Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO II

Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung

INHALT

Verantwortlichkeiten und Aufgaben nach der Datenschutz-Grundverordnung

Mit Geltung der Datenschutz-Grundverordnung (DS-GVO) ab dem 25. Mai 2018 haben sich Unternehmen und öffentliche Stellen bei der Verarbeitung personenbezogener Daten erstmals unmittelbar an europäisches Recht zu halten. Das aktuell maßgebliche BDSG soll zu diesem Zeitpunkt in weiten Teilen aufgehoben sein. Sollte dies nicht der Fall sein, genießt die DS-GVO ab dem genannten Zeitpunkt Anwendungsvorrang vor dem nationalen Recht: Stehen Vorschriften des BDSG oder andere Rechtsvorschriften im Widerspruch zur DS-GVO, so muss die Regelung der DS-GVO angewendet werden.

Die DS-GVO führt teilweise zu einer Verschiebung der datenschutzrechtlichen Zuständigkeiten und Verantwortlichkeiten bei den Daten verarbeitenden Stellen. So verantwortet der Datenschutzbeauftragte nicht mehr operative Aufgaben wie die Mitarbeiterschulung und die Vorabkontrolle kritischer Datenverarbeitungen sondern nimmt verstärkt die Stellung eines Kontrollorgans ein.

Im Folgenden wird dargelegt, welche datenschutzrechtlichen Verantwortlichkeiten und Aufgaben der Leitung des Unternehmens bzw. der öffentlichen Stelle, den Fachbereichen, dem Datenschutzbeauftragten sowie den konkret mit der Datenverarbeitung befassten Mitarbeitern zukommen. Hieraus wird abgeleitet, welches Leitbild die DS-GVO der Organisation des Datenschutzes zugrunde legt und welche Rolle dem Datenschutzbeauftragten in diesem System zukommt.

1. Verantwortlichkeiten und Aufgaben nach der DS-GVO

1.1 Leitung des für die Verarbeitung Verantwortlichen

>> Leitung des Unternehmens (AG-Vorstand, Vereinsvorstand, Geschäftsführung etc.) bzw. der öffentlichen Stelle trägt **Gesamtverantwortung für den Datenschutz** und damit auch die Verantwortung für die Umsetzung der DS-GVO

>> **Abschreckende Sanktionen für Datenschutzverstöße; Annäherung des Datenschutzes an Verbraucherschutz:** Recht der betroffenen Person, sich durch Schutzvereinigungen/-organisationen vertreten zulassen, und Verbandsklagerecht; **Beweislastumkehr durch Nachweispflichten (Accountability)**

>> **Organisationsverantwortung** im Hinblick auf die Umsetzung der DS-GVO mittels Anweisung bzw. Policies (Vermeidung von Organisationsverschulden), ggf. Delegation an die Fachabteilung

>> **Sicherstellung ordnungsgemäßer Überwachung** der datenschutzrelevanten Unternehmensprozesse durch Installation ausreichender Kontrollmechanismen und -systeme (Vermeidung des Überwachungsversagens)

>> **Bereitstellung erforderlicher** finanzieller, sachlicher und personeller **Ressourcen** zur Umsetzung der DS-GVO sowie für die nach der DS-GVO-Umsetzungsphase erforderliche Datenschutzorganisation

>> **Einrichtung einer DS-Organisation;** ggf. Bestellung eines Datenschutzbeauftragten; selbst bei Nichtbestehen einer Bestellpflicht muss trotzdem Datenschutzfachkunde bzw. Knowhow vorhanden sein oder eingekauft werden; Empfehlung der Installation eines „Datenschutzkoordinators“

>> Publizität des Datenschutzbeauftragten (Art. 37 Abs. 7 DS-GVO): Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten und Mitteilung der Daten an die Aufsichtsbehörde

Wie ein Vergleich mit Art. 13 Abs. 1 Buchst. a) DS-GVO zeigt, wo von „Name und Kontaktdaten“ des Verantwortlichen die Rede ist, muss der Name des Datenschutzbeauftragten nicht genannt werden. Gegenüber der Aufsichtsbehörde ist die namentliche Nennung des Beauftragten hingegen notwendig.

