Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO

Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung

INHALT

Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DS-GVO) überträgt dem Verantwortlichen bzw. Auftragsverarbeiter die Pflicht, durch organisatorische Maßnahmen die Einhaltung des Datenschutzes sicherzustellen. Wie bei der Umsetzung aller regulatorischen Vorgaben kommt dabei der klaren Definition und Zuordnung von Verantwortlichkeiten und Aufgaben eine entscheidende Bedeutung zu.

Die GDD-Praxishilfe „Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung“ versucht auf der Grundlage der gesetzlichen Vorgaben, der Entwicklungen in Unternehmen und Behörden seit Geltung der DS-GVO sowie allgemeiner Organisationsformen ein Modell hierfür aufzuzeigen. Die Herausforderung dabei besteht einerseits darin, dass die Umsetzung der Aufgaben aus der DS-GVO grundsätzlich unabhängig von Größe und Organisationsgrad der betroffenen Einheit, z.B. als kleines oder mittleres Unternehmen (KMU), Konzern oder Behörde, sicherzustellen und somit nicht disponibel ist. Andererseits unterliegt die konkrete interne Zuweisung von Kompetenzen, Rollen und operativen Verantwortlichkeiten der jeweiligen Situation im Unternehmen / in der Behörde und ist in Abhängigkeit der Größe und räumlichen Verteilung der Geschäftsstrategie, es allgemeinen Steuerungs- und Führungsmodells und der individuellen Risikosituation anzupassen.

In dem nachfolgenden Modell wird hierzu zwischen Umsetzungsverantwortung (Leitung, operative Fachabteilungen/Geschäftsbereiche, Fachabteilungen in Management- und Support-Funktionen (MSF) und Mitarbeiter/-innen) und operativ unterstützenden Rollen im Datenschutz (Datenschutzteam, Datenschutzmanager/-in (DSMgr), Datenschutzkoordinator/-in (DSK) Datenschutzexperten/-expertinnen oder Datenschutzreferenten/-referentinnen) unterschieden. Sofern ein/-e Datenschutzbeauftragte/-r benannt wird, unterstützt diese/-r die vorgenannten Rollen im Rahmen seiner/ihrer gesetzlich definierten Beratungs- und Überwachungsfunktion.

Ausgehend von dieser Aufteilung wird in gesonderten Kapiteln auf die Besonderheiten zur Anpassung des Modells an die unterschiedlichen Bedürfnisse von KMU und Konzernen eingegangen. Zur besseren Übersichtlichkeit stehen die in der GDD-Praxishilfe vorgestellten Rollen und Aufgaben ab S. 17 als synoptische Darstellung zur Verfügung.

1. Einführung

Aus der „Rechenschaftspflicht“ (Art. 5 Abs. 2, 24 DS-GVO) lässt sich ableiten, dass der Verantwortliche eine risikoadäquate Datenschutzorganisation und ein Datenschutz-Managementsystem (DSMS) errichtet. Gemeint ist hiermit die Etablierung und kontinuierliche Weiterentwicklung risikoadäquater Strukturen und Prozesse mit entsprechenden Verantwortlichkeiten und Regelungen zur Kooperation. Die Einrichtung und Weiterentwicklung einer solchen Datenschutzorganisation hat dabei unabhängig von der gesetzlichen Benennungspflicht eines/einer Datenschutzbeauftragten (DSB) gem. DS-GVO bzw. nationaler Regelungen (Bundesdatenschutzgesetz - BDSG bzw. jeweiliges Landesdatenschutzgesetz - LDSG) zu erfolgen. Auch ohne eine/-n DSB muss der Datenschutz im Unternehmen durch den Verantwortlichen organisiert werden!

Orientiert am sog. PDCA-Zyklus (Plan, Do, Check, Act), der Bestandteil vieler Managementsysteme ist, sowie an Art, Umfang und Zwecken der Verarbeitung personenbezogener Daten ergeben sich allgemein die „Aufgaben“ im Datenschutz. Die Kompetenzen, Rollen und operativen Verantwortlichkeiten zur Erfüllung der Aufgaben sind i.d.R. im Unternehmen verteilt bzw. ggf. auch intern gar nicht vorhanden, wenn diese auf Dienstleister ausgelagert sind.

Die Verantwortlichkeiten und Aufgaben nach der DS-GVO sowie das Verhältnis zur Stellung des/der DSB werden nachfolgend anhand von „Rollen“ beschrieben. Welche konkreten Organisationseinheiten diese Rollen im Einzelfall wahrnehmen, ist in Abhängigkeit von der Größe und Struktur des Verantwortlichen und ggf. weiterer Faktoren individuell festzulegen. Die Aufgabenzuweisung sollte dabei nach dem Grundsatz der Deckungsgleichheit von Aufgabe, Kompetenz und Verantwortung erfolgen.

Sofern ein/-e DSB benannt ist, sind die in Art. 38 f. DS-GVO bzw. im BDSG / im jeweiligen LDSG getroffenen Festlegungen zu dessen Stellung und Aufgaben zu beachten. Für die übrigen Rollen und Verantwortlichkeiten im Rahmen der Datenschutzorganisation gibt es keine konkreten gesetzlichen Vorgaben.

Verallgemeinernd lässt sich aber folgende Zuordnung von Verantwortlichkeiten, Aufgaben und Rollen feststellen (s. Abbildung basierend auf dem RASCI-Modell):

Accountability	* Gesamtverantwortung für den Datenschutz * Nachweis- und Rechenschaftspflicht * Einrichtung einer DS-Organisation	Leitung (Vorstand, Geschäftsführung)
Responsibility	* Verantwortung für risikobasierte operative Umsetzung der Datenschutz-Anforderungen * Prozess-/Organisationsverantwortung	* Führungskräfe der operativen Fachabteilungen * Mitarbeiter der Fachbereiche
Support	Unterstützung operativer Fachbereiche bei der risikobasierten operativen Umsetzung durch spezifisches Fach-Know-how	Führungskräfte/Mitarbeiter in Fachbereichen mit Unterstützungsfunktion (z.B. Einkauf, Recht, IT, Sicherheit)
Consulting	* Beratung der Verantwortlichen und Mitarbeiter * Monitoring der Umsetzung und Einhaltung externer und interner Vorgaben	* Datenschutzbeauftragter * weitere Mitarbeiter des Datenschutz-Teams
Information	Regelmäßige und spezifische Information und Kommunikation über z.B. rechtliche, prozessuale, funktionale, risikorelevante Aspekte	alle Rollen in Abhängigkeit konkreter datenschutzbezogener Aspekte

Die Darstellung in dieser Praxishilfe geht von einem idealtypischen Modell aus, das je nach Struktur des Unternehmens, des Konzerns bzw. der Behörde nach Bedarf zu skalieren ist. Dies kann dazu führen, dass in kleineren Einheiten verschiedene Rollen durch eine Person ausgefüllt werden.

2. Glossar und Abkürzungen

Datenschutzbeauftragte/-r (DSB)

>> gesetzlich definierte Rolle (Artt. 37 bis 39 DS-GVO; §§ 5–7, 38 BDSG bzw. LDSG)
>> Beratung und Überwachung als Kernaufgaben
>> keine Weisungsbefugnisse/keine operative Datenschutzverantwortung

Datenschutzkoordinator/-in (DSK)

>> keine gesetzlich definierte Rolle
>> Schnittstelle zwischen den Fachbereichen bzw. lokalen Einheiten und den Datenschutzverantwortlichen sowie dem/der ggf. benannten DSB
>> dezentrale Funktion
>> Unterstützung der datenverarbeitenden Einheiten bei der Umsetzung des Datenschutzes

Datenschutzmanager/-in (DSMgr)

>> keine gesetzlich definierte Rolle
>> (Weiter-)Entwicklung und Führung der Datenschutzorganisation
>> fachbereichsübergreifende Tätigkeit
>> zentrale Ansiedlung, z.B. als Leiter/-in des Datenschutzteams

Datenschutzorganisation

>> Gesamtheit der Maßnahmen zur Umsetzung des Datenschutzes

Datenschutzteam

>> nicht gesetzlich vorgesehen oder definiert
>> umfasst die operativen Datenschutzfunktionen
>> institutionalisiert oder virtuell
>> Unterstützung der operativen Fachbereiche bei ihren Datenschutzaufgaben
>> Förderung der gemeinsamen Ausrichtung des Datenschutzes bei komplexen bzw. dezentralen Organisationen

Gemeinsame/-r Datenschutzbeauftragte/-r

>> Personenidentische/-r Datenschutzbeauftragte/-r einer Unternehmensgruppe bzw. mehrerer öffentlicher Stellen

Konzerndatenschutzbeauftragte/-r (KDSB)

>> Bezeichnung für den/die gemeinsame/-n Datenschutzbeauftragte/-n mehrerer Konzerngesellschaften

