# 1. Einleitung

Mit der Datenschutzgrundverordnung (DS-GVO) vollzieht sich aus deutscher Sicht eine grundsätzliche Änderung bei der Organisation des Datenschutzes. Während noch unter dem Bundesdatenschutzgesetz in der bis zum 25. Mai 2018 gültigen Fassung (BDSG alt) sowohl die verantwortliche Stelle, also das Unternehmen oder die Behörde, als auch deren Datenschutzbeauftragter für Organisation und Umsetzung des Datenschutzes zum Teil gemeinsam zuständig waren, werden die Aufgaben der verantwortlichen Stelle und des Datenschutzbeauftragten durch die DS-GVO klar gegeneinander abgegrenzt. Damit einher geht auch eine neue Aufgabenbeschreibung des Datenschutzbeauftragten.

**Der verantwortlichen Stelle obliegt es, in eigener Verantwortung die Umsetzung und Sicherstellung des Datenschutzes zu organisieren und zu kontrollieren.**

Die Aufgabenstellung des Datenschutzbeauftragten wird durch die DS-GVO dagegen vollkommen von operativen Aufgaben entflochten. Ihm verbleibt **die Aufgabe, die verantwortliche Stelle hinsichtlich ihrer Datenschutzaufgaben zu unterstützen**. Hierzu hat er ihr beratend zur Seite zu stehen und zu überwachen, ob die ergriffenen Maßnahmen zur Einhaltung der datenschutzrechtlichen Vorgaben wirksam sind.

Diese – zumindest aus deutscher Sicht – neue Aufgabenteilung ist dem Umstand geschuldet, dass der Datenschutzbeauftragte im Konstrukt der DS-GVO „lediglich“ eine Option darstellt, die bei weitem nicht für alle Normadressaten der DS-GVO verpflichtend ist. D.h. aber auch im Umkehrschluss, die Datenschutzorganisation **muss auch ohne Datenschutzbeauftragten** voll funktionstüchtig, wirksam und so kontrolliert funktionieren, dass sie Fehler aufdeckt und Prozesse verbessert.

Damit rückt der Datenschutzbeauftragte hinsichtlich seiner neu zu definierenden Überwachungsfunktion näher in Richtung einer Aufgabenstellung, die mit der einer Aufsichtsbehörde vergleichbar ist, ohne dass er über deren Sanktionsmittel verfügt oder solche gebrauchen soll. Im Gegenteil, seine Überwachungstätigkeit soll dazu beitragen, die verantwortliche Stelle hinsichtlich ihrer datenschutzrechtlichen Pflichten, zu denen auch die Sicherstellung der wirksamen Umsetzung der Vorgaben des Datenschutzes gehört, zu unterstützen.

Die Datenschutzbeauftragten in Deutschland sahen in der Vergangenheit den Schwerpunkt ihrer Tätigkeit in der Beratungstätigkeit bei den strategischen und operativen Datenschutzfragen der verantwortlichen Stellen. Nunmehr wird durch Bußgeldandrohung auch für die Tätigkeit des Datenschutzbeauftragten sowohl für die verantwortliche Stelle als auch für den Datenschutzbeauftragten die Herausforderung darin bestehen, wirksame Überwachungskonzepte zu entwickeln und umzusetzen. Wie man sich diesem Tätigkeitsfeld unter den Prämissen der DS-GVO nähern kann, soll im Folgenden diskutiert und Lösungsansätze aufgezeigt werden.

# 2. Verantwortung und Accountability

Zentraler Punkt für die Umsetzung des Datenschutzes in Wirtschaft und Verwaltung ist die Rechenschaftspflicht, auch Accountability genannt, der verantwortlichen Stelle. Hierüber ist die verantwortliche Stelle gehalten, nachweisen zu können, ob sie rechtmäßig Daten verarbeitet (siehe Art. 5 DS-GVO) bzw. dass sie sich datenschutzkonform organisiert hat (siehe Art. 24 DS-GVO).

Bereits die Art. 29 Gruppe hat die Rechenschaftspflicht/ Accountability im WP 173[1] wie folgt beschrieben:

> *„Allgemein gesagt drückt er [der Begriff „Accountability"] … aus, wie Verantwortung überprüfbar wahrgenommen wird. Verantwortung und Rechenschaftspflicht sind zwei Seiten einer Medaille und wesentliche Bestandteile der Good Governance."*

Vor diesem Hintergrund ist zunächst zu klären, welche Verantwortung im Datenschutz ein Unternehmen bzw. eine Behörde trifft und wie sie umzusetzen ist.