1.2 Fachabteilungen

>> Ausführung der Anweisungen der Unternehmensleitung zur Umsetzung der DS-GVO

>> **Prozessverantwortung;** diese umfasst insbesondere die Definition der Schnittstellen (auch zum Datenschutz) und die Erfüllung von Dokumentationspflichten (z.B. Verzeichnis der Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzung, Nachweis der Einwilligung)

>> **Verantwortung für die Vermeidung datenschutzrechtlicher Risiken** durch Prozess-, Produkt- und Technikgestaltung, d.h. privacy by design/default, Löschkonzept usw.

>> **Erfüllung von Transparenz- und Informationspflichten sowie Gewährleistung der Betroffenenrechte** (Prozesse entwickeln für Information, Auskunft, Löschung, Berichtigung, Recht auf Vergessenwerden, Datenportabilität, Widerspruch und Datenpannen)

>> **arbeitsplatzbezogene Instruktion** des einzelnen Mitarbeiters

>> frühzeitige **Einbindung des Datenschutzbeauftragten** (erfolgskritischer Faktor)

1.3 Mitarbeiter

>> **Vertrautmachen** mit internen Regelungen und gesetzlichen Vorschriften sowie Einhaltung derselben (z.B. hinsichtlich Eskalationsmodellen bei Datenpannen)

>> Bei Datenschutzverstößen **ggf. persönliche Haftung** gegenüber dem Arbeitgeber bzw. den betroffenen Personen; Mitarbeiter als **möglicher Adressat von Bußgeldbescheiden** der Datenschutzaufsicht und möglicher Täter im Bereich des Datenschutzstrafrechts

>> **In datenschutzrechtlichen Zweifelsfällen stets den Datenschutzbeauftragten zurate ziehen**

1.4 Datenschutzbeauftragter (DSB)

>> Adressatengerechte **Kommunikation der Erforderlichkeit zur Anpassung an die kommende Gesetzeslage (DS-GVO)** gegenüber Leitung und Fachabteilung

>> **Hinwirkung auf die Projektierung der Umsetzung der DS-GVO**

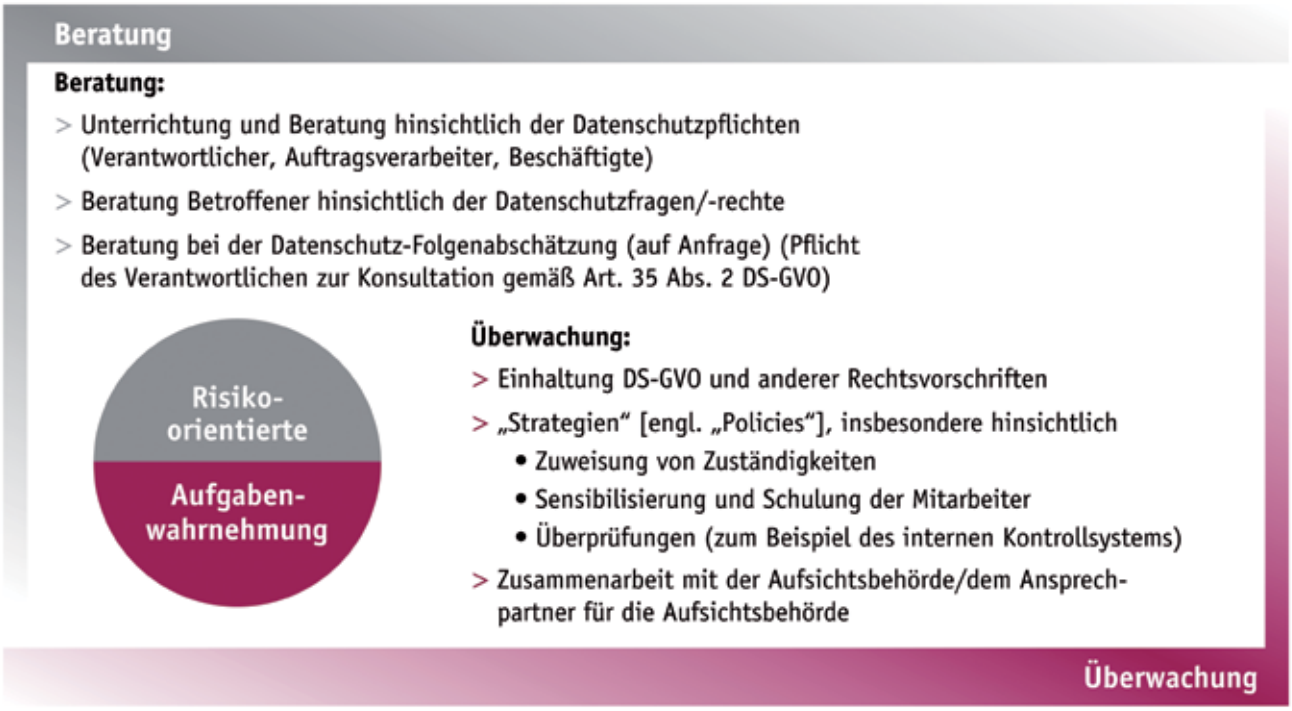
>> Unterstützung bei der Umsetzung und im laufenden Betrieb **(Beratungsauftrag)**; Erläuterung und Präzisierung der gesetzlichen Anforderungen