Leitung

>> gesetzliche Vertretung der datenverarbeitenden Stelle, z.B. der Geschäftsführung bei der GmbH oder der Vorstand beim Verein
>> verantwortlich für den Datenschutz
>> Delegation der Verantwortung im Innenverhältnis möglich

Management- und Support-Funktionen (MSF)

>> Organisationseinheiten, in denen spezielle Kompetenzen und spezielles Knowhow gebündelt sind und operativen Fachbereichen unterstützend zur Verfügung gestellt werden, z.B. in den Bereichen Organisation, Recht, Kontrolle/Audit, IT-Sicherheit

Verantwortlicher

>> gesetzlich definiert in Art. 4 Nr. 7 DS-GVO
>> juristische Person, Verein, Behörde o.ä.
>> vertreten durch die Leitung
>> Normadressat der DS-GVO

Verantwortlichkeiten (RASCI-Modell)

>> A = Accountability – Rechenschaftspflicht; Verantwortlichkeit im Sinne von „genehmigen“ oder „billigen“; Nachweis der Umsetzung und Einhaltung von Maßnahmen

>> R = Responsibility – Zuständigkeit für die eigentliche Durchführung von Aufgaben (Durchführungsverantwortung); Person, welche die Initiative für die Durchführung (auch durch andere) gibt oder die Aktivität selbst durchführt

>> S = Support – Unterstützung, z.B. durch Expertise oder Bereitstellung von Mitteln

>> C = Consulting – Beratung; Person, die nicht direkt an der Umsetzung beteiligt ist, aber relevante Informationen für die Umsetzung hat und deshalb befragt werden soll oder muss

>> I = Information – Information; Person, die Informationen über den Verlauf bzw. das Ergebnis der Aktivitäten erhält oder die Berechtigung besitzt, Auskunft zu erhalten

3. Die Verantwortlichkeiten und Aufgaben nach der DS-GVO im Detail

3.1 Leitung

Normadressat der DS-GVO ist der sog. „Verantwortliche“. Dieser wird in **Art. 4 Nr. 7 DS-GVO** definiert als „juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Die als „Verantwortliche“ in der Pflicht stehenden Unternehmen, Vereine oder Behörden werden **gesetzlich vertreten durch** ihre **Leitung** (AG-Vorstand, Vereinsvorstand, Geschäftsführung, Behördenleiter/-in etc.). Letztere tragen damit als „Leitung des Verantwortlichen“ insbesondere die folgenden grundsätzlichen Datenschutzverantwortlichkeiten:

>> Die Leitung trägt die **Gesamtverantwortung für den Datenschutz.** Dies umfasst die Verantwortung für die wirksame Umsetzung der DS-GVO und des BDSG bzw. des jeweiligen LDSG.

>> Sie ist für die **Einhaltung der Grundprinzipien des Datenschutzes** gem. DS-GVO verantwortlich und muss deren Einhaltung – durch entsprechende Dokumentation – nachweisen können (**„Rechenschaftspflicht/Accountability“**[1]).

>> Die Leitung trägt die **Organisationsverantwortung** im Hinblick auf die nachweisbare[2] Umsetzung der DS-GVO (Vermeidung von Organisationsverschulden), insbesondere hinsichtlich der Delegation/Bestimmung von Aufgaben und Verantwortlichkeiten (Rollen):

> **Delegation/Bestimmung von Aufgaben und Verantwortlichkeiten (Rollen)** in der Aufbau- und Ablauforganisation mittels Anweisungen, z.B. Leitlinien, Richtlinien/Policies, Arbeitsanweisungen (Vermeidung von Anweisungsverschulden)

> **Implementierung angemessener Datenschutzprozesse**, insbesondere der Datenschutzkernprozesse „datenschutzkonforme Datenverarbeitung“, „Sicherstellung von Betroffenenrechten und Transparenzpflichten“, „Handhabung von Datenschutzverletzungen“ sowie z.B. von Prozessen zur Risikobewertung, zur Durchführung gesetzlich erforderlicher Datenschutz-Folgenabschätzungen oder zur Beauftragung von Dienstleistern bzw. zur Zusammenarbeit mit Dritten allgemein

> **Einrichtung und Aufrechterhaltung einer Datenschutzorganisation**, durch die Datenschutzfachkunde mittels interner oder externer Ressourcen sicher verfügbar gemacht wird (Vermeidung von Selektionsverschulden); es empfiehlt sich, die erforderlichen Fachkompetenzen zur operativen Unterstützung der Fachverantwortlichen in einem Datenschutzteam unter Leitung eines/einer „Datenschutzmana-

1 Siehe Art. 5 Abs. 2 DS-GVO.

2 Siehe Art. 24 DS-GVO.

gers/-managerin (DSMgr)“ zu bündeln (zum Datenschutzteam vgl. auch Abschnitt 4.2)
  - **Sicherstellung ordnungsgemäßer Überwachung** der datenschutzrelevanten Prozesse durch Einrichtung ausreichender Kontrollmechanismen und -systeme (Vermeidung von Überwachungsverschulden)
- **verantwortlicher Vertreter des Unternehmens bzw. der öffentlichen Stelle gegenüber der Aufsichtsbehörde** (Normadressat und, soweit kein/-e DSB benannt ist, alleinige Anlaufstelle für die Behörde)
  - auskunftspflichtig
  - verantwortlich für die Umsetzung aufsichtsbehördlicher Anweisungen

Diese grundsätzlichen Datenschutzverantwortlichkeiten der Leitung konkretisieren sich im Einzelnen wie folgt:

- Bestimmung, ggf. gestuft, eines/einer verantwortlichen Bereichs/Führungskraft/Mitarbeiters/Mitarbeiterin **(Verarbeitungsverantwortlicher)** für jeden Fall der Verarbeitung personenbezogener Daten
- Sicherstellung, dass alle internen und externen Mitarbeiter/-innen der Organisationseinheit, die mit der Verarbeitung personenbezogener Daten betraut sind, zur **Vertraulichkeit verpflichtet** und über ihre datenschutzrechtlichen Pflichten informiert sind sowie **regelmäßig geschult werden**
- Sicherstellung, dass in der Organisationseinheit und nachgeordneten Einheiten in hinreichendem Umfang **kompetente Mitarbeiter** vorhanden sind, die angemessen und fokussiert die datenschutzrechtlichen Anforderungen umsetzen bzw. die Umsetzung koordinieren können, z.B. durch Einsatz von Datenschutzkoordinatoren
- **Bereitstellung erforderlicher** finanzieller, sachlicher und personeller Ressourcen zur Umsetzung und Einhaltung der DS-GVO sowie für die kontinuierliche Verbesserung des Datenschutzes und seiner Organisation
- **Initialisierung / Beauftragung von Audits**
- **Sicherstellung eines Reportingsystems** im Rahmen der Überwachung der Einhaltung des Datenschutzes
- **Anweisungen zur Umsetzung von Empfehlungen/Feststellungen** aus Kontrollen und Überwachungen zwecks Weiterentwicklung des Datenschutzes
- **Benennung eines/einer DSB**, soweit gesetzlich erforderlich[3] bzw. unternehmerisch sinnvoll (**Achtung:** Auch bei Nichtbestehen einer Benennungspflicht muss trotzdem Datenschutzfachkunde vorhanden sein oder eingekauft werden!). Bei der Benennung ist insbesondere Folgendes sicherzustellen:
  - Publizität des/der DSB[4]: Veröffentlichung der Kontaktdaten des/der DSB und Mitteilung der Daten an die Aufsichtsbehörde
  - Bereitstellung erforderlicher **Ressourcen**[5] für den/die DSB, z.B. durch ausreichende Freistellung des/der internen DSB von anderen Tätigkeiten
  - Gewährleistung einer **Vertretung des/der DSB** für den Fall der Abwesenheit
  - organisatorische Sicherstellung, dass der/die DSB seine/ihre gesetzlichen Aufgaben erfüllen kann,[6] insbesondere **Unterstellung** des/der DSB **unter die Leitung** im Hinblick auf dessen/deren Informations-, Reporting- und Überwachungsaufgaben
  - organisatorische Sicherstellung der **unabhängigen, weisungsfreien und vertraulichen Wahrnehmung der Aufgaben** durch den/die DSB[7]
  - klare **Abgrenzung und Regelung der Zusammenarbeit zwischen operativen Datenschutzrollen und dem/der DSB**

3 Art. 37 Abs. 1, 4 DS-GVO i.V.m. § 38 BDSG.
4 Art. 37 Abs. 7 DS-GVO.
5 Art. 38 Abs. 2 DS-GVO.
6 Art. 38 Abs. 3 DS-GVO.
7 Art. 38 Abs. 3, 5 DS-GVO; Erwägungsgrund 97 S. 4 DS-GVO.

