Christian-Albrechts-Universität zu Kiel

Vorlesung Datenschutz SS 2025

19. Mai 2025

Der Datenschutzbeauftragte

Benennung, Stellung und Aufgaben

Heiko Behrendt
Experte für Datenschutz und Informationssicherheit
ISO 27001, ISO 27701 Lead-Auditor, Fachbegutachter der DAkkS
0179 2184795 - mail@heiko-behrendt.de - https://www.heiko-behrendt.de

Niemeyerweg 2 - 24226 Heikendorf

0179 218 47 95

https://www.datenschutz-expert.de

mail@datenschutz-expert.de oder mail@heiko-behrendt.de

Prüfer, Gutachter und Berater für Datenschutz und Informationssicherheit beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, ISO/IEC 27001, ISO/IEC 27017+18 und ISO/IEC 27701 Leadauditor der datenschutz cert GmbH, Fachbegutachter der Deutschen Akkreditierungsstelle (DAkkS) für Zertifizierungsstellen und Produkte.

In der Funktion als Datenschutz- und Informationssicherheitsexperte einer Aufsichtsbehörde führe ich bei Organisationen Datenschutz- und Informationssicherheits-**Audits** sowie datenschutzrechtliche **Kontrollen** der Einhaltung der Datenschutzgrundverordnung (DSGVO) durch. Darüber hinaus begleite ich als ISO 27001 Auditor Organisationen bei der Umsetzung und Aufrechterhaltung der **Zertifizierung** ihres Informationssicherheitsmanagements (ISMS). Die **Ausbildung** von Datenschutzbeauftragten und die **Überprüfung** der Datenverarbeitung auf vorhandene technische und organisatorische Schwachstellen gehören zu meinen Schwerpunkten.

Als **ISO 27001 Auditor** führe ich Audits z. B. in folgenden Sektoren durch:

- Colocation-, Hyperscale- und Cloud-Rechenzentren
- IT- und Consulting-Dienstleister
- Softwareentwicklung
- Gesundheitswesen
- Immobilienmanagement
- Rennwettgesellschaften

Als **Referent** führe ich Lehrtätigkeiten bei folgenden Institutionen durch:

- KEDUA GmbH in Berlin
- Fortbildungskampagne öffentliches Recht in Berlin
- Studieninstitut für kommunale Verwaltung Westfalen-Lippe in Münster
- Christian-Albrechts-Universität zu Kiel im Studiengang Informatik
- Datenschutzakademie Schleswig-Holstein
- Berufsverband der Datenschutzbeauftragten Deutschlands

Inhalte

- Aufgaben und Stellung des Datenschutzbeauftragten (DSB)
- Persönliche und fachliche Voraussetzungen des DSB
- Aufgabenjahresplan
- Verantwortliche beraten und informieren
- Aufgaben im Datenschutz und Informationssicherheitsmanagement-Team
- Audits und Datenschutzkontrollen durchführen
- Ablauf und Methodik bei der Überwachung der Einhaltung der Datenschutzanforderungen

Informationsquellen

- Datenschutzaufsichtsbehörden des Bundes und der Länder
  https://www.datenschutzkonferenz-online.de/index.html
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
  https://www.bfdi.bund.de/DE/Home/home_node.html
- Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.
  https://www.gdd.de/
- Berufsverband der Datenschutzbeauftragten (BvD)
  https://www.bvdnet.de
- Berufsverband der IT-Revisoren, Information Security Manager und IT-Governance-Experten
  https://www.isaca.de
- Datenschutz-Berater
  https://www.datenschutz-berater.de/
- IT-Sicherheit DATAKONTEXT
  https://www.itsicherheit-online.com/
- Security-Insider
  https://www.security-insider.de/
- BSI-Magazin
  https://www.bsi.bund.de/

Hinweis: Der Inhalt des Vortrags stellt die persönliche Rechtsauffassung des Referenten anhand der Gesetzesmaterialien dar. Informationen zur Umsetzung der Inhalte sind als Empfehlungen und bewährte Vorgehensweisen (best practice) zu verstehen.

