Christian-Albrechts-Universität zu Kiel

Vorlesung Datenschutz SS 2024

13. Mai 2024

Der Datenschutzbeauftragte

Benennung, Stellung und Aufgaben

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

Themen

1. Regelungen der Datenschutz-Grundverordnung (DSGVO)
2. Aufgaben des Datenschutzbeauftragten
3. Aufgabenjahresplan

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.

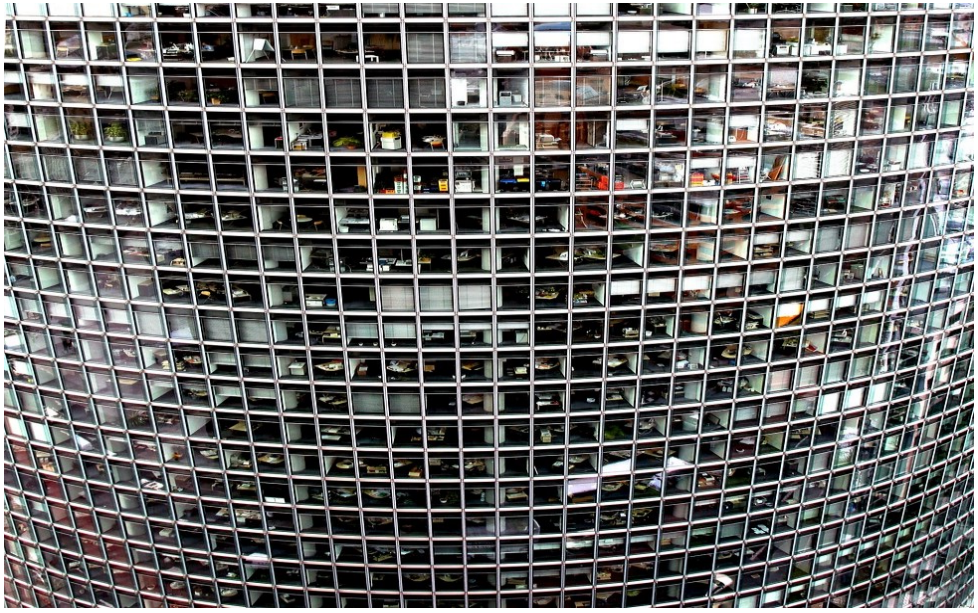
Informationsquellen zur DSGVO

- https://www.datenschutzkonferenz-online.de
- https://www.bfdi.bund.de
- https://www.datenschutzzentrum.de
- https://www.gdd.de
- https://www.datenschutz-grundverordnung.eu
- https://www.bvdnet.de (Das berufliche Leitbild des DSB)
- Working Paper 243 der Art. 29-Gruppe (Leitlinien für Datenschutzbeauftragte)
- Kurzpapier Nr. 12 Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern

Stellenwert „Datenschutz“ in der Organisation

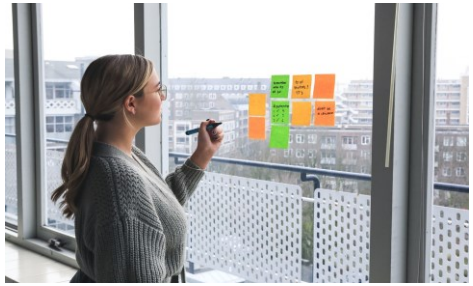
- **Ziele** der Organisation
- **Schutzbedarf** der Daten
- **Rechte** der Betroffenen
- Umgang mit **Risiken**
- Festlegung **technischer und organisatorischer Maßnahmen**
- Erkennen und Bearbeiten von **Datenschutzverletzungen**
- **Überwachung** der Vorschriften
- …