Wie bei jeder anderen gesetzlichen Auflage für ein Unternehmen oder eine Behörde ist diese Organisationseinheit zunächst als Ganzes Normadressat. D.h. derjenige, der diese Organisationseinheit vertritt, muss dafür sorgen, dass die Verpflichtungen der betreffenden Normen in der Organisation umgesetzt werden. Mit anderen Worten: Die Unternehmens- bzw. Behördenleitung muss die aus den Normen entstehenden Pflichten erkennen und so in der Organisation delegieren, dass sie wirksam umgesetzt werden.

Tut sie dies nicht, trifft sie ein **Organisationsverschulden**[2]. Dies kann bis hin zu einer persönlichen Haftung der Leitungsorgane führen. Beim Organisationsverschulden wird nach folgenden Formen unterschieden:

- ⇨ **Selektionsverschulden:** die Verantwortung wird an ungeeignete Mitarbeiter delegiert;
- ⇨ **Anweisungsverschulden:** Arbeitsanweisungen fehlen, sind fehlerhaft oder lückenhaft;

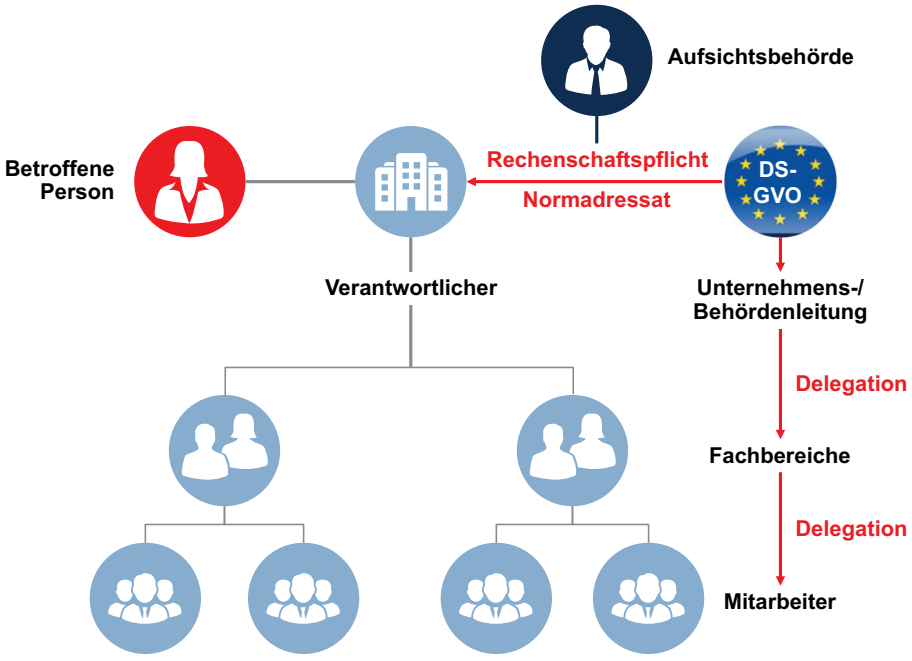


**Abb. 1:** Umsetzung gesetzlicher Pflichten



1. Artikel-29-Datenschutzgruppe (Art. 29 Gruppe), WP 173 vom 13.07.2010, Stellungnahme 3/2010 zum Grundsatz der Rechenschaftspflicht
2. D.h., es wird versäumt, allgemeine organisatorische Anordnungen zu treffen