- regelmäßiger **Informationsaustausch** der Leitung **mit dem/der DSB** und Ergreifen von geeigneten Maßnahmen, sofern erforderlich

Ein Mangel in der Wahrnehmung der **Organisationsverantwortung** durch die Leitungsorgane ist ein z.B. nach OWiG (Ordnungswidrigkeitengesetz) sanktionierbares **Organisationsverschulden**. Dies kann bestehen in:

- **Anweisungsverschulden**: Anweisungen fehlen, sind fehler- oder lückenhaft;
- **Selektionsverschulden**: Verantwortung wird an ungeeignete Mitarbeiter delegiert;
- **Überwachungsverschulden**: Kontrollen werden gar nicht oder lückenhaft durchgeführt.

3.2 Operative Fachabteilungen/Geschäftsbereiche

Die operativen Fachabteilungen/Geschäftsbereiche sind die Organisationseinheiten, die maßgeblich für die Umsetzung und Einhaltung der datenschutzrechtlichen Anforderungen verantwortlich sind. Im Rahmen der von ihnen verantworteten Prozesse und Verarbeitungen tragen sie Sorge für einen angemessenen Schutz der personenbezogenen Daten.

Ihnen obliegen dabei folgende Rollen und Aufgaben:

- **Durchführungsverantwortung**: Ausführung der Anweisungen der Leitung zur Umsetzung der DS-GVO (**Responsibility**), z.B.
  - arbeitsplatzbezogene Instruktion der einzelnen Mitarbeiter
  - Durchführung fachbereichsspezifischer Schulungs- und Awarenessmaßnahmen
- **Prozessverantwortung**; diese umfasst insbesondere:
  - **Definition der organisatorischen Schnittstellen (auch zum Datenschutz), insbes. Anbindung an die Datenschutzkernprozesse** wie „datenschutzkonforme Datenverarbeitung“, „Handhabung von Datenschutzverletzungen“ etc.
  - **Erfüllung von Dokumentationspflichten**, z.B. Dokumentation von Zwecken und Mitteln der Verarbeitung personenbezogener Daten, Verzeichnis der Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung, Nachweis der Einwilligung
  - **Verantwortung für die datenschutzrechtliche Risikobewertung** und, sofern möglich, für die Vermeidung datenschutzrechtlicher Risiken durch Prozess-, Produkt- und Technikgestaltung, d.h. data protection by design/default, Löschkonzept usw.; sofern notwendig, Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)
  - **Erfüllung von Transparenz- und Informationspflichten sowie Gewährleistung der Betroffenenrechte** (Anbindung an die vorgesehenen Prozesse bzw. Entwicklung eigener Prozesse für Information, Auskunft, Löschung, Berichtigung, Recht auf Vergessenwerden, Datenportabilität, Einwilligungswiderruf, Widerspruch und Datenpannen)
  - **Sicherstellung von wirksamen und datenschutzkonformen Vertragsbeziehungen** mit den ausgewählten Verarbeitern personenbezogener Daten, z.B. Auftragsverarbeiter, Geschäftspartner im Rahmen der gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO
  - **Kontrolle der Auftragsverarbeiter**
  - **frühzeitige Einbindung des/der DSB (erfolgskritischer Faktor!)**
  - **Implementierung und Durchführung geeigneter prozessimmanenter Kontrollen** zur Gewährleistung der Einhaltung der ge-

setzlichen und internen Vorgaben zum Datenschutz

- >> regelmäßige Prüfung und ggf. Anpassung der Datenschutzmaßnahmen mit dem Ziel der **kontinuierlichen Verbesserung**
- >> **Unterstützung** insbes. des/der DSMgr und des/der DSB **bei Berichts- und Reportingmaßnahmen**
- >> **Unterstützung der Datenschutzorganisation bei der Zusammenarbeit mit der Aufsichtsbehörde**; verantwortlich insbes. für Sachverhaltsaufklärung/-darstellung sowie für relevante Dokumentationen zur Zusammenarbeit mit der Behörde

> **Es empfiehlt sich die Benennung von „Datenschutzmanagern/-managerinnen (DSMgr)" und/oder „Datenschutzkoordinatoren/-koordinatorinnen (DSK)" mit ausreichenden zeitlichen wie fachlichen Ressourcen in den Fach-/Geschäftsbereichen, welche die diesbezüglichen datenschutzrechtlichen Anforderungen angemessen und fokussiert umsetzen bzw. die Umsetzung koordinieren können.**

3.3 Fachabteilungen in Management- und Support-Funktionen (MSF)

Zur effektiven Wahrnehmung ihrer datenschutzrechtlichen Verantwortung benötigen die operativen Bereiche spezielle fachliche Unterstützung, insbesondere Kompetenzen in den Bereichen Organisation, Recht, Kontrolle/Audit, IT-Sicherheit. Soweit im Unternehmen, in der Unternehmensgruppe, im Konzern bzw. in der Behörde Personen und/oder Abteilungen mit entsprechenden Fähigkeiten vorhanden sind, können ihnen entsprechende Aufgaben zugewiesen werden. In dieser Rolle können diese Personen auch Teil eines Datenschutzteams (siehe unten) sein. Ansonsten sind die benötigten Kompetenzen auf andere Weise sicherzustellen, z.B. durch Einschaltung externer Dienstleister. Sofern eigene Fachabteilungen mit Management- und Support-Funktionen betraut werden, obliegen diesen folgende Rollen und Aufgaben:

- >> **Verantwortung für** im Unternehmen bzw. bei der öffentlichen Stelle gebündelte **Querschnittsprozesse** inkl. der damit verbundenen Dokumentations- und Transparenzpflichten sowie der Gewährleistung von Betroffenenrechten
- >> **Unterstützung der operativen Fachabteilungen** bei der Umsetzung der DS-GVO mit spezifischem Knowhow, z.B. Einkauf in Beschaffungs- und Lieferantenmanagementprozessen; Recht bei der Vertragsprüfung und Datenschutzrechtsfragen; IT-Sicherheit bei der Festlegung und Prüfung von technischen Maßnahmen; Revision bei der Durchführung von (Datenschutz-) Audits; Compliance, Qualitäts- und Risikomanagement beim Managementsystem

Bezogen auf die eigenen Tätigkeiten der MSF treffen diese im Übrigen die datenschutzrechtlichen Verpflichtungen als Fachbereich, vgl. dazu „Punkt 3.2 Operative Fachabteilungen/Geschäftsbereiche".

3.4 Mitarbeiter/-innen

Alle Mitarbeiter/-innen des Unternehmens, der Unternehmensgruppe bzw. der Behörde sind im Rahmen ihres Tagesgeschäfts verpflichtet, die gesetzlichen und internen Regelungen zum Datenschutz einzuhalten und einen angemessenen Schutz personenbezogener Daten zu gewährleisten.

Im Einzelnen obliegen ihnen folgende Pflichten:

- >> **Vertrautmachen mit den internen Regelungen und gesetzlichen Vorschriften zum Datenschutz sowie Einhaltung derselben**, z.B. hinsichtlich Eskalationsmodellen bei Datenpannen
- >> Verpflichtung zur Teilnahme an allen relevanten **Schulungs- und Awarenessmaßnahmen**
- >> effektiver und effizienter **Schutz personenbezogener Daten i.R. des Tagesgeschäfts** auf

Grundlage der geltenden internen Regelungen

- **Löschung** von strukturierten und unstrukturierten Daten entsprechend der Löschkonzepte des Geschäftsbereichs bzw. der Fachabteilung
- **unverzügliche Information** der Führungskraft und der vorgesehenen Meldestellen **bei potenziellen oder tatsächlichen Verstößen gegen den Datenschutz**, z.B. bei unrechtmäßiger Weitergabe oder Missbrauch personenbezogener Daten
- in datenschutzrechtlichen **Zweifelsfällen** stets - und möglichst frühzeitig - die intern vorgesehenen Datenschutzansprechpartner bzw. den/die DSB zurate ziehen

4. Operativ unterstützende Rollen im Datenschutz

4.1 Allgemeines

Die Verantwortung für die operative Umsetzung des Datenschutzes liegt vornehmlich bei der Leitung bzw. den Fachbereichen (siehe Abschnitte 3.1 und 3.2). In der Regel verfügen diese allerdings nicht in vollem Umfang über die notwendigen Ressourcen bzw. das notwendige datenschutzrechtliche Fachwissen, um diese Aufgabe kompetent wahrnehmen zu können. Soweit die Organisationseinheit über eine/-n DSB verfügt, steht diese/-r mit seinem/ihrem Expertenwissen zwar beratend zur Verfügung, die operative Unterstützung oder Umsetzung bleibt ihm/ihr aber im Hinblick auf den gesetzlichen Auftrag verwehrt. **Es ist also unabhängig von der Existenz eines/einer DSB sicherzustellen, dass die Anforderungen des Datenschutzes operativ umgesetzt werden.**

Daher ist es wichtig, dass insbesondere den Fachbereichen im Hinblick auf die Koordination und Umsetzung ihrer operativen Datenschutzaufgaben Hilfestellung gegeben wird. Hierzu sind im Einzelfall insbesondere Kompetenzen aus den Bereichen Organisation, Recht, IT-Sicherheit und Audit bereitzustellen. Diese Kompetenzen können sich – wie im Folgenden dargestellt – auf interne Rollen mit speziellen Datenschutzaufgaben verteilen. Sie können aber auch – quasi im „Nebenjob" – bestehenden internen Ressourcen übertragen werden, wie z.B. die Behandlung von Verträgen oder Datenschutzrechtsfragen der Rechtsabteilung (vgl. dazu auch oben Abschnitt 3.3). Möglich ist auch die Unterstützung durch externe Ressourcen, wie z.B. betreuende Anwaltskanzleien.