Firma Kiel-X GmbH



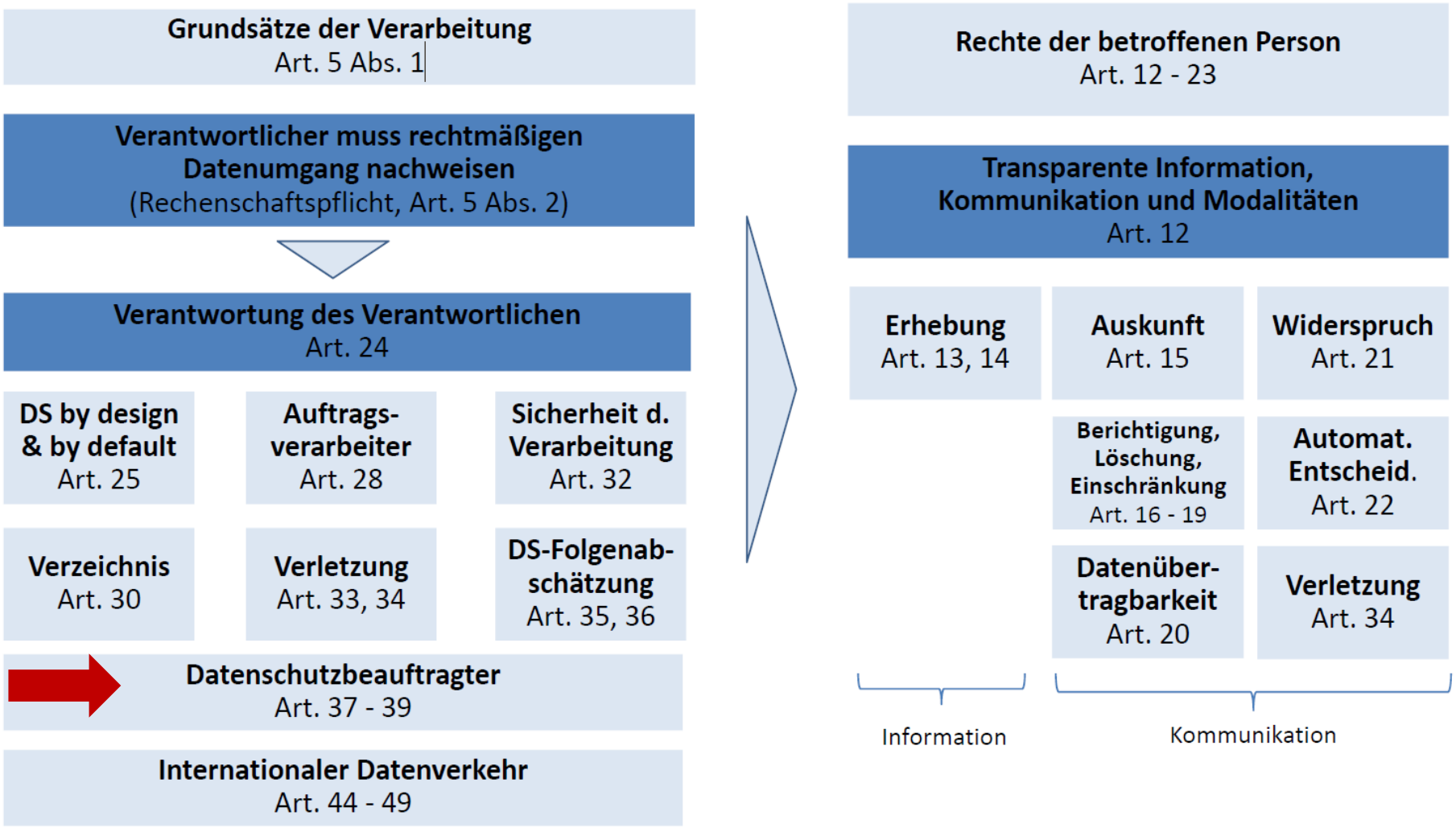
Stellenwert Datenschutz ?

Datenschutzbeauftragte ?



Quelle: https://pixabay.com/

Datenschutzregelungen



Quelle: Kranig/Sachs/Gierschmann, Datenschutz-Compliance nach der DSGVO, 2017, Bundesanzeiger Verlag

Benennung eines 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 Artikel 9 DSGVO.

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

Richtlinie (EU 2016/680) – Polizei, Justiz

Öffentliche Stellen (z. B. Behörden, CAU) und

nicht öffentliche Stellen (z. B. Schuster GmbH)