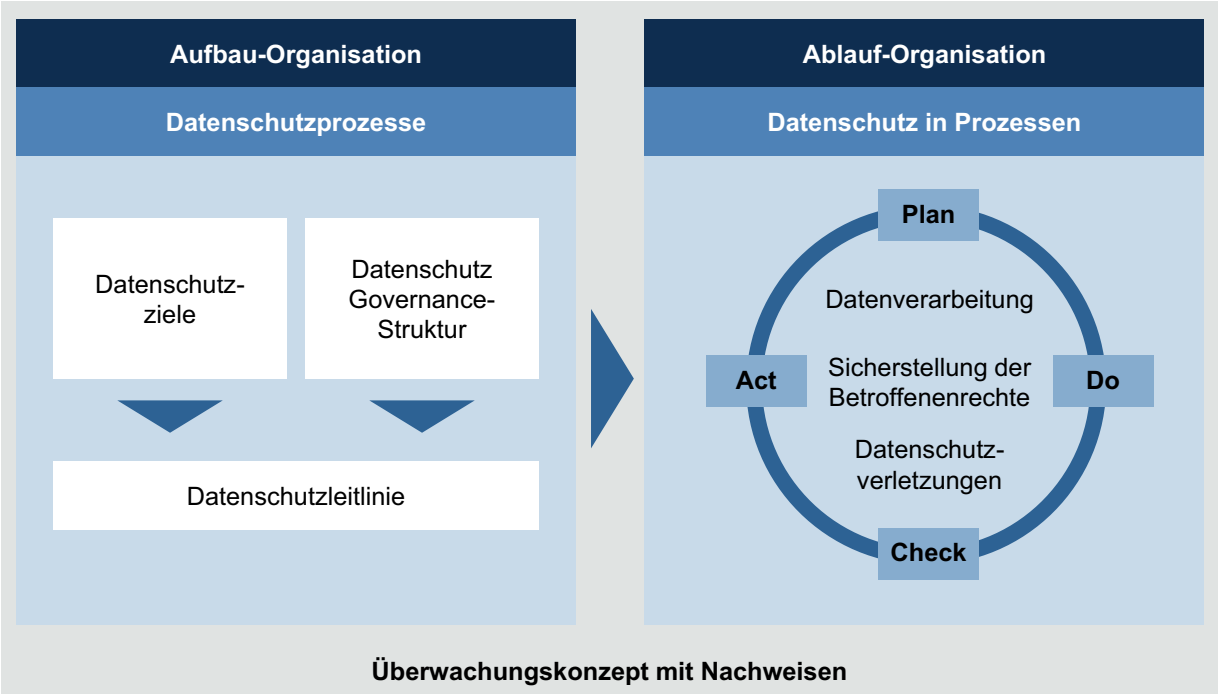


**Abb. 2:** Umsetzung der Rechenschaftspflicht der DS-GVO



⇨ **Überwachungsverschulden:** Kontrollen werden gar nicht oder lückenhaft durchgeführt.

Die Einbeziehung des „Überwachungsverschulden" in das Organisationsverschulden bedeutet zum einen, dass es nicht ausreicht, Verantwortung lediglich zu delegieren und Anweisungen zu schreiben, sondern es auch erforderlich ist, dass die Wahrnehmung der Verantwortung und die Einhaltung der Anweisungen systemimmanent kontrolliert werden. Das heißt zunächst, dass solche Kontrollen zu bestimmen und durchzuführen sind. Darüber hinaus erstreckt sich das „Überwachungsverschulden" auch darauf, dass die Kontrollen nicht oder nur lückenhaft durchgeführt werden. Daraus ergibt sich, dass die Leitungsorgane sicherzustellen – also zu überwachen – haben, dass die vorgesehenen Kontrollen auch funktionieren.

Überträgt man diese Ansätze auf die DS-GVO, ergibt sich folgendes Szenario:

Im Rahmen der Aufbauorganisation sind durch eine Datenschutzleitlinie und konkretisierende Datenschutzrichtlinien besonders für zentrale Datenschutzprozesse Verantwortlichkeiten und Vorgehensweisen zur Umsetzung des Datenschutzes zu regeln (s. a. Kap. 5 „Zielsetzung und Gegenstand der Überwachung"). Zuständig hierfür ist die jeweilige Unternehmens- bzw. Behördenleitung (s. insbes. Vermeidung des Selektions- bzw. Anweisungsverschuldens).

Im Rahmen der Ablauforganisation ist sicherzustellen, dass insbesondere in den Fachprozessen diese Vorgaben eingehalten werden und die Anbindung an die zentralen Datenschutzprozesse sichergestellt ist. Darüber hinaus ist über das gesamte System ein nachweisbares Überwachungskonzept zur Vermeidung des Überwachungsverschuldens zu etablieren (s. a. Kap. 7.7„ Überwachungskonzept"). Was die hierzu festzulegenden Kontrollen sowie die Überwachung ihrer Wirksamkeit angeht, hat sich bezüglich der Sicherstellung der Einhaltung anderer, insbesondere gesetzlicher, Vorgaben die Begrifflichkeit eines „internen Kontrollsystems" oder kurz: „IKS"[3] etabliert.