Die im Folgenden dargestellten Rollen orientieren sich an den Rollenmodellen in der Unternehmens- und Behördenpraxis. Da es für die Rollen zwar einen praktischen Bedarf, aber keine gesetzliche Regelung gibt, sind die Bezeichnungen nicht verbindlich.

4.2 Datenschutzteam

Um die operativen Fachbereiche bei ihren Datenschutzaufgaben **zu unterstützen** und insbesondere bei komplexen bzw. dezentralen Organisationseinheiten **eine gemeinsame Ausrichtung des Datenschutzes**, den Informationsaustausch und die Kommunikation **zu unterstützen und zu fördern**, kann ein „Datenschutzteam" gebildet werden. Dieses ist gesetzlich nicht definiert und auch eine klar definierte Bezeichnung hat sich bislang nicht etabliert.

Je nach Bedarf können dem Team

- ein/-e zentrale/-r Datenschutzmanager/-in (DSMgr),
- unterstützende Datenschutzexperten/-expertinnen mit spezieller Fachkompetenz,
- dezentral agierende Datenschutzkoordinatoren/-koordinatorinnen (DSK) sowie
- ggf. weitere unmittelbar mit der Steuerung und Umsetzung von Datenschutzanforderungen befasste Funktionsträger/-innen (z.B. aus dem Bereich Informationssicherheit)

angehören.

Abhängig von der konkreten Struktur und dem Bedarf der jeweiligen Organisationseinheit kann ein solches Datenschutzteam **institutionalisiert oder virtuell** gebildet werden.

Soweit ein/-e DSB benannt ist, berät und überwacht diese/-r das operativ agierende Gremium. Die konkrete Zusammenarbeit ist entsprechend zu regeln und zu dokumentieren.

4.3 Datenschutzmanager/-in (DSMgr)

Der/die DSMgr ist **keine gesetzlich definierte Rolle**, insofern finden sich in der Praxis verschiedene Ausgestaltungen. Typischerweise delegiert die Leitung an den/die DSMgr die Wahrnehmung ihrer datenschutzrechtlichen Pflichten. Die **Delegation der Datenschutzverantwortung** wirkt sich allerdings nur im Innenverhältnis aus. Im Außenverhältnis, also im Verhältnis zur betroffenen Person bzw. zur Aufsichtsbehörde bleibt es bei der Verantwortlichkeit der Leitung. **Der Funktion** als DSMgr **können, müssen aber nicht, datenschutzrechtliche Weisungsbefugnisse zugeordnet sein**.

In der Abgrenzung zum/zur Datenschutzkoordinator/-in (DSK) (vgl. dazu im Einzelnen nachstehend unter 4.4) zeichnet sich der/die DSMgr durch eine **übergeordnete, fachbereichsübergreifende Aufgabenstellung** aus. Typischerweise handelt es sich daher um eine zentral angesiedelte Position (Leitung des Datenschutzteams).

Der/die DSMgr hat **keine Stellung als DSB**.

Zu seinen/ihren Aufgaben gehören im Einzelnen:

- >> fachliche **Führung, Steuerung und Weiterentwicklung** der jeweiligen **Datenschutzorganisation**, insbesondere
  - > Verantwortung für die in den Fachbereichen/MSF geltenden **Regelwerke, Prozesse und Tools** für den Datenschutz
  - > **Koordination der fachlichen Unterstützung** der Fachbereiche/MSF in Datenschutzfragen
  - > **Steuerung und Unterstützung der DSK**
  - > **Zusammenarbeit mit dem/der DSB** zur Weitentwicklung der Datenschutzorganisation und zur Nutzung seines/ihres Expertenwissens bei Fachfragen
- >> **Unterstützung bei der organisatorischen und operativen Umsetzung der DS-GVO**, z.B.
  - > **Förderung der Einhaltung der externen und internen Datenschutzvorgaben**
  - > **Pflege und Weiterentwicklung der Datenschutzorganisation**
  - > **Ermittlung potenzieller Datenschutzrisiken** und Entwicklung entsprechender Lösungsvorschläge; Begleitung der Umsetzung
  - > **Erstellung von Vorgaben** zur Erfüllung der Transparenzpflichten und Betroffenenrechte, zur/zum Dienstleisterauswahl, -einsatz und -kontrolle etc.
  - > frühzeitige **Einbindung des/der DSB**
- >> **Kontrolle/Überwachung** und **kontinuierliche Verbesserung** des Datenschutzes
  - > Unterstützung bei Überwachung des Datenschutzes durch die Leitung bzw. den/die DSB, z.B. durch Erstellen von Berichten, Analysen etc.
  - > Unterstützung bei der Implementierung und Durchführung prozessimmanenter Kontrollen
  - > ggf. Durchführung oder Begleitung von Datenschutzaudits
  - > Implementierung eines kontinuierlichen Verbesserungsprozesses und Umsetzung von Maßnahmen
- >> **Untersuchung datenschutzrelevanter Ereignisse** und Initiierung bzw. Umsetzung erforderlicher Maßnahmen sowie Information des/der DSB über Feststellungen
- >> **Koordination der Zusammenarbeit mit der Aufsichtsbehörde**
- >> Organisation, ggf. auch Durchführung von **Schulungen** zum Datenschutz

4.4 Datenschutzkoordinator/-in (DSK)

Der/die DSK ist **keine gesetzlich definierte Rolle**. Die Rolle des/der DSK wird in der Praxis mit unterschiedlicher organisatorischer Anbindung, Fachkunde und unterschiedlichem Aufgabenzuschnitt ausgestaltet. DSK haben keine Stellung als DSB und ihre Einrichtung ist unabhängig von der Benennung eines/einer DSB. DSK bilden die **Schnittstelle** zwischen den Fachbereichen bzw. lokalen Einheiten und den Datenschutzverantwortlichen (Leitung, Fachbereichsverantwortliche, DSMger/-in) sowie dem/der ggf. benannten DSB.

Die DSK-Funktion leitet sich ab aus der dezentralen Verantwortung für den Datenschutz in den Fach-/Geschäftsbereichen, Standorten, Gesellschaften einer Unternehmensgruppe bzw. den Abteilungen von Behörden. Auf Basis von **Checklisten und Mustern** unterstützen DSK die datenverarbeitenden Einheiten und sorgen dafür, dass der Datenschutz bis in diese Bereiche hinein umgesetzt wird.

Der/die DSK kann Mitarbeiter/-in der jeweiligen Organisationseinheit, z.B. aber auch in der zentralen Datenschutzeinheit (Datenschutzteam, vgl. Abschnitt 4.2) **angesiedelt sein**. DSK aus dem Fachbereich haben den Vorteil, dass diese die Prozesse, in denen personenbezogene Daten verarbeitet werden, von fachlicher Seite kennen und mögliche Datenschutzthemen qualifiziert erkennen können. Je nach Komplexität und Heterogenität der Geschäftsprozesse können mehrere DSK benannt werden.