Aufgaben und Stellung des DSB

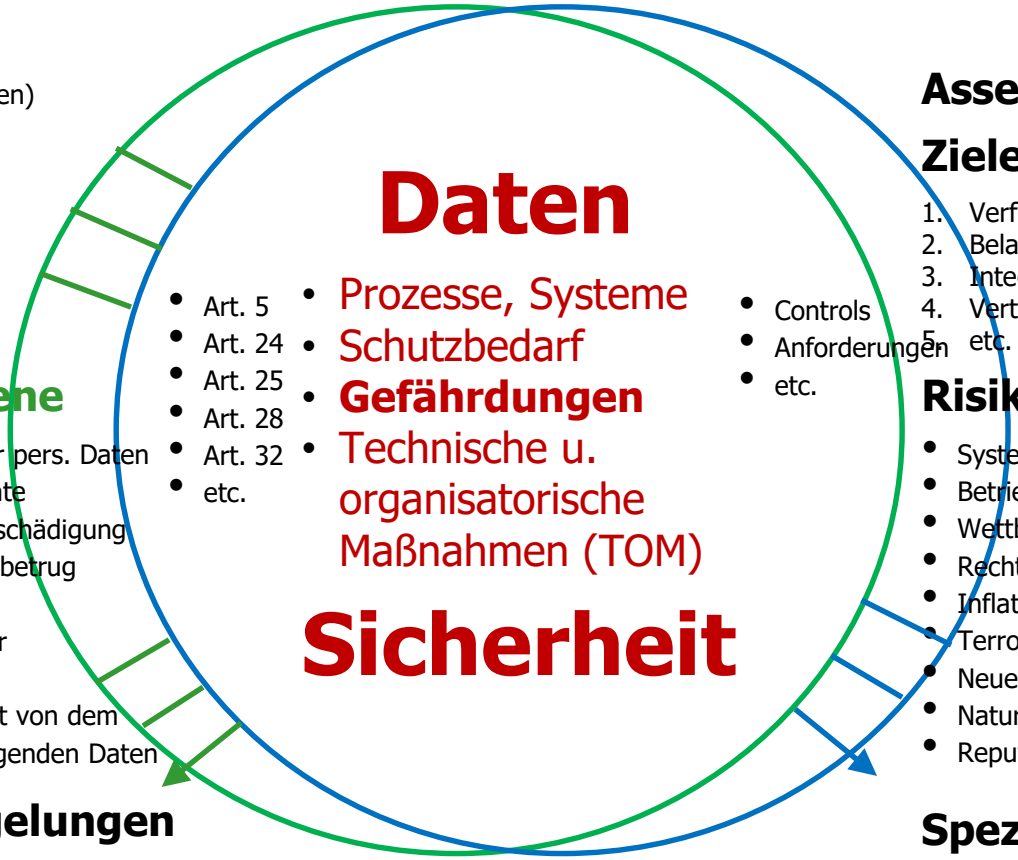
Datenschutz und Informationssicherheit

Kombination – Synthese

Datenschutz DSGVO
Datenschutzanforderungen

Organisation

Informationssicherheit
ISMS ISO 27001



Daten (personenbezogen)

Ziele

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit
4. Transparenz
5. etc.

Risiken Betroffene

- Verlust der Kontrolle über pers. Daten
- Einschränkung ihrer Rechte
- Diskriminierung oder Rufschädigung
- Identitätsdiebstahl oder -betrug
- finanzielle Verluste
- Unbefugte Aufhebung der Pseudonymisierung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten

Spezifische Regelungen

- Betroffenenrechte, Informationspflichten
- Datenschutz-Folgenabschätzung
- Verzeichnis der Verarbeitungstätigkeiten
- etc.

Assets/Werte

Ziele

1. Verfügbarkeit
2. Belastbarkeit
3. Integrität
4. Vertraulichkeit
5. etc.

Risiken Organisation

- Systemausfall, Viren, Hackerangriffe
- Betriebsunterbrechung
- Wettbewerber Konkurrenz
- Rechtliche Veränderungen
- Inflation
- Terrorismus
- Neue Technologien
- Naturkatastrophen
- Reputationsverlust

Spezifische Regelungen

- ISO 27002 Leitfaden für ISO 27001
- ISO 27005 Risikomanagement
- ISO 27017+18 Cloud
- ISO 27701 Datenschutz
- BSIG (Kritische Infrastruktur)
- etc.

Datenschutzgrundverordnung

Art. 5 Grundsätze für die Verarbeitung pb Daten mit Rechenschaftspflicht

Art. 6 Rechtmäßigkeit der Verarbeitung

Verantwortung	Personenbezogene Datenverarbeitung	Rechte der Personen
Art. 24 Verantwortung für die Datenverarbeitung		Art. 12 Transparente Informationen
Art. 25 Datenschutz durch Technikgestaltung		Art. 13 + 14 Mitteilung über Datenerhebung
Art. 28 Auftragsverarbeiter		Art. 15 Auskunft
Art. 30 Verzeichnis der Verarbeitungstätigkeiten		Art. 16 Berichtung
Art. 32 Sicherheit der Verarbeitung (TOM)		Art. 17 Löschung
Art. 33+34 Meldung von Datenschutzverletzungen		Art. 18 Einschränkung
Art. 35 Datenschutz-Folgenabschätzung		Art. 19 Mitteilung über Datenänderungen
Art. 37 – 39 Benennung, Stellung, Aufgaben DSB		Art. 20 Datenübertragbarkeit
Art. 40 – 43 Verhaltensregeln und Zertifizierung		Art. 21 Widerspruchsrecht
Art. 44 – 49 Datenübermittlung an Drittländer		Art. 22 Automatisierte Entscheidungen, Profiling