>> Beratung bzgl. Aufbau und Koordination eines Datenschutzmanagements

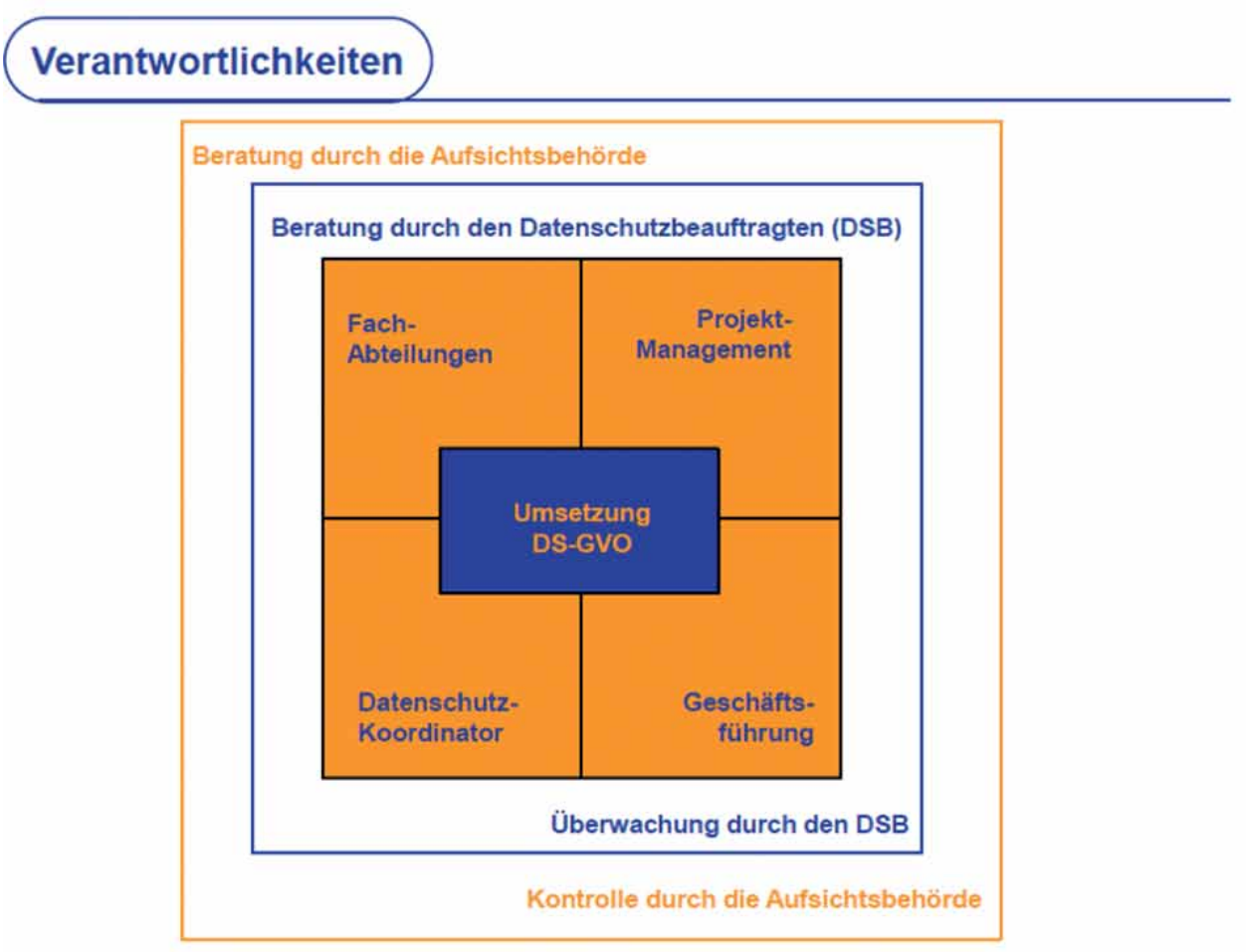
>> **Monitoring** der Umsetzung der DS-GVO