Wesentliche Aufgaben:

- **(dezentraler) Ansprechpartner/-in** der jeweiligen Gesellschaften/Fachbereiche/Abteilungen **zu Datenschutzfragestellungen**
- **Unterstützung der Fachbereiche etc. im Rahmen der Ablauforganisation**, insbes. bei den Schnittstellen zu den Datenschutzprozessen
- **Annahme und Koordination von Anfragen** sowie Weiterleitung von Datenschutzfragestellungen zwecks sachgerechter Unterstützung an die MSF, den/die DSMgr oder den/die DSB
- **operative Unterstützung der Fachbereiche/ Organisationseinheiten bei der Wahrnehmung ihrer Datenschutzverantwortung**, z.B.
  - bei der Dokumentation und Risikobewertung der jeweiligen Verarbeitungstätigkeiten
  - bei der Erfüllung der Transparenz-, Auskunfts-, Melde- und Rechenschafts-/Nachweispflichten sowie bei der Umsetzung von Betroffenenrechten
  - bei Dienstleisterauswahl, -einsatz und -kontrolle
- **frühzeitige Einbindung des/der DSB**
- **Unterstützung bei Kontroll- und Überwachungsmaßnahmen**
  - Durchführung von bzw. Unterstützung bei prozessimmanenten Kontrollen
  - Unterstützung bei der Durchführung von Datenschutzaudits, z.B. durch die Revision oder ähnliche Stellen
  - Erstellen von Berichten und Analysen, Ermittlung von Kennzahlen etc.
  - Unterstützung bei der Umsetzung und Nachverfolgung von kontinuierlichen Verbesserungsmaßnahmen, z.B. aus einem Management Review
- regelmäßige **Berichterstattung über die Risikosituation in den Fachbereichen** an DSMgr und DSB; ggf. Kennzahlen bezüglich aufgetretener Datenschutzvorgänge/-vorfälle
- **Unterstützung bei bzw. Durchführung von Schulungen** und Awarenessmaßnahmen zum Datenschutz
- Unterstützung der Fachbereiche bei Anfragen der Aufsichtsbehörde

4.5 Datenschutzexperten/-expertinnen oder Datenschschutzreferenten/-referentinnen

Je nach Geschäftsausrichtung und Komplexität der Verarbeitungen benennt der Verantwortliche im erforderlichen Umfang „Datenschutzexperten/-expertinnen“ oder „Referenten/Referentinnen“, die das Datenschutzteam **unterstützen**. Diese weisen eine entsprechende **Fachkompetenz** auf.

Datenschutzexperten/-expertinnen oder Referenten/Referentinnen besitzen ebenfalls **keine gesetzlich definierte Rolle**. In der Praxis gibt es verschiedene Ausgestaltungen hinsichtlich der orga-nisatorischen Anbindung. Datenschutzexperten/-expertinnen oder Referenten/Referentinnen können gleichzeitig Mitarbeiter/-innen eines spezifischen Fachbereichs sein wie auch fachlich und disziplinarisch vom bzw. von der DSMgr geführte Mitarbeiter/-innen im Rahmen einer Datenschutzorganisation.

5. Datenschutzbeauftragte/-r (DSB)

Eine **Pflicht zur Benennung** eines/einer DSB ergibt sich dann, **wenn die Kriterien des Art. 37 DS-GVO bzw. § 38 BDSG erfüllt sind**. Unabhängig vom Bestehen einer Verpflichtung kann der Verantwortliche freiwillig eine/-n DSB benennen.[8]

Der/die DSB kann Beschäftigte/-r des Verantwortlichen sein (sog. **„interne/-r" DSB**) oder seine/ihre Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen (sog. **„externe/-r" DSB**)[9]. Eine Unternehmensgruppe bzw. mehrere öffentliche Stellen dürfen unter bestimmten Voraussetzungen eine/-n gemeinsame/-n DSB benennen.[10]

Stellung und (Mindest-)Aufgaben des/der DSB **ergeben sich aus Artt. 38 und 39 DS-GVO**. Der/die DSB kann andere Aufgaben und Pflichten wahrnehmen, solange diese nicht zu einem Interessenkonflikt führen.

Der/die DSB hat u.a. folgende Aufgaben:

- adressatengerechte Information und **Kommunikation** über **Umsetzungs- und Anpassungserfordernisse aus europäischen und nationalen Gesetzgebungen zum Datenschutz** gegenüber Leitung (Accountability), Fachabteilung (Responsibility) sowie Datenschutzteam, DSMgr, DSK[11]
- **Unterrichtung und Beratung** der Leitung, des Datenschutzteams, des/der DSMgr, der DSK, der Fachbereiche/MSF und allgemein aller Mitarbeiter/-innen, die mit der Verarbeitung personenbezogener Daten betraut sind, zu ihren datenschutzrechtlichen Pflichten[12]
- **Initiierung und Überwachung von Maßnahmen zur Sensibilisierung und Schulung** von Mitarbeitern, ggf. auch Konzeption von entsprechenden Maßnahmen (wenn zusätzlich zu den Pflichtaufgaben übertragen)
- Beratung bei Fragen im Zusammenhang mit **Risikobewertungen** von Datenverarbeitungen **und Datenschutz-Folgenabschätzungen** sowie Überwachung ihrer Durchführung[13]
- **Beratung** der Leitung **zur** risikoorientierten **Beauftragung von Datenschutzaudits**
- **Initiierung und Beratung bezüglich des Aufbaus und der Weiterentwicklung eines Datenschutzmanagements**, Koordination von Verbesserungsmaßnahmen
- **Überwachung der Einhaltung der gesetzlichen Vorgaben, der internen Strategien und Vorschriften sowie der Funktionsfähigkeit des Datenschutzmanagements[14]**, z.B. durch Nutzung/Auswertung implementierter Kontrollinstrumente
- **regelmäßige Berichterstattung** über Datenschutzthemen und -risiken an die Leitung, z.B. quartalsweises Reporting, bzw. bei Ad-hoc-Anfragen zu bestimmten Sachverhalten
- **Anlaufstelle für die Aufsichtsbehörde[15] und Zusammenarbeit mit dieser** bei allen Fragen der Verarbeitung personenbezogener Daten[16] (Anm.: Der/die DSB wiederum hat Anspruch auf kostenlose Beratung durch die Behörde.[17])

8 Art. 37 Abs. 4 S. 1 Hs. 1 DS-GVO.
9 Art. 37 Abs. 6 DS-GVO.
10 Art. 37 Abs. 2 und 3 DS-GVO.
11 Art. 39 Abs. 1 lit. a DS-GVO.
12 Art. 39 Abs. 1 lit. a DS-GVO.
13 Art. 39 Abs. 1 lit. c DS-GVO.
14 Art. 39 Abs. 1 lit. b DS-GVO.
15 Art. 39 Abs. 1 lit. e DS-GVO.
16 Art. 39 Abs. 1 lit. d DS-GVO.
17 Art. 39 Abs. 1 lit. e i.V.m. Art. 57 Abs. 3 DS-GVO.

>> **Anlaufstelle**[18] **für die betroffenen Personen** zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der DS-GVO im Zusammenhang stehenden Fragen

>> organisatorische und operative Unterstützung der Fachbereiche/MSF sowie **fachliche Unterstützung des/der DSMgr und der DSK** bei Bedarf und vorhandenen zeitlichen Ressourcen des/der DSB

Der/die DSB ist nicht für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Die Verantwortung für den Datenschutz kann dem/der DSB auch nicht übertragen werden, da sich dieser dann selbst überwachen müsste und es ihm insofern als internem Überwachungsorgan an der notwendigen Unabhängigkeit (ErwGr 97 S. 3 DS-GVO) fehlen würde.

Zu den Voraussetzungen der Benennungspflicht, Aufgaben und Stellung des/der DSB nach der DS-GVO vgl. etwa

GDD-Praxishilfe DS-GVO: „Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung“: https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_i_dsb-nach-ds-gvo_version-2.0

GDD-Ratgeber: „Der betriebliche Datenschutzbeauftragte nach DS-GVO und BDSG, Arbeitshilfe für die betriebliche Praxis“, Version: 2.1

Datenschutzkonferenz, Kurzpapier Nr. 12 „Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern“ (Stand: 17.12.2018), aktuell in Überarbeitung

Leitlinien der *Art-29-Datenschutzgruppe* in Bezug auf Datenschutzbeauftragte („DSB“), WP 243 rev. 01 (bestätigt durch den EDSA am 25.05.2018), abrufbar etwa unter https://datenschutz-hamburg.de/assets/pdf/wp243rev01_de.pdf.

6. Besonderheiten im Konzern

In Konzernen und Unternehmensgruppen mit mehreren juristisch selbstständigen Unternehmen empfiehlt sich die **Einrichtung eines zentralen konzernweit zuständigen Datenschutzteams und** die Einrichtung eines „Konzerndatenschutzes“ mit **Benennung eines/-r „Konzerndatenschutzbeauftragten (KDSB)“** (in der Terminologie der DS-GVO: „gemeinsamer DSB“), um eine konzernweite Datenschutzpolitik/-strategie sowie einheitliche Empfehlungen, Vorgaben und Prozesse in Form von Mindeststandards zu etablieren. Insbesondere vor dem Hintergrund der Bußgeldregelungen der DS-GVO und der Bemessungsgrundlage für die Bußgeldhöhe ist eine konzernweite gemeinsame Ausrichtung im Datenschutz risikominimierend.