Bundes- und Landesdatenschutzgesetze

Gesetze und Verordnungen für Datenschutz und Cybersicherheit

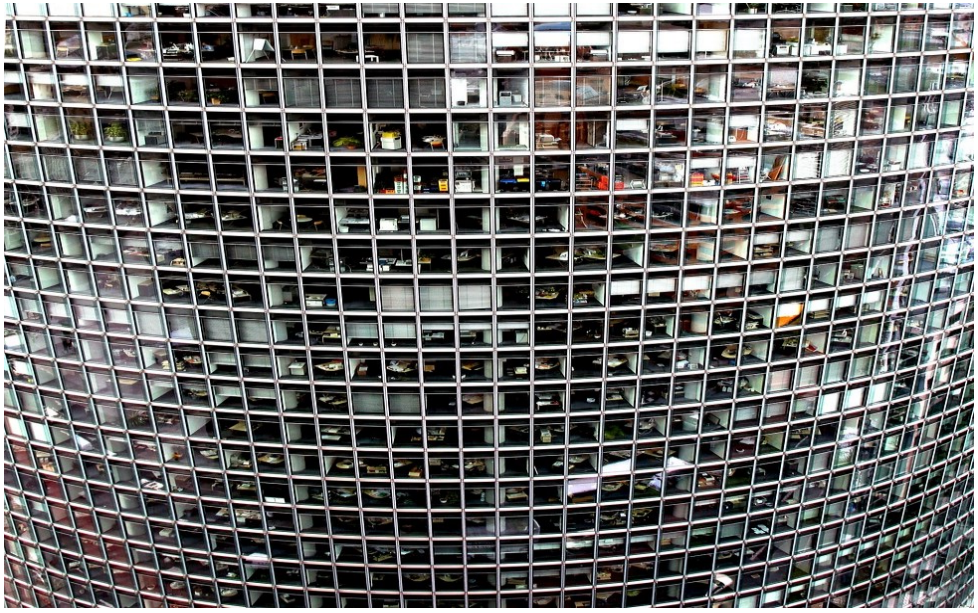
Datenschutzgrundverordnung 27.04.2016	Schutz **natürlicher Person**en bei der Verarbeitung personenbezogener Daten
E-Privacy-Richtlinie aus 2002 und den Entwurf der E-Privacy-Verordnung (veraltet)	Die Richtlinie 2002/58/EG oder Datenschutzrichtlinie für elektronische Kommunikation regelt seit 2002 verbindliche Mindestvorgaben für den Datenschutz in der Telekommunikation. Anfang 2025 zog die EU-Kommission den **Verordnungsentwurf** zurück
Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) v. 14.05.2024	Das TDDDG regelt u. a. das **Fernmeldegeheimnis** und den Schutz der Privatsphäre in der Telekommunikation, z. B. **Cookie-Einwilligung**
Datenverordnung (EU Data Act) vom 13.12.2023, gilt ab 09.2025	Bereitstellung v. Produkt- u. verbundenen **Dienstdaten** für den Nutzer und „Datenempfänger" (Firmen) f. einen **fairen Datenzugang** und eine faire Datennutzung
NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – Entwurf 2024 (IT-Sicherheitsgesetz 3.0)	Anforderungen an die Cybersicherheit, um das **Sicherheitsniveau** in der EU zu **stärken**. Mantelgesetz, das gleichzeitig mehrere Gesetze in sich vereint, z. B. BSI-Gesetz, BND-Gesetz, TDDDG und weitere
KI-Verordnung (Artificial Intelligence Act) vom 13.06.2024, gilt vollständig 08.2027	Festlegung harmonisierter Vorschriften für **künstliche Intelligenz**
Cyberresilienz-Verordnung 23.10.2024 (Cyber Resilience Act) gilt vollständig 12.2027	**Cybersicherheitsanforderungen** an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen für ein **hohes** Cybersicherheitsniveau in EU
Cybersolidaritätsverordnung 19.12.2024 (Cyber Solidarity Act) gilt vollständig 01.2025	Regelungen zur **Stärkung** der **Solidarität** und der Kapazitäten in der EU für die Erkennung/Vorsorge von **Cyberbedrohungen** und **Sicherheitsvorfällen.** Einrichtung eines EU-Warnsystems für Cybersicherheit

Datenschutz und Informationssicherheit

Welchen Stellenwert hat Datenschutz in der Organisation?

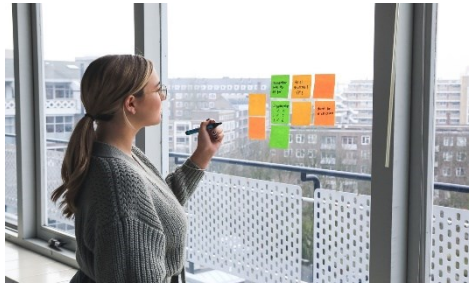
- **Ziele** der Organisation
- **Schutzbedarf** der Daten
- **Rechte** der Betroffenen
- Umgang mit **Risiken**
- Festlegung **technischer und organisatorischer Maßnahmen**
- Erkennen und Bearbeiten von **Datenschutzverletzungen**
- **Überwachung** der Vorschriften
- …

Firma X GmbH



Stellenwert Datenschutz ?

Datenschutzbeauftragte ?



Quelle: https://pixabay.com/

Datenschutz- und Informationssicherheitsstrategie

Hat der Verantwortliche eine Strategie festgelegt?

- Bestimmung der **schützenswerten Güter/Daten** (Assets)
- Festlegung der **Datenschutz- und Informationssicherheitsziele**
- Umsetzung von **Sicherheitsstandards**, z. B. IT-Grundschutz
- Implementierung eines Datenschutz- und Informationssicherheitsmanagements **(DISM)**
- Bestellung eines Datenschutz- und ggf. eines Informationssicherheitsbeauftragten **(DSB)**
- Priorisierung der **Aufgaben** des DSB
- Sensibilisierung und **Schulung** der Beschäftigten
- Standardisierung der **Prozesse** für Datenschutz und Informationssicherheit
- …

Datenschutz- und Informationssicherheitskonzept

Gibt es überprüfbare Regelungen?

- Datenschutz- und Informationssicherheitsleitlinie
- Verzeichnis der Verarbeitungstätigkeiten
- Schutzbedarfsfeststellung
- Dokumentation der Aufbau- und Ablauforganisation
- Beschreibung der eingesetzten IT-Komponenten für die Datenverarbeitung
- Gefährdungs- und Risikoanalyse
- **Technische und organisatorische Maßnahmen** (TOMs) für den Schutz der Daten
- Sicherheitsrichtlinien für IT-Komponenten
- Dienstanweisungen für Beschäftigte
- Verträge und Vereinbarungen mit Dienstleistern
- etc.