3. Das interne Kontrollsystem wird laut „Gabler Wirtschaftslexikon" wie folgt definiert: *„Das interne Kontrollsystem ist ein Teilsystem des Systems zur Überwachung einer Unternehmung, das die Gesamtheit der Mechanismen zur Kontrolle enthält."*, *https://wirtschaftslexikon.gabler.de/definition/internes-kontrollsystem-iks-41197*

Im Bereich des Datenschutzes nach DS-GVO tritt neben dieses interne Kontrollsystem eine weitere Schicht, die aus unterschiedlichen Motivationen einen Blick auf die Wirksamkeit der Datenschutzorganisation hat:

- **Aufsichtsbehörden:** haben den gesetzlichen Auftrag, die Einhaltung des Datenschutzes in Unternehmen zu überwachen – **Fremdkontrolle**
- **Betroffene bzw. Verbände:** Betroffene können selbst durch Ausübung ihrer Rechte Einfluss und Kontrolle auf die Datenverarbeitung ausüben. Dies kann auch durch Überleitung ihrer Rechte auf entsprechende Verbände geschehen – **Selbstkontrolle**
- **Betriebsrat:** gesetzlicher Auftrag zur Überwachung der Einhaltung von Gesetzen zum Schutze von Arbeitnehmern. Hierzu zählen auch Datenschutzgesetze. Ein Betriebsrat ist nur dann zu gründen, wenn bestimmte gesetzliche Voraussetzungen hierzu vorliegen oder er auf freiwilliger Basis gegründet wird. Insoweit ist er optional.
- **Datenschutzbeauftragter:** als Teil der verantwortlichen Stelle mit der Beratung hinsichtlich der Datenschutzpflichten und Überwachung der Einhaltung des Datenschutzes durch Gesetz beauftragt. Seine Benennung ist nur dann verpflichtend, wenn bestimmte gesetzliche Voraussetzungen vorliegen oder er freiwillig bestellt wird. Insofern ist er optional – **innerbetriebliches Überwachungsorgan**.

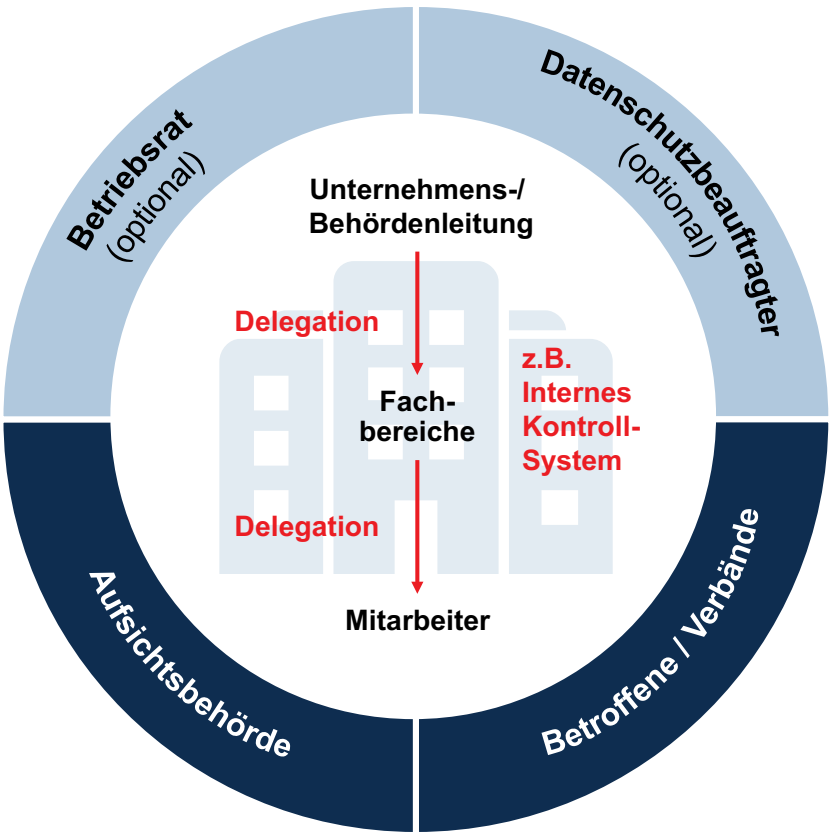


**Abb. 3:** Überwachung

# 3. Datenschutz und Risikomanagement

Die Einhaltung oder – besser – die Nichteinhaltung insbesondere gesetzlicher Vorgaben stellt für Unternehmen ein Risiko dar. Um diesen Risiken gerecht zu werden, gibt es verschiedene Modelle zum Risikomanagement. Dabei handelt es sich in der Regel um Risikomanagementmodelle, die unabhängig vom Datenschutz meist in Richtung der Vermeidung – finanzieller – Schäden für das betroffene Unternehmen bzw. die betroffene Behörde entwickelt wurden.