>> **Überwachung der Einhaltung der gesetzlichen Vorgaben, der internen Vorschriften sowie der Funktionsfähigkeit des Datenschutzmanagements**

Datenschutzbeauftragter



Zu den Voraussetzungen der Bestellpflicht, Aufgaben und Stellung des Datenschutzbeauftragten nach der DS-GVO vgl. im Detail „GDD-Praxishilfe DS-GVO I: Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung“:
https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_1.pdf bzw.
das Working Paper 243 „Guidelines on Data Protection Officers“ der Artikel-29-Gruppe
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf



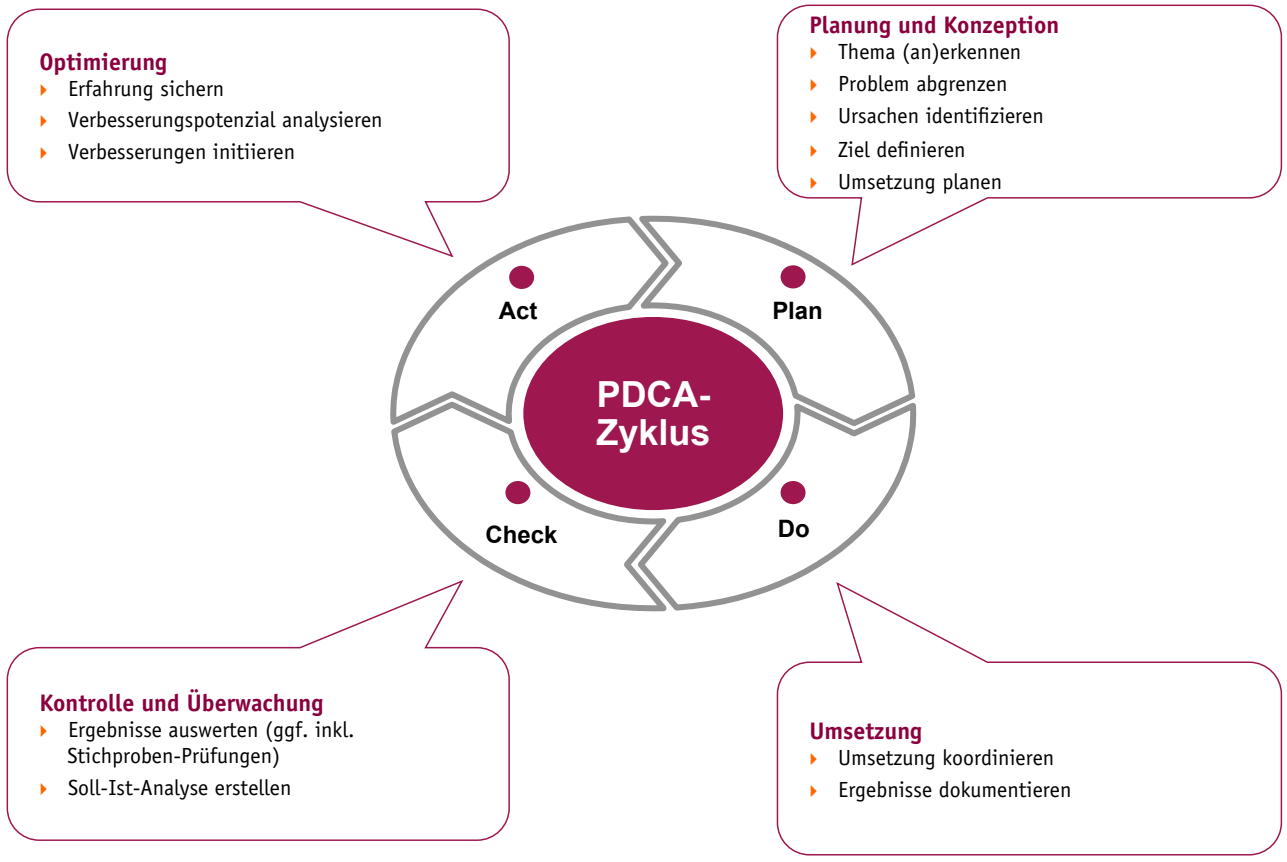
2. Datenschutzmanagement nach der DS-GVO und Rolle des Datenschutzbeauftragten