Benennung des Datenschutzbeauftragten

Art. 37 DSGVO

- Der Verantwortliche und der Auftragsverarbeiter **benennen** auf jeden Fall einen Datenschutzbeauftragten, wenn
  - die Verarbeitung von einer **Behörde oder öffentlichen Stelle** durchgeführt wird,
  - regelmäßige und systematische **Überwachung** von betroffenen Personen,
  - Verarbeitung **besonderer Kategorien** von Daten gemäß Art. 9 DSGVO.
- Eine Unternehmensgruppe / Behörde darf einen **gemeinsamen Datenschutzbeauftragten** ernennen, sofern der DSB seine Aufgaben auch an allen Standorten erfüllen kann.
- Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen **Qualifikation** und seines **Fachwissens** benannt.
- Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die **Kontaktdaten** des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Bundesdatenschutzgesetz

- §§ 5 - 7 BDSG Datenschutzbeauftragter öffentlicher Stellen
- § 38 BDSG Datenschutzbeauftragter nicht öffentlicher Stellen

Benennung des Datenschutzbeauftragten

§ 38 BDSG

Auszug Gesetzestext § 38 BDSG

Ergänzend zu Art. 37 Abs. 1 Buchstabe b und c DSGVO benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens **20 Personen ständig** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor,

- die einer **Datenschutz-Folgenabschätzung** nach Art. 35 DSGVO unterliegen, oder
- verarbeiten sie pb Daten **geschäftsmäßig zum Zweck** der **Übermittlung**, oder
- für Zwecke **der Markt- oder Meinungsforschung**,

haben sie **unabhängig von der Anzahl** der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

Stellung des Datenschutzbeauftragten

Art. 38 DSGVO

- Der Verantwortliche und der Auftragsverarbeiter
  - stellen sicher, dass der DSB **ordnungsgemäß und frühzeitig** in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen **eingebunden** wird,
  - stellen zur Erfüllung seiner Aufgaben gemäß Art. 39 DSGVO die **erforderlichen Ressourcen** und den **Zugang zu pb Daten und Verarbeitungsvorgängen** sowie die zur **Erhaltung seines Fachwissens** erforderlichen Ressourcen zur Verfügung,
  - stellen sicher, dass der DSB bei der Erfüllung seiner Aufgaben **keine Anweisungen bezüglich der Ausübung dieser Aufgaben** erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht **abberufen oder benachteiligt** werden.
  - Der DSB kann auch **andere Aufgaben** wahrnehmen. Der Verantwortliche stellt sicher, dass es dabei zu keinem **Interessenkonflikt** kommt.
- Der **DSB berichtet** unmittelbar der **höchsten Managementebene** des Verantwortlichen oder des Auftragsverarbeiters.

Aufgaben des Datenschutzbeauftragten

Art. 39 DSGVO

Dem DSB obliegen **zumindest** folgende Aufgaben:

- Unterrichtung und **Beratung** des Verantwortlichen und der Beschäftigten
- **Überwachung** der Einhaltung der **DSGVO** und anderer Datenschutzvorschriften
- **Überwachung** der Einhaltung der **Strategien** des Verantwortlichen/Auftragsverarbeiters
- Überwachung der **Sensibilisierung und Schulung** der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen
- **Beratung** im Zusammenhang mit der **Datenschutz-Folgenabschätzung** (DSFA) und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als **Anlaufstelle für die Aufsichtsbehörde** in mit der Verarbeitung zusammenhängenden Fragen

Verantwortliche beraten und informieren

Informationsaustausch

- Festlegung der **Kommunikationswege** (digital, persönlich) und Kommunikations-instrumente, z. B.
  - E-Mail
  - Videokonferenz
  - Sharepoint
  - Intranet
- Durchführung von wöchentlich und anlassbezogenen **Sitzungen** im Rahmen des **Datenschutzmanagement-Teams** (wenn vorhanden)
- Teilnahme an **Abteilungsleitersitzungen** mit Berichtspflicht
- **Besprechung** nach Absprache mit Verantwortlichen in der **Fachabteilung**
- Durchführung einer **Informationsveranstaltung** für Verantwortliche und ggf. Beschäftigte in der der DSB über seine Tätigkeiten und über aktuelle Themen berichtet
- Bearbeitete Aufgaben werden vom DSB **verschriftlicht** und den Verantwortlichen zur Kenntnis bzw. Stellungnahme gegeben (Vermerk, Prüfbericht, Vorfall)

Aufgabenjahresplan

Beispiel: Wie plane ich als DSB meine Aufgaben?

Erstellung einer **Übersicht** mit einer kurzen **Aufgabenbeschreibung** (Jahresplanung)

Aufgaben-Jahresplan	Zeitplan
• Vorbereitung und Leitung der Sitzungen des Datenschutzmanagements • Beratung der Fachabteilungen • Mitwirkung/Bearbeitung der Anfragen von Betroffenen • Teilnahme an Sitzungen neuer Projekte • Mitwirkung/Bearbeitung von Datenschutzvorfällen • Fortbildung, Teilnahme an Seminaren • Mitwirkung bei der Erstellung von Dokumentation (Dienstanweisungen, Konzepte)	Ganzjährig
• Erstellung eines Berichts über die durchgeführten Aufgaben des Vorjahres (Tätigkeitsbericht)	1. Qtl.
• Erarbeitung eines Schulungskonzepts nach Zielgruppen des Unternehmens • Erstellung von Rundschreiben und Datenschutzhinweisen • Aufbau und Pflege der Intranet-Plattform mit Datenschutzregelungen	1. Qtl.
• Erstellung einer Leitlinie für Datenschutz und Informationssicherheit • Bestandsaufnahme der Dokumentation im technischen Bereich (Konzepte, Richtlinien etc.) • Festlegung einer Dokumentationsstruktur für die Verwaltung der Dokumente	2. Qtl.
• Audit 1 Personalwesen: Aktenführung und Aktenaufbewahrung in Büros und Archiven • Audit 2 Benutzer- und Rechtemanagement: Active-Directory, Fachanwendung Personal • Audit 3 Digitalkopierer: Bestand, Aufstellungsorte, Aussonderung, AV-Verträge, Datenlöschung	1. – 4. Qtl.
• Mitwirkung bei der Einführung von neuen Fachanwendungen (Schwellwertanalyse, Datenschutz-Folgenabschätzung) • Mitwirkung/Beratung der Verantwortlichen bei der Umsetzung der DSFA • Unterstützung bei der Dokumentation und der Erstellung der Risikoanalyse • Mitwirkung bei der Nutzung eines Tools für die DSFA	2. – 4. Qtl.

