend des risikobasierten Ansatzes der DS-GVO sowohl von der spezifischen Situation in der jeweiligen Organisation als auch vom jeweiligen Regelungsinhalt einer Richtlinie abhängig. Sofern die Organisation einen DSB benannt hat, gehört es auch zu seinen Aufgaben, die Einhaltung

der gesetzlichen Vorgaben, der internen Strategien und Vorschriften sowie die Funktionsfähigkeit des Datenschutzmanagements zu überwachen.

7. Abstimmung/Mitprüfung

Für alle Richtlinien besteht ein Abstimmungsbedarf im Hinblick auf die gesamten Rahmenbedingungen, denen die Organisation unterliegt. In großen Organisationen empfiehlt es sich daher, sofern vorhanden

>> die Rechtsabteilung,
>> die Compliancestelle,
>> das Qualitätsmanagement,
>> die Revision,
>> die Personalabteilung und
>> ggf. die Mitbestimmungsorgane

dabei einzubinden.

Je nachdem, welche Schnittmenge die vorhandenen Fachabteilungen mit den Inhalten der Richtlinie aufweisen, sollten diese Stellen gebeten werden, die Erstellung der Richtlinie durch ihre fachliche Mitprüfung zu unterstützen, indem sie den Richtlinien-Entwurf einer kritischen Durchsicht unterziehen und sicherstellen, dass die darin geregelten Sachverhalte nach ihrer Einschätzung korrekt und angemessen dargestellt sind und keiner Ergänzung bedürfen.

Mögliche Prüffragen können bspw. im Einzelfall sein:

>> Ist es möglich, dass durch Inhalte der Richtlinie Informations-, Mitwirkungs- und Mitbestimmungsrechte des Betriebs-/Personalrats (soweit vorhanden) ausgelöst werden?
>> Ist sichergestellt, dass die Richtlinie nicht in Widerspruch zu bereits existierenden Richtlinien steht (insbesondere, wenn es sich um eine Organisation innerhalb eines Konzernverbundes handelt)?
>> Werden Formalia des Qualitätsmanagements beachtet?
>> Führt der Inhalt der Richtlinie ggf. zu Inkonsistenzen mit gesetzlichen Vorgaben bzw. mit nationalgesetzlichen Vorgaben?

Praxis-Tipp: In kleineren und mittleren Organisationen werden die zuständigen Funktionsträger in der Datenschutz-Organisation diese Fragen häufig allein klären und mit der Leitung abstimmen müssen.

8. Besonderheiten im Konzern

In großen Unternehmensgruppen und internationalen Konzernen mit rechtlich selbständigen Organisationen besteht die Herausforderung darin, ein geeignetes Maß an zentralen und dezentralen Regelungen zu finden. In Abhängigkeit des Beherrschungsgrads der Konzernmutter, der rechtlichen Regelungen zu den generellen Organ-Verantwortlichkeiten, spezifischer nationaler (Datenschutz-) Gesetze und Anforderungen der jeweiligen Aufsichtsbehörden ist zu klären, inwieweit Datenschutz-Richtlinien unmittelbar oder mittelbar von der Konzernmutter angewiesen werden können.

In der Regel wird es in einem Konzern ein mehrstufiges Regelungs- und Anweisungssystem geben. Konzernrichtlinien zum Datenschutz regeln dabei grundlegende Aspekte eines konzernweit relevanten Sachverhalts auf konzerneinheitliche Weise, mit verbindlichen Vorgaben für eine Vielzahl an Beschäftigten. Konzernrichtlinien zum Datenschutz sollten von der Konzernmutter über die Organe der nachgeordneten Gesellschaften in Kraft gesetzt werden. Dabei sollte explizit gefordert werden, dass die Organe im Rahmen der bestehenden Einwirkungsmöglichkeiten und nationalen Gesetze

die Einhaltung der Konzernrichtlinien sicherstellen sollen. Es empfiehlt sich einen Prozess zu definieren, der die Anweisung der Konzernrichtlinien in den nachgeordneten Gesellschaften dokumentiert, z.B. durch Bestätigungsschreiben der jeweiligen Geschäftsführungen. Sollten einzelne Konzernrichtlinien oder auch Teile von Konzernrichtlinien von nachgeordneten Gesellschaften nicht umgesetzt werden können, sollten die Gründe hierfür sowie die ggf. ergriffenen Ersatzmaßnahmen ebenfalls dokumentiert und an die Konzernmutter kommuniziert werden. Es empfiehlt sich zur Beurteilung der Anwendbarkeit von Konzernrichtlinien eine standardisierte Risikobewertung vorzugeben und vorzunehmen.

Da die Konzernrichtlinien zum Datenschutz lediglich grundlegende Aspekte regeln können, besteht die Erfordernis in den nachgeordneten Organisationen weitergehende Richtlinien oder Anweisungen zu erstellen, die die Konzernregelungen weiter präzisieren und für den konkreten Anwendungsbereich spezifizieren. Dabei ist von der Leitung und den Fachverantwortlichen auf Widerspruchsfreiheit zum Konzernregelwerk zu achten.