Abhängig vom generellen Steuerungs- und Führungsmodell, der Geschäftsstrategie und der Art, Anzahl und regionalen Verteilung der Geschäftseinheiten finden sich **in der Praxis sowohl zentrale als auch dezentrale Organisationsmodelle für den Konzerndatenschutz.** In beiden Modellen kann - soweit rechtlich zulässig[19] - ein/-e KDSB die Rolle und die Aufgaben des/der DSB in den einzelnen Tochterunternehmen übernehmen. Dann ist

18 Art. 38 Abs. 4 DS-GVO.

19 Vgl. Art. 37 Abs. 3 DS-GVO.

ihm/ihr entsprechend der oben unter Ziff. 5 aufgeführte Aufgabenkreis zugeordnet.

Es können jedoch auch eigene DSB in den einzelnen Tochterunternehmen benannt werden. Dann nimmt der/die KDSB primär (konzerninterne) steuernde und koordinierende Aufgaben wahr, hat aber für die Unternehmen mit eigenem DSB nicht die entsprechende gesetzliche Rolle.

Die Umwandlung von einer dezentralen Organisation mit personenverschiedenen Datenschutzbeauftragten bei den verschiedenen Unternehmen hin zu einer zentralen Organisation mit nur einem/einer Konzerndatenschutzbeauftragten setzt regelmäßig das Einverständnis der einzelnen benannten Beauftragten voraus. Nach dem BAG[20] begründet allein die Organisationsentscheidung, den Datenschutz konzernweit vereinheitlichen zu wollen, keinen wichtigen Grund i.S.v. § 626 BGB.

Mögliche Aufgaben des Konzerndatenschutzes:

- **Koordination und Förderung von Zusammenarbeit und Abstimmung** zu allen Fragen des Datenschutzes im Konzern bzw. in der Unternehmensgruppe
- **Information und Beratung der Konzernholding/Gruppenleitung** zu aktuellen Entwicklungen im Datenschutzrecht, der Einhaltung und Umsetzung datenschutzrechtlicher Anforderungen im Konzern bzw. in der Gruppe **sowie Formulierung von (konzern-/gruppenweiten) Empfehlungen**
- **Etablierung und Weiterentwicklung konzern-/gruppenweiter Empfehlungen** zur Datenschutzpolitik/-strategie, Strukturen, Regelwerken, Prozessen und Tools **im Rahmen eines konzern-/gruppenweiten Datenschutzmanagementsystems**
- **Definition und Implementierung eines regelmäßigen Reportings** zur Verfolgung des Reifegrads des Datenschutzes, des Datenschutzmanagements und der Datenschutzorganisation
- **Koordination der Arbeit der DSBs** in den Unternehmen **und** - sofern implementiert - **des Datenschutzteams**
- **Koordination eines regelmäßigen Informationsflusses und -austausches** sowie einer effizienten und effektiven Einbindung der dezentralen Datenschutzressourcen

Weitere mögliche Regelungen im Rahmen des Konzerndatenschutzes:

- **Benennung eines/einer KDSB** durch die Konzernholding/Gruppenleitung
- ggf. Benennung des/der KDSB auch als DSB für die dezentralen Unternehmen des Konzerns- bzw. der Unternehmensgruppe
- bei der Benennung eines eigenen DSB durch die dezentralen Unternehmen sinnvollerweise vorherige Konsultation des KDSB
- **Regelung von Steuerungs- und Koordinationsaufgaben des/der KDSB unter Berücksichtigung der Weisungsfreiheit ggf. benannter einzelner DSBs** sowie ggf. operativen Aufgaben im Konzern-/Gruppenkontext (z.B. gesellschaftsübergreifende Projekte, IT-Systeme oder Dienstleisterverträge)
- Der/die KDSB ist rechtzeitig zu allen Angelegenheiten hinzuzuziehen, die sich auf den Schutz personenbezogener Daten mit potenziell unternehmensübergreifender oder konzernweiter Auswirkung beziehen. Dies gilt in besonderem Maße bei offiziellen Kontakten zu Datenschutzbehörden oder anderen Institutionen.
- Der/die KDSB ist unverzüglich zu informieren bzw. hinzuzuziehen, sobald sich ein Datenschutzverstoß oder sonstiger **Vorfall mit möglichen Auswirkungen auf den Datenschutz von größerer lokaler, übergreifender oder konzernweiter Bedeutung** ereignet.

20 BAG v. 23.3.2011 - 10 AZR 562/09.

7. Besonderheiten im Hinblick auf kleinere und mittlere Unternehmen (KMUs)

Die Größe einer Datenschutzorganisation und die Anzahl der mit dem Datenschutz befassten Personen muss in einem angemessenen Verhältnis zur Größe der Gesamtorganisation und zu der Kritikalität der durchgeführten Verarbeitungen personenbezogener Daten stehen. Selbstverständlich kann nicht jedes kleine produzierende Unternehmen ein eigenes Team mit der Unterstützung der operativen Umsetzung des Datenschutzes betrauen. Ohnehin setzt effektiver operativer Datenschutz nicht zwingend eine personelle bzw. organisatorische Verkörperung voraus, z.B. in Form eines/einer DSMgr.

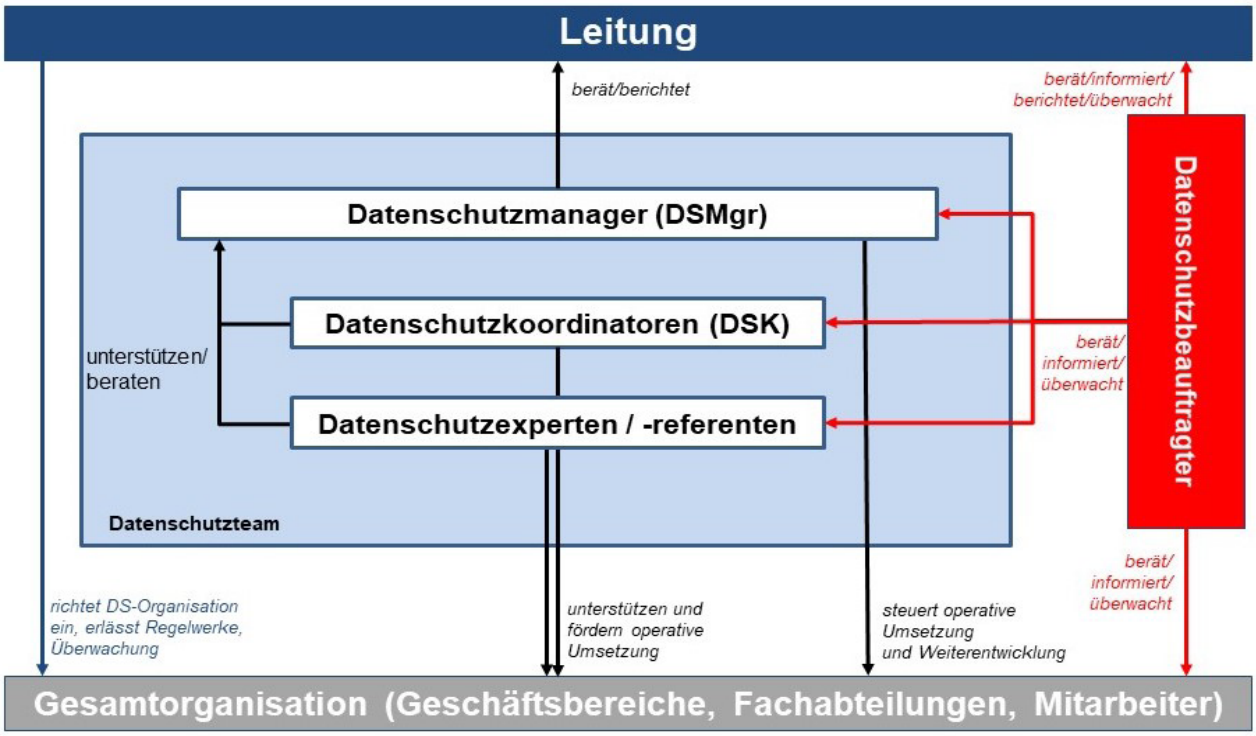
Entscheidend ist nicht das Ausmaß der Datenschutzorganisation, sondern das Ausmaß der Organisation des Datenschutzes.

Die Verantwortung für die Umsetzung des Datenschutzes liegt im Ausgangspunkt bei der Leitung bzw. – im Wege der Delegation – **bei den im Einzelnen für die Verarbeitungen zuständigen Fachabteilungen**. Ist ein/-e DSB benannt, gehört es zu seinen/ihren Aufgaben, Leitung und Fachabteilungen mittels seiner/ihrer Expertise im Hinblick auf die organisatorische und operative Umsetzung des Datenschutzes zu beraten.