Aufgabenjahresplan

Warum ist ein Aufgabenjahresplan wichtig?

- Der Aufgabenjahresplan schafft **Transparenz** über die geplanten Tätigkeiten des DSB
- Den **Verantwortlichen** wird deutlich, welche **Datenschutzprozesse** bearbeitet werden
- Die **Interessen der Organisation** können vom DSB berücksichtigt werden
- Der Verantwortliche kann gemeinsam mit dem DSB **Prioritäten** setzen
- Die **geplanten Aufgaben** können **rechtzeitig** in die **Betriebsabläufe** integriert werden
- Der DSB macht **deutlich**, dass er seinen Aufgaben nach der DSGVO **gerecht** wird
- **Mangelnde Ressourcen** bzw. Personalkapazitäten werden erkannt
- Im Aufgabenjahresplan kann hervorgehoben werden, wo **Unterstützung durch Dritte** (Schulung, Audits) notwendig wird
- Auf der Grundlage des Aufgabenjahresplans kann der DSB den **Tätigkeitsbericht** erstellen

www.bvdnet.de

Das berufliche Leitbild der Datenschutzbeauftragten

Code of Practice for Data Protection Officers

4. Ausgabe 2018 | *Edition 4/2018*

Publikation des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Publication of the Association of Data Protection Officers of Germany (BvD) e.V.

Aufgabe	Quelle (DSGVO)	Beschreibung
Managementaufgaben	Art. 24 Art. 38 Abs.1 ErwGr 97	• Einbindung des Datenschutzbeauftragten durch den Verantwortlichen in datenschutzrelevante Managementsysteme • Beratung zu Zielen und Aufgaben sowie bei der Fortschreibung des Datenschutzmanagementsystems • Review des Datenschutzmanagementsystems
Beraten	Art. 38 Abs. 1, 4 Art. 39 ErwGr 77, 97 Art. 35 Art. 88 ErwGr 155	• Beratung der Leitung • Beratung der Bereiche, insbesondere der Fachabteilungen • Beratung der betroffenen Personen (Beschäftigte, Kunden, Geschäftspartner) • Beratung in Zusammenhang mit der Datenschutz-Folgenabschätzung • Beratung der Mitarbeitervertretung
Überwachen	Art. 39 ErwGr 81	• Risikoorientierte Festlegung datenschutzrelevanter Prüfungen • Veranlassen, begleiten oder durchführen von Auditierungen und Prüfungen inkl. erforderlicher Dokumentation • Überwachung der Prüfungen ◦ der datenverarbeitenden Geschäftsprozesse und Regelungen ◦ von IT-Systemen ◦ der datenschutzrelevanten Verträge ◦ der Dokumentation von Verarbeitungsvorgängen inkl. deren Risiko, insbesondere des Verzeichnisses von Verarbeitungstätigkeiten ◦ der Angemessenheit und Einhaltung der technischen und organisatorischen Maßnahmen ◦ von Verfahren, die einer Datenschutz-Folgenabschätzung unterliegen ◦ von Garantien externer Dienstleister (Auftragsverarbeiter) • Überwachung der Bearbeitung von Beschwerden und sicherheitsrelevanten Vorfällen
Berichten und informieren	Art. 39	• Regelmäßige Unterrichtung der Leitung • Zusammenarbeit mit der Aufsichtsbehörde • Regelmäßige Tätigkeitsberichte an den Verantwortlichen

Quelle: https://www.bvdnet.de

DSK

INFOTHEK LINKS DIE DSK KONTAKT

Datenschutzkonferenz

Herzlich willkommen auf dem offiziellen Webauftritt der Datenschutzkonferenz (DSK), dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder.

Auf diesen Seiten finden Sie offizielle Entschließungen, Orientierungshilfen und weitere Informationen zum Thema Datenschutz.

NEU Pressemitteilung: 107. Sitzung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden am 14. und 15. Mai in Bremerhaven

NEU Pressemitteilung: Datenschutzkonferenz bezieht Position: Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO)

Pressemitteilung: Künstliche Intelligenz datenschutzkonform einsetzen: Datenschutzkonferenz veröffentlicht Orientierungshilfe für Unternehmen und Behörden

Orientierungshilfe der DSK zu Künstlicher Intelligenz und Datenschutz

Quelle: https://www.datenschutzkonferenz-online.de/

Kurzpapier Nr. 12
Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Die nachfolgenden Erläuterungen zum Datenschutzbeauftragten (DSB) gelten sowohl für Verantwortliche als auch für Auftragsverarbeiter.