2.1 Grundzüge der Datenschutzorganisation

Wie das BDSG sieht auch die DS-GVO die Verantwortung für den Datenschutz bei der verantwortlichen Stelle, die nunmehr als „Verantwortlicher" (Art. 4 Nr. 7 DS-GVO) bezeichnet wird. Dem für die Datenverarbeitung Verantwortlichen kommt die Aufgabe zu, den Datenschutz so zu organisieren, dass er auch in der Fläche gelebt wird und seine Umsetzung jederzeit nachgewiesen werden kann.

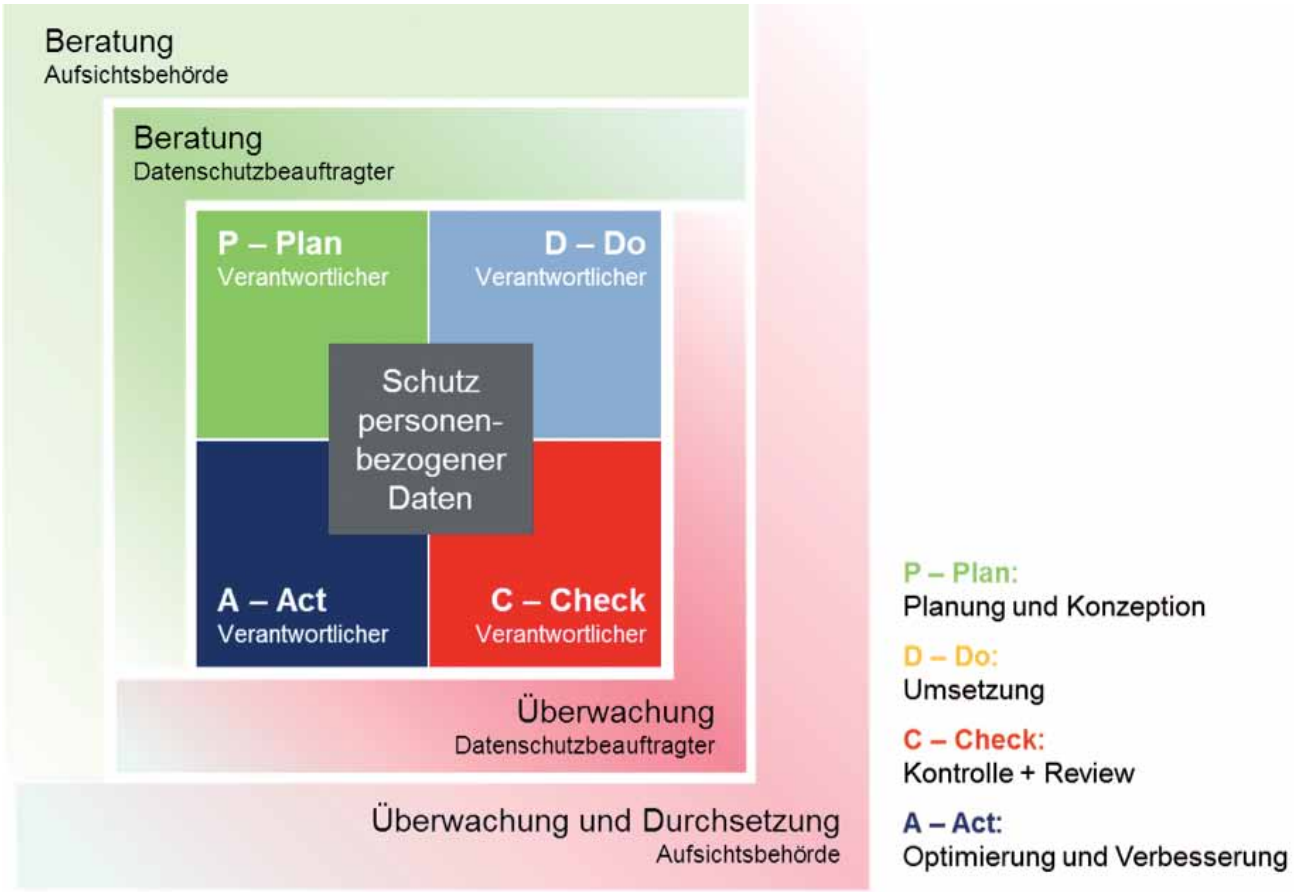
Der sog. PDCA-Zyklus („Plan-Do_Check-Act") nach Deming beschreibt einen kontinuierlichen Verbesserungsprozess und ist die Grundlage aller Qualitätsmanagement-Systeme. PDCA findet sich z.B. auch in der ISO 27001