Die Konzernmutter sollte über die dort implementierte Datenschutzorganisation (Konzerndatenschutz, DSMgr bzw. Datenschutzteam) die (Weiter-) Entwicklung der Gesamtheit an zentralen und dezentralen Leit- und Richtlinien zum Datenschutz koordinieren und überwachen. Hierfür sind entsprechende Informations- und Kommunikationsprozesse zwischen Konzernmutter und den nachgelagerten Gesellschaften zu etablieren.

9. Fazit

Eine oder mehrere Datenschutz-Richtlinie(n) bildet/bilden das Fundament zur Umsetzung der gesetzlichen datenschutzrechtlichen Regelungen in der spezifischen Organisation. Datenschutz-Richtlinien überführen und übersetzen die rechtlichen Anforderungen in die spezifischen Verantwortlichkeiten und Prozesse einer Organisation und sind somit ein wesentliches Element des risikoorientierten Managementsystems.

Mit den Richtlinien (ggf. in Verbindung mit einer Datenschutz-Leitlinie) als verbindlichem Regelungsrahmen wird Datenschutz, Teil der gemeinsamen Werte und der gelebten (Datenschutz-)Praxis der Organisation. Die regelmäßige Schulung/Vermittlung und Kommunikation der organisationsweiten Regelungen, die Konkretisierung spezifischer Sachverhalte in nachgeordneten Regelungen und die regelmäßige Weiterentwicklung des gesamten Regelwerkes ist für die Erfüllung der gesetzlichen Nachweispflichten zwingend notwendig.

Praxis-Tipp: Erst durch die Schulung und direkte Vermittlung der Prozesse, Kommunikations- und Entscheidungsketten wird eine Datenschutz-Organisation mit ihren Leit- und Richtlinien erlebbar und lebendig!

Anlage I

Praxis-Beispiel: Möglicher Aufbau einer Datenschutz-Richtlinie Betroffenenrechte

1. **Zweck und Geltungsbereich der Richtlinie Betroffenenrechte**
   a. Was sind die Ziele der Richtlinie?
   b. An wen richtet sie sich?
   c. Welche Bereiche der Organisation sind involviert?
   d. Bedeutung der schnellen und zuverlässigen Bearbeitung von Betroffenenanfragen klarstellen
2. **Datenschutzrechte betroffener Personen (Betroffenenrechte)**
   a. Welche Rechte haben Betroffene?
   b. Erläuterung typischer Anfragen
   c. Evtl. Abgrenzung Werbesperre/Löschung
   d. Negativauskunft
   e. Erläuterung der Identitätsprüfung
   f. Hinweis auf mögliche Einschränkungen der Rechte (zu häufige Inanspruchnahme)
3. **Zuständigkeiten und Fristen bei der Bearbeitung von Betroffenenrechten**
   a. Über welche Kanäle sind Betroffenenanfragen möglich?
   b. Wohin werden sie weitergeleitet?
   c. Wer beantwortet wie schnell? Evtl. Vertretungsregelungen
4. **Genaue Beschreibung der einzelnen Prozessschritte**
   a. Zu jedem möglichen Kommunikationskanal wird das Vorgehen im Falle einer Inanspruchnahme von Betroffenenrechten beschrieben
   b. Beantwortung/Umsetzung innerhalb der Frist
   c. Ablauf der Identitätsprüfung/Verantwortlichkeiten
   d. Vorgehen: Kopie und Datenexport
   e. Vorgehen: Berichtigung
   f. Vorgehen: Einschränkung/Sperre
   g. Vorgehen: Widerruf Einwilligung
   h. Vorgehen: Löschung
   i. Dokumentation der Umsetzung/Beantwortung
   j. Löschfristen
5. **Dokumentation der Umsetzung/rechtlicher Nachweis**
   a. Speicherfristen
   b. Zugriffsrechte
6. **Schulung der einbezogenen Mitarbeiter**
7. **Evtl. Anlagen**
   a. Musterschreiben
   b. Vorlagen Dokumentation Erfüllung Betroffenenanfrage
   c. Löschkonzept

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Mitglied werden? Mehr Informationen?

https://www.gdd.de/service/mitglied-werden oder eine E-Mail an: info@gdd.de

Eine Mitgliedschaft bietet wesentliche Vorteile:

>> Mitglieder-Nachrichten mit aktuellen Fachinformationen
>> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
>> Beratung bei konkreten Einzelfragen
>> Zugriff auf Rechtsprechungs- und Literaturarchiv
>> Online-Service „Dataagenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
>> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
>> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.800 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 2 28 96 96 75-00
Fax: +49 2 28 96 96 75-25
www.gdd.de
info@gdd.de

Diese Praxishilfe wurde im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt durch:

RA Levent Ferik, LL.M. (Datenschutzbeauftragter, HIL Heeresinstandsetzungslogistik GmbH)
Stefan Hardelt (Fachberatung Datenschutz)
Dirk Niedernhöfer (dn Datenschutz UG)
Uwe Bargmann (Berater Datenschutzmanagement)
Thomas Müthlein (DMC - Datenschutz Management & Consulting, GDD-Vorstand)

Ansprechpartnerin: RAin Yvette Reif, LL.M.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn
Stand: Version 2.0 (November 2021)