Benennung des DSB

Eine Pflicht zur Benennung eines DSB kann sich sowohl aus der DS-GVO als auch aus dem nationalen Recht ergeben. Eine Benennungspflicht kann für den Verantwortlichen, für den Auftragsverarbeiter oder für beide bestehen, je nachdem wer durch seine Tätigkeit selbst die Voraussetzungen für diese Pflicht erfüllt. Wer bisher einen DSB bestellen musste, muss in der Regel auch weiterhin einen DSB benennen.

Benennung des DSB nach Art. 37 DS-GVO

Nach Art. 37 Abs. 1 lit. a – c DS-GVO ist auf jeden Fall ein DSB zu benennen, wenn eine der folgenden Voraussetzungen gegeben ist:

- Behörde oder öffentliche Stelle (mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln),
- Kerntätigkeit mit umfangreicher oder systematischer Überwachung von Personen oder
- Kerntätigkeit mit umfangreicher Verarbeitung besonders sensibler Daten (Artikel 9, 10 DS-GVO).

„Kerntätigkeit" ist die Haupttätigkeit eines Unternehmens, die es untrennbar prägt, und nicht die Verarbeitung personenbezogener Daten als Nebentätigkeit (ErwGr. 97 der DS-GVO). Zu den Kerntätigkeiten gehören danach auch alle Vorgänge, die einen festen Bestandteil der Haupttätigkeit des Verantwortlichen darstellen. Hierzu gehören nicht die das Kerngeschäft unterstützenden Tätigkeiten wie z. B. die Verarbeitung der Beschäftigtendaten der eigenen Mitarbeiter.

Für die Definition des Begriffs "umfangreich" können aus ErwGr 91 der DS-GVO folgende Faktoren herangezogen werden:

- Menge der verarbeiteten personenbezogenen Daten (Volumen),
- Verarbeitung auf regionaler, nationaler oder supranationaler Ebene (geografischer Aspekt),
- Anzahl der betroffenen Personen (absolute Zahl oder in Prozent zur relevanten Bezugsgröße) und
- Dauer der Verarbeitung (zeitlicher Aspekt).

Sind mehrere Faktoren hoch, so kann dies für eine "umfangreiche" Überwachung bzw. Verarbeitung sprechen.

Erfolgt eine Verarbeitung von Patienten- oder Mandantendaten durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalt, handelt es sich regelmäßig nicht um eine die Benennungspflicht auslösende umfangreiche Datenverarbeitung (siehe ErwGr. 91). Unter Berücksichtigung der Umstände des Einzelfalls und der konkreten Elemente einer umfangreichen Verarbeitung im Sinne des ErwGr. 91 – beispielsweise bei einer Anzahl von Betroffenen, die erheblich über

Stellenbeschreibung Datenschutzbeauftragte(r)

100 % - Beispiel

Aufgaben	Zeitanteil in %
Unterweisung der Beschäftigten	10
Prüfung der Verpflichtung der Beschäftigten auf die Vertraulichkeit (Art. 5, 24, 29, 32 DSGVO)	
Einweisung der Beschäftigten in die datenschutzkonforme Nutzung der Informationstechnik (Art. 5 DSGVO)	
Beantwortung konkreter Anfragen von Beschäftigten zum Datenschutz	
Prüfungen, Kontrollen, Audits	30
Prüfung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme zur Verarbeitung personenbezogener Daten beim Verantwortlichen und beim Auftragsverarbeiter (Art. 5, 24, 25, 28, 32 DSGVO)	
Auskunfts- und Registeraufgaben	15
Mitwirkung bei der Auskunftserteilung gegenüber Betroffenen (Art. 15 DSGVO)	
(Mitwirkung) bei der Verwaltung des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO)	
Mitwirkung bei der Bearbeitung von Datenschutzvorfällen und ggf. von Meldepflichten des Verantwortlichen gegenüber der Aufsichtsbehörde und dem Betroffenen (Art. 33 und 34 DSGVO)	
Herstellung der Transparenz bei technischen und organisatorischen Abläufen der Datenerhebung und -verarbeitung	15
Erstellung und Pflege der Datenschutz-Dokumente	
Entwicklung von Anweisungen / Richtlinien zum datenschutzkonformen Umgang mit personenbezogenen Daten	
Zusammenarbeit mit der IT-Abteilung und den Fachabteilungen bei der Beschreibung interner Prozesse und der Dokumentation technischer und organisatorischer Maßnahmen	
Unterstützung und Beratung bei der Planung und Umsetzung neuer Projekte und Datenverarbeitungen	15
Prüfung auf Konformität der datenschutzrechtlichen Vorschriften bei neuen Datenverarbeitungen (Art. 25 DSGVO)	
Beratung bei und ggf. Durchführung der Datenschutzfolgenabschätzung (Art. 35 DSGVO)	
ggf. Entwicklung von Alternativlösungen, die datenschutzrechtlich unbedenklich und datensparsam sind	
Schulung und Sensibilisierung der Beschäftigten	15
Durchführung und/oder Koordination von Schulungen zum Datenschutz	
Erstellung eines Schulungskonzepts und von Materialien/Infos zur Sensibilisierung der Beschäftigten	

Datenschutz- u. Informationssicherheitsmanagement

DISM-Team

Abhängig von der **Größe** der Organisation:

- Mindestens ein „**Datenverantwortlicher**“ (Behörden- oder Abteilungsleiter, Geschäftsführer)
- Datenschutzbeauftragter
- Informationssicherheitsbeauftragter
- Leiter IT-Abteilung
- Ggf. Koordinatoren in den Fachabteilungen
- Ggf. Leiter Revisionsabteilung
- Ggf. Personal- bzw. Betriebsrat
- Ggf. DSB von Auftragsverarbeiter
- …