PDCA-Zyklus



Zur Organisation des Datenschutzes verfolgt die DS-GVO ein bestimmtes Leitbild, das in den folgenden Punkten skizziert wird:

1. Die DS-GVO setzt auf – etablierte – Managementsysteme und schärft diese auch schon im BDSG angelegte Managementsysteme.
2. Art. 24 DS-GVO definiert die Organisationspflichten im Sinne des etablierten PDCA (Plan–Do–Check–Act)-Zyklus.
3. Grundsätzlich soll das Datenschutzmanagement/die Datenschutzorganisation im Bereich der Unternehmensorganisation angesiedelt sein und ist Aufgabe des gesamten Unternehmens.
4. Die Kontrolle [engl. audit] des Datenschutzes in der Phase C - Check ist durch das Unternehmen intern sicherzustellen (z. B. Internes Kontrollsystem (IKS), Compliance-Organisation).
5. (Externe) Überwachung [engl. monitoring] erfolgt durch die Aufsichtsbehörden oder (bei Zertifizierung/Verhaltensregeln) durch Auditoren - und auch durch die Betroffenen.
6. Durch Datenschutzbeauftragte muss die Organisation unterstützt (Beratung, Anknüpfungspunkt ist insbesondere die Phase P - Plan) und überwacht werden, insbesondere im Hinblick auf die Funktionalität des internen Kontrollsystems.
7. Im Bereich der Überwachung stellt der Datenschutzbeauftragte zugleich auch eine eigenständige ergänzende Überwachung zur Aufsichtsbehörde dar.
8. Insbesondere die Überwachung durch den Datenschutzbeauftragten erfolgt risikoorientiert.
9. Keine Garantenstellung des Datenschutzbeauftragten besteht durch Beratung insbesondere im Rahmen der Phase P - Plan – und die Überwachung insbesondere in Anknüpfung an die Phase C - Check. Die (Umsetzungs-) Verantwortung im Rahmen des vollständigen PDCA-Zyklus liegt bei der verantwortlichen Stelle.



Verantwortlicher = Verantwortliche Stelle/Unternehmen/öffentliche Stelle

2.2 Einzelne Aspekte des Datenschutzmanagements

Wesentliche Bestandteile, die im Rahmen des Datenschutzmanagements gefordert werden, betreffen insbesondere:

- **„Strategien" („policies")**, die insbesondere Regelungen treffen hinsichtlich der
  - Zuweisung von Zuständigkeiten
  - Risikobewertungen
  - Sensibilisierung und Schulung der Mitarbeiter
  - Durchführung von Kontrollen
- **Einsatz „datenschutzfreundlicher" Technologien**
- **IT-Sicherheit nach dem „Stand der Technik"**
- **Datenschutz-Folgenabschätzung, ggf.** mit Konsultation der Aufsichtsbehörde
- weitreichende **Nachweis- / Dokumentationspflichten, die sich aus der DS-GVO ergeben**
- **Umsetzung der Betroffenenrechte**, insbes. im Hinblick auf die Neuerungen bei
  - Löschung/Vergessenwerden
  - Transparenz
  - Datenportabilität

Die angemessene Etablierung und Einhaltung eines Datenschutzmanagementsystems kann das Unternehmen durch die Einhaltung von Verhaltensregeln oder Zertifizierungsverfahren im Sinne der DS-GVO nachweisen.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Die Inhalte dieser Praxishilfe wurden im Rahmen des GDD-Arbeitskreises „DS-GVO Praxis“ erstellt.

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

Stand:
Version 1.0 (Dezember 2016)