Ein solches gängiges Modell zur Organisation des Risikomanagements ist das vom Dachverband der europäischen Revisionsinstitute (ECCIA) bereits 2010 herausgegebene Corporate-Governance-Modell der drei Verteidigungslinien (Three-Lines-of-Defence-Modell)[4]. Dieses Modell hat sich inzwischen in vielen Unternehmen etabliert. Von daher stellt sich immer wieder die Frage, wie sich die Vorgaben der DS-GVO in diesem Modell wiederfinden.

Anhand der Abbildung 4 soll beispielhaft die Einordnung der Umsetzung und Überwachung der Einhaltung der Datenschutzvorschriften in ein Risikomanagementsystem nach diesem Modell skizziert werden.

Die nachfolgende Tabelle beschreibt die allgemeinen Zuständigkeiten und Aufgaben der drei Verteidigungslinien und nimmt eine Zuordnung der verschiedenen Maßnahmen und Instrumente zur Umsetzung und Überwachung der Datenschutzvorschriften vor.

| | Allgemeine Aufgaben | Datenschutzaufgaben |
|---|---|---|
| **1. Verteidigungslinie** | Das **operative Management** ist als Risiko-Eigentümer verantwortlich für die Bewertung, Steuerung und Reduzierung von Risiken | Operatives Management (Prozessverantwortliche):<br>⇨ Einhaltung von Datenschutzrichtlinien<br>⇨ Implementierung und Durchführung von Datenschutzkontrollen |
| **2. Verteidigungslinie** | Verschiedene **Funktionen der Internal Governance** (Compliance, Risikomanagement, Qualität, Umwelt, Informationssicherheitsmanagement etc.) haben folgende Aufgaben:<br>⇨ Steuerung und Überwachung der 1. Verteidigungslinie<br>⇨ Festlegung von Methoden und Verfahren für das Risikomanagement<br>⇨ Erstellung von Vorgaben<br>⇨ Überwachung der Risiken<br>⇨ Reporting an die Unternehmensleitung | Aufgaben des **Datenschutz-Managements**:<br>⇨ Erstellung von Datenschutzrichtlinien<br>⇨ Unterstützung der Prozessverantwortlichen<br>Aufgaben des **Datenschutzbeauftragten**:<br>⇨ Beratung<br>⇨ Unterrichtung<br>⇨ Datenschutz-Reporting an die Unternehmensleitung<br>⇨ Überwachung durch die Nutzung von Überwachungsinstrumenten (z. B. Datenschutz-Audits) |
| **3. Verteidigungslinie** | **Interne Revision**<br>(objektive und unabhängige Prüfinstanz) | |

4. S. FERMA/ECIIA, Guidance on the 8th EU Company Law Directive – article 41, 2010, https://www.ferma.eu/app/uploads/2011/09/eciia-ferma-guidance-on-the-8th-eu-company-law-directive.pdf