Quelle: https://pixabay.com

Datenschutz- und Informationssicherheitsbeauftragter

Abgrenzung

Informationssicherheit

- **Informationssicherheitsziele und –strategien** bestimmen
- **Leitlinie zur Informationssicherheit** entwickeln und Umsetzung überprüfen
- **Risiken** für die Prozesse des Unternehmens identifizieren
- Sicherheitsprozess initiieren, **steuern und kontrollieren**
- Erstellung des Sicherheitskonzepts
- **TOMs** festlegen, umsetzen lassen und im Rahmen von Audits überprüfen
- Schulungs- und Sensibilisierungsprogramme für Informationssicherheit konzipieren
- Fachverantwortliche in Fragen der Informationssicherheit **beraten**
- …

Datenschutz

- **Rechtmäßigkeit** der Datenverarbeitung prüfen und sicherstellen
- Schutz der Daten des Betroffenen sicherstellen = **Risiken** identifizieren, bewerten und durch technische und organisatorische Maßnahmen eindämmen
- Datenschutzprozess initiieren, **steuern und kontrollieren**
- Mitwirkung bei der **Datenschutz-Folgenabschätzung**
- Mitwirkung bei der Bearbeitung von **Datenschutzvorfällen**
- Fachverantwortliche in Fragen des Datenschutzes **beraten**
- …

Checkliste DSB

- Wurden die **Aufgaben und Zuständigkeiten** des **DSB** im angemessenen Verhältnis zur Organisationsgröße umgesetzt?
- Sind DSB / ISB **nicht** gleichzeitig auch **„Datenverantwortliche“**?
- Wurden von der Organisation die **finanziellen und personellen Ressourcen für Datenschutzaufgaben** vollständig ausgeschöpft?
- Wurde die **Aufgabenzuweisung** des DSB unter Berücksichtigung des **Status Quo der Organisation** in einer **Stellenbeschreibung** festgelegt?
- Sind **fachliche Kenntnisse** des DSB ausreichend vorhanden?
- Wurde vom DSB ein **Aufgabenjahresplan** erstellt?
- Sind **Vertretungsaspekte** bei **Abwesenheit** des DSB berücksichtigt?
- Sind die **Schnittstellen** zwischen verschiedenen **Rollen des DSB** eindeutig definiert und voneinander abgegrenzt?
- Hat der DSB mit **Doppelfunktion ausreichende Zeit** für die Umsetzung der ihm zugewiesenen Aufgaben?
- Werden vom DSB regelmäßig oder anlassbezogen **Besprechungen** im Rahmen des **DISM-Teams** und/oder mit **Verantwortlichen** durchgeführt?

Audits und Datenschutzkontrollen durchführen

Methodische Vorgehensweise = 5 Schritte/Phasen

1. **Vorbereitung**
   Abstimmung mit Verantwortlichem, Vorbereitung: Scope, DSGVO, Referenzdokumente, Prüfplan, Checkliste, Termine
2. **Auftaktgespräch**
   Besprechung mit Verantwortlichen und Beteiligten, Einführung, Ablauf, Ansprechpartner
3. **Vor-Ort-Audit**
   Auditgegenstand analysieren, Prüfen, ob Sollvorgaben (DSGVO) eingehalten werden
4. **Abschlussgespräch**
   Besprechung mit Verantwortlichen und Beteiligten, Ablauf, Darstellung der Feststellungen, Vorab-Fazit, Abweichungen
5. **Auditbericht**
   Erstellung des Auditberichts, Übergabe und Erörterung der Inhalte

\+ **Folgeaktivitäten**
Unterstützung bei der Bearbeitung der Abweichung, ggf. „Überwachungsaudit"

1. Vorbereitung

Wie bereite ich mich vor?

- **Abstimmung mit der Verantwortlichen Ebene:** Durchführung des Audit mit dem Verantwortlichen besprechen und Zustimmung/Beteiligung/Unterstützung „beantragen"
- **Gesetzliche Reglungen und interne Richtlinien**: Prüfungsgrundlage analysieren und festlegen. Was muss die Organisation beachten?
- **Scope:** Auditgegenstand festlegen. Was will ich genau im Rahmen des Audits prüfen? Z. B. Fachanwendungen, IT-Komponenten, Netz, Gebäude- und Räume, etc.
- **Strategie:** Vorgehensweise festlegen. Standorte, Bereiche, Fachanwendungen (Daten) und IT-Komponenten, die Vorort geprüft werden sollen. Begehung, Interviews planen
- **Audit- bzw. Prüfplan:** Erstellung eines Auditplans. Dient als Orientierung und roter Faden während der Durchführung des Audits.
- **Termine mit Ansprechpartnern:** Beteiligte Personen informieren und Termine für das Audit insbesondere für das Auftaktgespräch festlegen.
- **Fachkenntnisse:** Ggf. Know-how für Prüfbereiche vertiefen.

2. Auftaktgespräch

Was gehört zum Auftaktgespräch?