8. Zusammenfassung

Eine zusammenfassende synoptische Darstellung zu den Verantwortlichkeiten und Aufgaben nach der DS-GVO finden Sie auf den nachfolgenden Seiten. Grafisch lässt sich das in dieser Praxishilfe dargestellte Konzept wie unten abgebildet zusammenfassen:

Es handelt sich hierbei um ein Modell, das im Hinblick auf unterschiedliche Einflüsse anzupassen ist, insbes. Größe der Organisationseinheit, Umfang und Kritikalität der Datenverarbeitung. Gerade in kleineren Stellen können mehrere Rollen zusammenfallen oder sind extern zu besetzen.



Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung (DS-GVO)

Nachfolgend werden die einzelnen Verantwortlichkeiten und Aufgaben zur wirksamen Umsetzung der DS-GVO, wie sie als Modell in der GDD-Praxishilfe DS-GVO: "Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung" im Detail erläutert werden, in Form einer Tabelle dargestellt. Dabei werden die einzelnen Aufgaben nach Themenbereichen geordnet und zur Verdeutlichung der Abgrenzung je Rolle nebeneinander dargestellt.

Themenbereich	Leitung	Fachbereich	MSF	DSMgr	DSK	DSB
Allg. Verantwortung	**Accountability** **Gesamtverantwortung für den Datenschutz,** Verantwortung insbes. für - wirksame Umsetzung von DS-GVO/BDSG - Einhaltung der Grundprinzipien des Datenschutzes gem. DS-GVO - Nachweis der Einhaltung durch entsprechende Dokumentation („Rechenschaftspflicht“ gemäß Art. 5 Abs. 2, Art. 24 DS-GVO) - Vertretung des Unternehmens / der öffentlichen Stelle nach außen - Bereitstellung erforderlicher finanzieller, sachlicher und personeller Ressourcen	**Responsibility** **Durchführungsverantwortung**, d.h. Ausführung der Anweisungen der Leitung zur Umsetzung der DS-GVO	**Support** **Verantwortung für** im Unternehmen bzw. bei der öffentlichen Stelle gebündelte **Querschnittsprozesse** inkl. der damit verbundenen datenschutzrechtlichen Anforderungen (Dokumentations- und Transparenzpflichten sowie Gewährleistung von Betroffenenrechten)	**Support** Fachliche **Führung, Steuerung und Weiterentwicklung der Datenschutzorganisation**, insbes. - Verantwortung für in den Fachbereichen/ MSF geltende Regelwerke, Prozesse und Tools für den Datenschutz inkl. deren kontinuierlicher Weiterentwicklung - Koordination der fachlichen Unterstützung der Fachbereiche/MSF in Datenschutzfragen - Steuerung und Unterstützung der DSK - Zusammenarbeit mit dem/der DSB zwecks Weitentwicklung der Datenschutzorganisation und Nutzung seines/ihres Expertenwissens bei Fachfragen	**Support** **(dezentrale/r) Ansprechpartner/in** im jeweiligen Unternehmen/Fachbereich **zu Datenschutzfragestellungen**	**Consulting** Gesetzlicher Auftrag zur **Unterrichtung (proaktiv) und Beratung (idR reaktiv)** über Umsetzungs- und Anpassungserfordernisse aus der europäischen und nationalen Gesetzgebung zum Datenschutz, insbes. gegenüber - Leitung - DSMgr - Fachbereichen/MSF **Überwachung der Einhaltung der gesetzlichen Vorgaben, internen Strategien und Vorschriften sowie der Funktionsfähigkeit des Datenschutzmanagements**, z.B. durch Nutzung/Auswertung implementierter Kontrollinstrumente
Datenschutzorganisation	**Einrichtung/Aufrechterhaltung einer Datenschutzorganisation**, durch die Datenschutzfachkunde mittels interner oder externer	**Arbeitsplatzbezogene Instruktion** der einzelnen Mitarbeiter	Soweit selbst als Fachbereich betroffen, siehe Spalte „Fachbereich“	Pflege/Weiterentwicklung der **Regelungen zur Datenschutzorganisation**	Unterstützung der Fachbereiche im Rahmen der **Ablauforganisation**,	**Fachliche Unterstützung** – insbes. des/der DSMgr – bei der (Weiter-)Entwicklung der Datenschutzorganisation

Themenbereich	Leitung	Fachbereich	MSF	DSMgr	DSK	DSB
	Ressourcen sicher verfügbar gemacht wird (Vermeidung von Selektionsverschulden) **Benennung eines/einer DSB, soweit gesetzlich erforderlich** bzw. sinnvoll			**Förderung der Einhaltung der** im Unternehmen bzw. bei der öffentlichen Stelle **geltenden externen und internen Vorgaben**	insbes. bei den Schnittstellen zu den Datenschutzprozessen	
Allg. operative Aufgaben	**Delegation/Bestimmung von Aufgaben und Verantwortlichkeiten (Rollen)** in der Aufbau- und Ablauforganisation mittels Anweisungen, z.B. - Leitlinien - Richtlinien/Policies - Arbeitsanweisungen (Vermeidung von Anweisungsverschulden) Implementierung **angemessener Datenschutzprozesse**	Der Fachbereich trägt die **Prozessverantwortung,** woraus insbes. folgende Aufgaben resultieren: - **Definition der organisatorischen Schnittstellen (auch zum Datenschutz), insbes. Anbindung an Datenschutzprozesse** - Erfüllung von **Dokumentationspflichten,** z.B. Erstellung/Pflege des Verzeichnisses der Verarbeitungstätigkeiten (VVT) und Nachweis der Einwilligung - **Verantwortung für datenschutzrechtliche Risikobewertung** (inkl. der Datenschutz-Folgenabschätzung, sofern erforderlich) - Vermeidung datenschutzrechtlicher Risiken durch Prozess-,	**Unterstützung der operativen Fachbereiche** bei der Umsetzung der DS-GVO **mit spezifischem Knowhow**, z.B.: - **Einkauf** in Beschaffungs- und Lieferantenmanagementprozessen - **Recht** bei der Vertragsprüfung und bei Datenschutzrechtsfragen - **IT-Sicherheit** bei der Festlegung/Prüfung von technischen Maßnahmen - **Revision** bei der Durchführung von (Datenschutz-)Audits - **Compliance, Qualitäts- und Risikomanagement** beim Managementsystem	**Unterstützung bei der organisatorischen und operativen Umsetzung der DS-GVO:** - **Ermittlung potenzieller Datenschutzrisiken** - Entwicklung entsprechender **Lösungsvorschläge** und Begleitung der Umsetzung - **Koordination der DSK sowie unterstützender Datenschutzexperten/-expertinnen** - frühzeitige **Einbindung des/der DSB**	**Unterstützung der Fachbereiche** bei der Wahrnehmung ihrer Datenschutzverantwortung, insbes. durch - **Annahme und Koordination von Anfragen** sowie Weiterleitung von Datenschutzfragestellungen der Fachbereiche zwecks sachgerechter Unterstützung an die MSF, den/die DSMgr oder den/die DSB - **operative Unterstützung** bei der Dokumentation und Risikobewertung von Verarbeitungstätigkeiten der jeweiligen Geschäftseinheit bzw. des jeweiligen Fachbereichs - frühzeitige **Einbindung des/der DSB**	**Unterrichtung/Beratung** der Leitung und aller Mitarbeiter/-innen, die mit der Verarbeitung personenbezogener Daten betraut sind, zu datenschutzrechtlichen Pflichten **Beratung** bei Fragen im Zusammenhang mit **Risikobewertungen** von Datenverarbeitungen und **Datenschutz-Folgenabschätzungen** (sowie Überwachung ihrer Durchführung) **Fachliche Unterstützung** des/der DSMgr und der DSK bei Bedarf