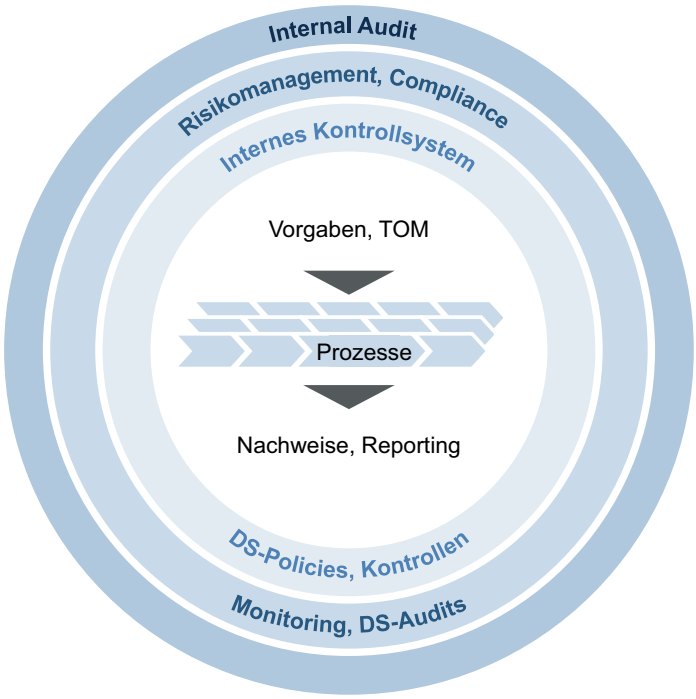


**Abb. 4:** Three lines of defence



Zu beachten ist bei dieser Art des Risikomanagements, dass sie lediglich die Risiken des Unternehmens/der Behörde betrachtet. Die DS-GVO dagegen stellt auf die „Risiken für die Rechte und Freiheiten natürlicher Personen“ ab. D.h. für den Datenschutz muss in ein bestehendes Risikomanagementsystem diese – neue – Sichtweise für den Umgang mit personenbezogenen Daten integriert werden.[5]

Die Zuordnung dieser drei Verteidigungslinien ist in Abbildung 4 noch einmal verdeutlicht.

5. zum Risikobegriff der DS-GVO siehe auch unten Kap. 4 „ Die Aufgaben des Datenschutzbeauftragten“

# 4. Die Aufgaben des Datenschutzbeauftragten

Die DS-GVO zielt darauf ab, dass der Datenschutz in allen Unternehmensprozessen wirksam umgesetzt und überwacht wird. Dies ist eine **Pflichtaufgabe**, die die verantwortliche Stelle zu gewährleisten hat. Hierfür ist sie schon aus allgemeinen Erwägungen zur Vermeidung eines Organisationsverschuldens verantwortlich (s.o. Kap. 2 „Verantwortung und Accountability“).

Dagegen stellt die Benennung eines Datenschutzbeauftragten nach der DS-GVO eine **Option** dar, die grundsätzlich nur für Unternehmen mit besonderen Risiken für die Rechte und Freiheiten von Betroffenen beim Umgang mit deren personenbezogenen Daten verpflichtend wird[6]. Der Datenschutzbeauftragte hat einen unterstützenden Auftrag, der frei von operativen Tätigkeiten ist. Eine Verschiebung der Verantwortung für die Umsetzung und Gewährleistung der Einhaltung des Datenschutzes vom Verantwortlichen auf den Datenschutzbeauftragten ist mit seiner Benennung **nicht** verbunden.

Dem Datenschutzbeauftragten obliegt neben der Aufgabe, den Verantwortlichen bzw. die Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Datenschutzpflichten zu beraten, auch die Überwachung der Einhaltung der Datenschutzvorschriften durch die Organisation.

Konkret heißt es dazu in Art. 39 Abs. 1 lit. b) DS-GVO:

> *„Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:*
>
> *...*
>
> *b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen; ...“*

Der Gesetzgeber unterscheidet in dieser Norm also zwischen der Überwachung durch den Datenschutzbeauftragten (in der englischen Fassung: *„to monitor compliance with ...“*) und den Überprüfungen durch den Verantwortlichen (in der englischen Fassung: *„... related audits;“*). Dabei ist unter dem „Verantwortlichen“ die datenverarbeitende Stelle i.S.d. Art. 4 Nr. 7 DS-GVO zu verstehen, die jeweils durch ihre Leitung, also z.B. die Geschäftsführung, vertreten wird.

Der Intention dieser Norm folgend ergibt sich, dass, wie es das LDA Bayern ausführt,

> *„... der Verantwortliche aufgrund der Pflichten-Zuweisungen in der DS-GVO, wie vor allem der Rechenschaftspflicht nach Art. 5 Abs. 2 und der Sicherstellungspflicht nach Art. 24 Abs. 1 DS-GVO, für die Einhaltung der Datenschutzvorschriften in seinem Unternehmen zu sorgen und dies auch zu kontrollieren hat. ...“*[7]

Zur Durchführung dieser „Kontrollen“ des Verantwortlichen verweist das LDA z.B. auf die

> *„... Beauftragung der Revision oder der Compliance-Abteilung mit bestimmten Prüfungen, gegebenenfalls auch durch Veranlassung externer Audits wie bspw. nach DIN EN ISO 19011 ...“*[8]

Das bedeutet also, dass die Leitung der verantwortlichen Stelle, z.B. die Geschäftsführung bzw. die Behördenleitung, diese **„Kontrollen“** sicherzustellen hat.