- Auftaktgespräch mit **allen Beteiligten** (Verantwortliche, IT-Abteilung) führen
- Festlegen, **wer** an den Gesprächen teilnehmen **muss**
- **Themen** sind z. B.:
  - **Aufbau- und Ablauforganisation** (Geschäftsverteilungsplan, Organigramm)
  - Zuständigkeiten und Verantwortlichkeiten klären
  - **Vorgehensweise** darstellen
  - Abfragen, welche **Datenverarbeitungsprozesse** zum Auditgegenstand gehören
  - Abfrage der **Dokumentation für den Auditgegenstand** (ggf. schon vorab angefordert)
  - Zusammensetzung und Aufgaben des **Datenschutzmanagements** bei externen Audits
  - **Stellenwert** Datenschutz und Informationssicherheit ausloten
  - Für den nächsten **Folgetermin** Benennung der zu **prüfenden Themen** zur besseren Vorbereitung aller Beteiligten
  - Im Anschluss nach dem Auftaktgespräch ggf. kurze **Begehung** des Standortes (Außenbereich, Gebäude, Keller, Dachboden, Büro- und **Technikräume)** durchführen

3. Vor-Ort-Audit

Wie gehe ich vor Ort vor?

- Zu Beginn des Vor-Ort-Audits Treffpunkt in einem **Besprechungsraum**
- Besprechung der **Tagesordnung** und des **Tagesablaufs**
- **Vorgehensweise:**
  - **Audithandlungen** grundsätzlich nur im **Beisein ausgewählter Personen**
  - Präsentation **technischer Prüfbereiche** (z. B. Berechtigungsmanagement) über IT-Administration im Besprechungsraum über **Beamer**
  - **Begehung** der Gebäude und Räume mit Begleitung (Verantwortliche) und ggf. **Befragung** der dort angetroffenen Beschäftigten im Interviewverfahren
  - **Abweichungen** von gesetzlichen und internen Regelungen aufschreiben, z. B. **Notizbuch, Klatte oder Notebook**
  - Bei schwerwiegenden Abweichungen ggf. **Sofortmaßnahmen** einleiten
  - Nach Abschluss des Audittages ggf. **Übertragung handschriftlicher Aufzeichnungen** in z. B. Excel-Tabelle oder Word-Dokument
- **Terminfestlegung** für die **Folgetermine**

4. Abschlussgespräch

Was teile ich den Verantwortlichen mit?

- **Termin** für ein Abschlussgespräch festlegen und Beteiligte (Leitungsebene, IT-Abteilung, Fachbereiche) einladen
- Auf das Gespräch **gut vorbereiten** und **Schwerpunkte** setzen
- **Ablauf des Audits** erläutern
- Festgestellte **Sachverhalte** darstellen
- **Mängel** gewichten und **Prioritäten** festlegen
- Schwere **Verstöße** gegen die **DSGVO** oder gegen **interne Regelungen** mitteilen
- Wenn eine **Abweichung** dargestellt wird, sollte ggf. eine **Lösung** empfohlen werden
- **Strategie**, Beteiligte und **Zeitplan** für die **Beseitigung der Mängel** fordern
- Ggf. anbieten, die Mängelbeseitigung zu **unterstützen** (Beratung, Mitwirkung)

5. Auditbericht

Was schreibe ich auf und worauf muss ich achten?

- Der **Hauptadressat** des Auditberichts ist die **Verantwortliche Ebene**
- Der **Auditbericht** muss für den Adressatenkreis **verständlich** formuliert werden
- Der Auditbericht sollte folgende **Aspekte** berücksichtigen:
  - **Objektive** präzise **Sachverhaltsdarstellung** mit **datenschutzrechtlicher Bewertung**
  - **Vollständigkeit** und konstruktive Empfehlungen
  - **Qualitätssicherung** in Bezug auf **Form, Sachverhalte und Bewertung**
  - **Zeitnahe** Zustellung
- In dem Auditbericht sind die **Feststellungen** – positive Ergebnisse und Mängel bzw. Verstöße – mit einer **datenschutzrechtlichen Bewertung** darzustellen
- Den Verantwortlichen sollte mit der Zustellung des Berichts ein **Besprechungstermin** angeboten werden
- Mit den **Verantwortlichen** ist festzulegen, welche **„Geheimhaltungsstufe"** der Auditbericht erhält
- Der Auditbericht dient als **Gesprächsgrundlage** und **entlastet** den **Auditor**

Checkliste Audit

- Hat der DSB gemeinsam mit dem Verantwortlichen festgelegt, auf welche Art und Weise die **Überwachung der Einhaltung der DSGVO** durchgeführt werden soll?
- Wurde mit ihm besprochen, in welchen **Bereichen** Audits durchgeführt werden sollen?
- Sind die **Verantwortlichen der Fachbereiche** darüber informiert, dass im Rahmen eines Audits das **Datenschutz- und Informationssicherheitsniveau** überprüft wird?
- Ist allen Audit-Teilnehmern verständlich, dass das **Audit** als **Instrument für die Überwachung** der Einhaltung der **DSGVO** dient?
- Verfügt der DSB über ausreichendes **Know-how**, ein Audit nach den **best practice Standards** durchzuführen?
- Hat der DSB für die Jahresplanung ein **Auditprogramm** erstellt?
- Werden für festgelegte Auditbereiche (Scope) ggf. **weitere Experten** bzw. interne oder externe **Unterstützung** benötigt?
- Kann der DSB die Audit-Teilnehmer, z. B. im Rahmen von Informationsveranstaltungen, über **die einzelnen Schritte (Methodik) der Durchführung** eines Audits informieren?
- Ist die **Berichtsform** der **Ergebnisse des Audits** festgelegt?

Christian-Albrechts-Universität zu Kiel

Vorlesung Datenschutz SS 2025

19. Mai 2025

Vielen Dank für Ihre Aufmerksamkeit!

Heiko Behrendt
Experte für Datenschutz und Informationssicherheit
ISO 27001, ISO 27701 Lead-Auditor, Fachbegutachter der DAkkS
0179 2184795 - mail@heiko-behrendt.de - https://www.heiko-behrendt.de