Themenbereich	Leitung	Fachbereich	MSF	DSMgr	DSK	DSB
		Produkt- und Technikgestaltung, sofern möglich (data protection by design/default, Löschkonzept usw.) - frühzeitige **Einbindung des/der DSB (erfolgskritischer Faktor!)**	Soweit selbst als Fachbereich betroffen, siehe Spalte „Fachbereich“			
Transparenzpflichten/ Betroffenenrechte	Anweisung **angemessener Datenschutzprozesse**, insbes. auch für Betroffenenrechte und Datenpannen **Festlegung der Rahmenbedingungen für Datenschutzinformationen** gegenüber den betroffenen Personen	**Erfüllung der Transparenz- und Informationspflichten** **Gewährleistung der Betroffenenrechte** (Anbindung an vorhandene Prozesse bzw. Entwicklung eigener Prozesse für Auskunft, Löschung, Berichtigung, Recht auf Vergessenwerden, Datenportabilität, Einwilligungswiderruf, Widerspruch und Datenpannen)	**Unterstützung der operativen Fachbereiche mit spezifischem Knowhow**, vgl. Zeile zu den *allgemeinen Aufgaben der MSF* Soweit selbst als Fachbereich betroffen, siehe Spalte „Fachbereich“	**Erstellung von Vorgaben** zur Erfüllung von Transparenzpflichten und Betroffenenrechten **sowie Förderung ihrer Einhaltung**	**Operative Unterstützung der Fachbereiche** bei - **Erfüllung von Nachweispflichten** im Zusammenhang mit den Transparenz-, Auskunfts-, Melde- und Rechenschaftspflichten - **Umsetzung von Transparenzpflichten/Betroffenenrechten**	**Anlaufstelle für betroffene Personen** zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der DS-GVO im Zusammenhang stehenden Fragen **Fachliche Unterstützung (Beratung)** bei Bedarf, insbes. des/der DSMgr und der DSK
Dienstleister/ Geschäftspartner	Anweisung **angemessener Datenschutzprozesse**, insbes. auch für die Beauftragung von Dienstleistern und Zusammenarbeit mit Dritten	**Sicherstellung von wirksamen und datenschutzkonformen Vertragsbeziehungen** mit den ausgewählten Verarbeitern personenbezogener Daten, z.B. - Auftragsverarbeiter nach Art. 28 DS-GVO	**Unterstützung der operativen Fachbereiche mit spezifischem Knowhow**, vgl. Zeile zu den *allgemeinen Aufgaben der MSF* Soweit selbst als Fachbereich betroffen, siehe Spalte „Fachbereich“	**Erstellung von Vorgaben zum Einsatz zuverlässiger Dienstleister**, die insbes. gewährleisten, dass - angemessene technische und organisatorische Maßnahmen umgesetzt werden	**Operative Unterstützung der Fachbereiche**, insbes. bei - **Auswahl und Einsatz von Auftragsverarbeitern** - **Kontrolle von Auftragsverarbeitern**	**Fachliche Unterstützung (Beratung)** bei Bedarf, insbes. des/der DSMgr und der DSK

Themenbereich	Leitung	Fachbereich	MSF	DSMgr	DSK	DSB
		- Geschäftspartner im Rahmen der gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO **Kontrolle der Auftragsverarbeiter**		- die Verarbeitung allen datenschutzrechtlichen Anforderungen genügt - der Schutz der Betroffenenrechte gewährleistet ist **Erstellung von Vorgaben für die Kontrolle der Dienstleister**		
Schulungen	**Anweisung angemessener Schulungen und Awarenessmaßnahmen** zum Datenschutz	**Durchführung fachbereichsspezifischer Schulungs- und Awarenessmaßnahmen**	**Unterstützung der operativen Fachbereiche mit spezifischem Knowhow**, vgl. Zeile zu den *allgemeinen Aufgaben der MSF* Soweit selbst als Fachbereich betroffen, siehe Spalte „Fachbereich“	**Organisation, ggf. auch Durchführung von Schulungen und Awarenessmaßnahmen** zum Datenschutz	**Unterstützung bei bzw. Durchführung von Schulungen und Awarenessmaßnahmen** zum Datenschutz	**Initiierung eines Konzeptes zur Schulung und Sensibilisierung** **Ggf. auch Konzeption** der Schulungs- und Sensibilisierungsmaßnahmen, sofern der/die DSB über die notwendigen zeitlichen Ressourcen verfügt und diese Aufgabe zusätzlich übertragen wird **Überwachung**, dass Verpflichtung zur Schulung und Sensibilisierung in angemessenen Umfang nachgekommen wird
Kontrolle/Überwachung und kontinuierliche Verbesserung	**Sicherstellung ordnungsgemäßer Überwachung** der datenschutzrelevanten Prozesse durch Einrichtung ausreichender Kontrollmechanismen und -systeme	**Implementierung und Durchführung geeigneter prozessimmanenter Kontrollen** zur Gewährleistung der Einhaltung der gesetzlichen und internen Vorgaben zum Datenschutz	**Unterstützung der operativen Fachbereiche mit spezifischem Knowhow**, vgl. Zeile zu den *allgemeinen Aufgaben der MSF*	**Unterstützung bei Implementierung/Durchführung prozessimmanenter Kontrollen** **Untersuchung datenschutzrelevanter Ereignisse** und Initiierung	**Durchführung von bzw. Unterstützung bei prozessimmanenten Kontrollen** **Unterstützung bei** der Verfolgung und Umsetzung von kontinuierli-	Gesetzlicher **Überwachungsauftrag**; hieraus ergeben sich insbes. folgende Aufgaben: - **Beratung** der Leitung **bezüglich der risikoorientierten Beauf-**

Themenbereich	Leitung	Fachbereich	MSF	DSMgr	DSK	DSB
	(Vermeidung von Überwachungsverschulden) **Initialisierung/Beauftragung von Audits** **Anweisungen zur Umsetzung von Empfehlungen/Feststellungen** aus Kontrollen und Überwachungen	**Regelmäßige Überprüfung und** erforderlichenfalls **Anpassung** der Datenschutzmaßnahmen **mit dem Ziel der kontinuierlichen Verbesserung**	Soweit selbst als Fachbereich betroffen, siehe Spalte „Fachbereich“	bzw. Umsetzung erforderlicher Maßnahmen **Implementierung eines kontinuierlichen Verbesserungsprozesses** und Umsetzung von Maßnahmen Ggf. Durchführung/Begleitung von **Datenschutzaudits** Unterstützung bei Überwachung des Datenschutzes durch die Leitung bzw. den/die DSB, z.B. durch **Erstellung von Berichten, Analysen** etc.	chen **Verbesserungsmaßnahmen** Unterstützung bei Überwachung des Datenschutzes, z.B. durch **Ermittlung und Bericht von Kennzahlen, Analysen** etc.	**tragung von Datenschutzaudits** - **kontinuierliche Überwachung der Einhaltung der Datenschutzvorgaben** durch Nutzung/Auswertung der Kontrollinstrumente - **Reporting** auf Grundlage der Kontrollinstrumente an die Leitung
Berichte/Reporting	**Sicherstellung eines Reportingsystems** im Rahmen der Überwachung der Einhaltung des Datenschutzes Regelmäßiger **Informationsaustausch** mit dem/der DSB **Anweisungen zur Umsetzung von Empfehlungen** zur Weiterentwicklung	**Unterstützung** – insbes. des/der DSMgr und des/der DSB – **bei Berichts- und Reportingmaßnahmen**	**Unterstützung der operativen Fachbereiche mit spezifischem Knowhow**, vgl. Zeile zu den *allgemeinen Aufgaben der MSF* Soweit selbst als Fachbereich betroffen, siehe Spalte „Fachbereich“	**Erstellen von Berichten gegenüber der Leitung** **Information des/der DSB** über Feststellungen	Regelmäßige **Berichterstattung** über die Risikosituation in den Fachbereichen **an DSMgr und DSB**; ggf. Kennzahlen aufgetretener Datenschutzvorgänge und -vorfälle	Regelmäßige **Berichterstattung** über Datenschutzthemen und -risiken an die Leitung
Aufsichtsbehörde	**Vertreter/-in des Verantwortlichen bzw. Auftragsverarbeiters gegenüber der Aufsichtsbehörde** (Normadressat und, soweit kein/e DSB	**Unterstützung** der Datenschutzorganisation **bei der Zusammenarbeit mit der Aufsichtsbehörde**	**Unterstützung der operativen Fachbereiche mit spezifischem Knowhow**, vgl. Zeile zu den *allgemeinen Aufgaben der MSF*	**Koordination der Zusammenarbeit mit der Aufsichtsbehörde**	**Unterstützung der Fachbereiche bei Anfragen der Aufsichtsbehörde**	**Anlaufstelle** für die Aufsichtsbehörde bei allen Fragen der Verarbeitung personenbezogener Daten

Themenbereich	Leitung	Fachbereich	MSF	DSMgr	DSK	DSB
	benannt ist, alleinige Anlaufstelle für die Behörde) **Auskunftspflichtig** Verantwortlich für die Umsetzung aufsichtsbehördlicher Anweisungen	**Verantwortlich insbes. für die Sachverhaltsaufklärung/-darstellung sowie für relevante Dokumentationen** zur Zusammenarbeit mit der Aufsichtsbehörde	Soweit selbst als Fachbereich betroffen, siehe Spalte „Fachbereich“			**Verpflichtung zur Zusammenarbeit** mit dieser **Beratung** nach Bedarf von Leitung, DSMgr, Fachbereich, MFS **hinsichtlich Anfragen oder Anordnungen der Aufsichtsbehörde** **Beratung** des/der DSB **durch die Aufsichtsbehörde**

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

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt unter Mitwirkung von:

> Uwe Bargmann (Berater Datenschutzmanagement)
> Thomas Müthlein (DMC - Datenschutz Management & Consulting, GDD-Vorstand)
> Yvette Reif, LL.M. (GDD-Geschäftsstelle)

Ansprechpartnerin: RAin Yvette Reif, LL.M.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Stand: Version 2.0 (August 2021)