Dagegen bezieht sich der Auftrag des Datenschutzbeauftragten darauf, zu **überwachen**, ob die verantwortliche Stelle in ihrer Gesamtheit ihren Pflichten zur Umsetzung und Sicherstellung des Datenschutzes gerecht wird.

6. In Deutschland unterstellt das BDSG für nicht öffentliche Stellen dieses Risiko zusätzlich zur DS-GVO ab einer Mitarbeiterzahl von 20, die in der Regel ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, s. § 38 Abs. 1 BDSG.
7. Bayerisches Landesamt für Datenschutzaufsicht (LDA Bayern), Tätigkeitsbericht 2017/18, S. 38
8. LDA Bayern, TB 2017/18, S. 38

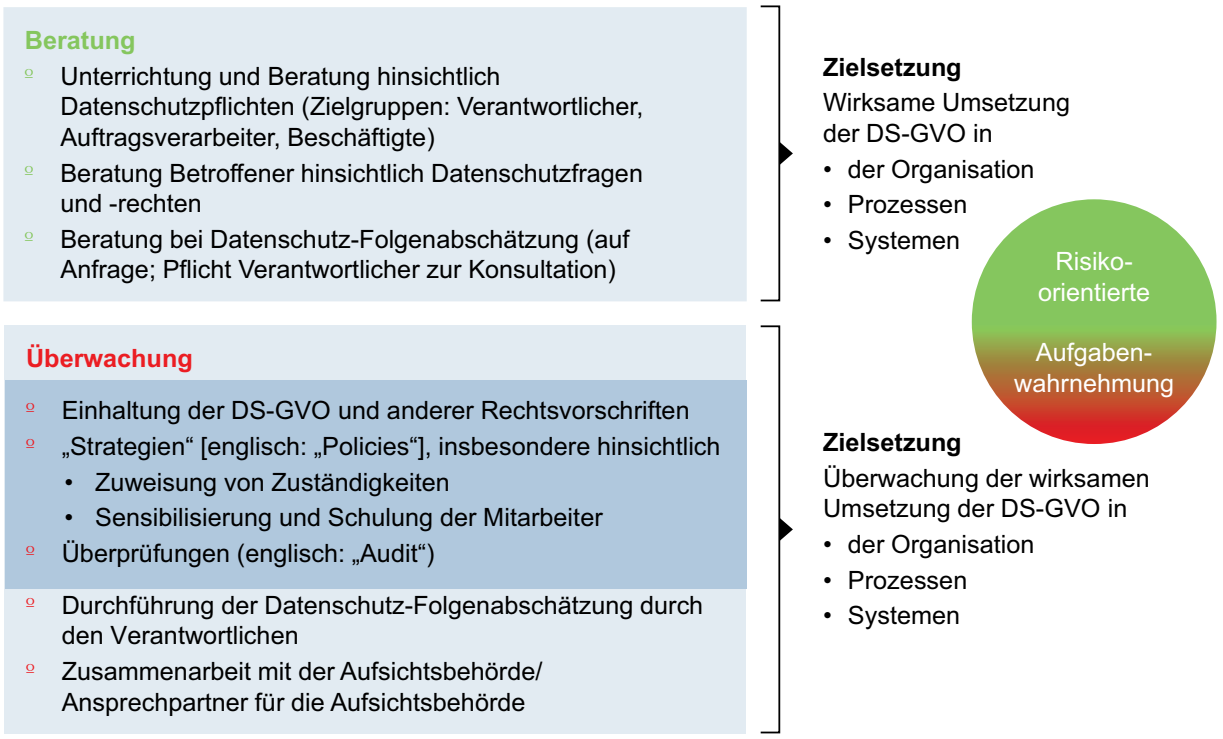


**Abb. 5:** Aufgaben des Datenschutzbeauftragten



Im Hinblick auf diese Ausgestaltung des Überwachungsauftrags stellt die Art. 29 Gruppe im WP 243 rev.01[9] fest, dass der Datenschutzbeauftragte auch hierbei vom Verantwortlichen hinreichend zu unterstützen ist. In diesem Zusammenhang sind dem Datenschutzbeauftragten insbesondere folgende Befugnisse zu erteilen:

⇨ **„Informationen** zu sammeln, um Verarbeitungsaktivitäten zu identifizieren,

⇨ die Gesetzmäßigkeit von Verarbeitungsaktivitäten zu **analysieren** und zu prüfen,

⇨ den Verantwortlichen oder den Auftragsverarbeiter zu informieren, beraten und **Empfehlungen** auszusprechen.“

Gleichzeitig stellt die Art. 29 Gruppe fest:

⇨ „Die Überwachung der Einhaltung bedeutet nicht, dass der Datenschutzbeauftragte im Falle eines Verstoßes verantwortlich ist.

⇨ Der **Verantwortliche**, nicht der Datenschutzbeauftragte, ist verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen und den Nachweis der Rechtmäßigkeit zu erbringen.

⇨ **Die Einhaltung des Datenschutzes ist eine unternehmerische Verantwortung des Verantwortlichen, nicht des Datenschutzbeauftragten**.“

Insbesondere durch den letzten Punkt wird noch einmal klargestellt, dass die Verantwortung für die Umsetzung und Gewährleistung der Einhaltung des Datenschutzes unter allen Aspekten des Organisationsverschuldens, also auch hinsichtlich der Überwachung, beim Verantwortlichen verbleibt. Mit anderen Worten:

Durch seine spezielle Fachkunde unterstützt der Datenschutzbeauftragte den Verantwortlichen im Rahmen seines Beratungsauftrags bei der operativen Umsetzung des Datenschutzes und im Rahmen seines Überwachungsauftrags bei der dem Verantwortlichen **eigenen** Überwachungspflicht!

Die Aufgabendurchführung des Datenschutzbeauftragten soll „**risikoorientiert**“ erfolgen. Hierbei stellt sich zunächst die Frage,

9. Art. 29 Gruppe, WP 243rev.01, vom 13. Dezember 2016, zuletzt überarbeitet vom 5. April 2017, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“). Diese Leitlinie gehört zu den vom Europäischen Datenschutz-Ausschuss gebilligten Leitlinien, s. https://edpb.europa.eu/node/89

wie der Begriff „Risiko“ in diesem Zusammenhang zu verstehen ist.

Grundsätzlich fokussiert die klassische Risikobetrachtung das Unternehmensrisiko, also regelmäßig Schadenausmaß und Eintrittswahrscheinlichkeit eines Ereignisses im Hinblick auf potentielle Schäden für das Unternehmen. Die DS-GVO dagegen nimmt die Position des Betroffenen ein, dessen Daten durch den jeweiligen Verantwortlichen verarbeitet werden. Ihr Risikoansatz betrachtet nicht die Unternehmensrisiken, sondern die Risiken für die jeweils Betroffenen. Insofern findet sich in den Organisationsregeln der DS-GVO (Artt. 24 ff. DS-GVO) stets die Formulierung „Risiken für die Rechte und Freiheiten natürlicher Personen“.

In der Aufgabenbeschreibung des Datenschutzbeauftragten ist dagegen lediglich davon die Rede, dass er *„... bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung ...“* trägt, s. Art. 39 Abs. 3 DS-GVO.

D.h., er ist hier nicht einseitig an die Berücksichtigung des Risikos für betroffene Personen gebunden, sondern – insbesondere im Hinblick auf seine Rolle zur Unterstützung des Verantwortlichen – hat er auch das unternehmerische Risiko mit zu betrachten. Vor diesem Hintergrund bedeutet die risikoorientierte Aufgabenwahrnehmung des Datenschutzbeauftragten im Hinblick auf seinen Überwachungsauftrag nach Auffassung der Art. 29-Gruppe insbesondere[10]:

- „einen selektiven und pragmatischen Ansatz ... hinsichtlich der Bereiche, die im Fokus eines internen/ externen **Datenschutzaudits** stehen sollten.
- **Priorisierung** der Aktivitäten im Hinblick auf Fragestellungen, die **höhere Datenschutzrisiken** darstellen.
- **Keine Vernachlässigung** der Überwachung von Datenverarbeitungsvorgängen mit vergleichsweise **geringen Risikograd.“**

10. Art. 29 Gruppe, WP 243rev.01, durch den Europäischen Datenschutzausschuss gebilligt (s.o.)