Benennung eines Datenschutzbeauftragten nicht-öffentlicher Stellen

§ 38 BDSG

§ 38 BDSG Datenschutzbeauftragte nichtöffentlicher Stellen

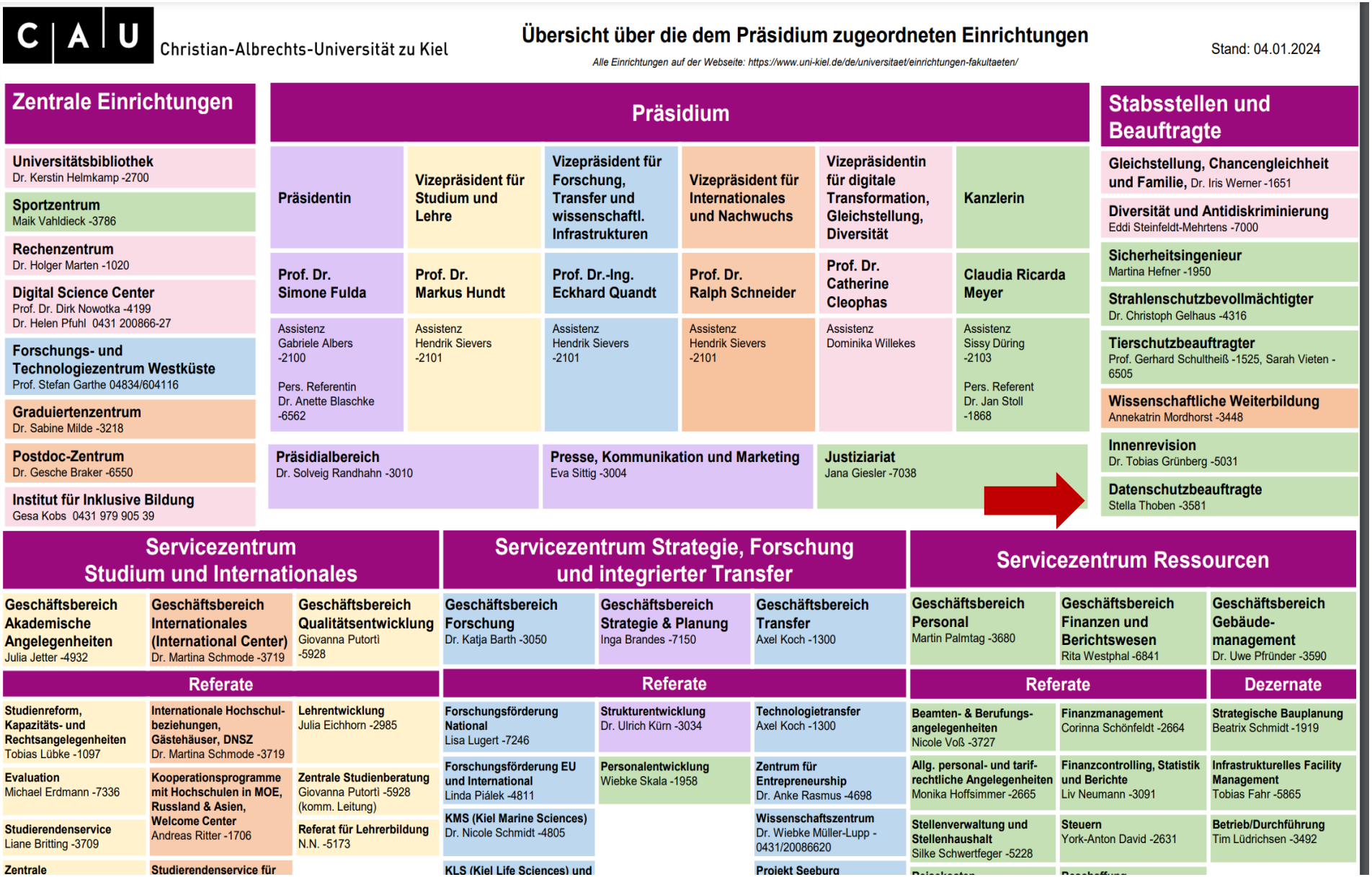
- Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 (DSGVO) benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel **mindestens 20 Personen ständig** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

- Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer **Datenschutz-Folgenabschätzung** nach Artikel 35 der Verordnung (EU) 2016/679 (DSGVO) unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum **Zweck der Übermittlung, der anonymisierten 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.

Benennung eines Datenschutzbeauftragten

Art. 37 DSGVO

- Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen **Qualifikation** und insbesondere des **Fachwissens** benannt.
- Der Verantwortliche oder der Auftragsverarbeiter **veröffentlicht** die **Kontaktdaten** des Datenschutzbeauftragten und teilt diese Daten der **Aufsichtsbehörde** mit.
- Der DSB kann **Beschäftigter der Organisation** sein **oder** seine Aufgaben auf der Grundlage eines **Dienstleistungsvertrags** erfüllen.
- Eine **Unternehmensgruppe** darf einen **gemeinsamen** Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der DSB **leicht erreicht** werden kann.
- Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine **Behörde oder öffentliche Stelle** handelt, kann ein **gemeinsamer Datenschutzbeauftragter** benannt werden. Die **Organisationsstruktur** und **Größe der Behörde** ist zu beachten.



Quelle: https://www.uni-kiel.de/gf-praesidium/de/innerer-dienstbetrieb/ordner-dateien-innerer-dienstbetrieb/organigramm

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 Artikel 39 DSGVO die **erforderlichen Ressourcen** und den **Zugang zu personenbezogenen 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** und Überwachung ihrer Durchführung gemäß Artikel 35 DSGVO
- Zusammenarbeit mit der **Aufsichtsbehörde**
- Tätigkeit als **Anlaufstelle für die Aufsichtsbehörde** in mit der Verarbeitung zusammenhängenden Fragen

Beraten und berichten: Verantwortliche informieren

Informationsaustausch

- Festlegung der **Kommunikationswege** (digital, persönlich) und Kommunikations-instrumente (E-Mail, Sharepoint, Videokonferenz)
- Durchführung von wöchentlich und anlassbezogenen **Sitzungen** im Rahmen des **Datenschutzmanagementteams** (wenn vorhanden)
- Teilnahme an **Abteilungsleitersitzungen** mit Berichtspflicht
- **Besprechung** nach Absprache mit Verantwortlichen in der **Fachabteilung**
- Durchführung zu 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)
- **Digitale Kommunikation** über Intranetdienste (E-Mail)

Überwachung: Audit, Kontrolle oder Sicherheitscheck?

Wie gehe ich bei der Überwachung der Einhaltung der DSGVO vor? Audit oder Kontrolle oder Prüfung?

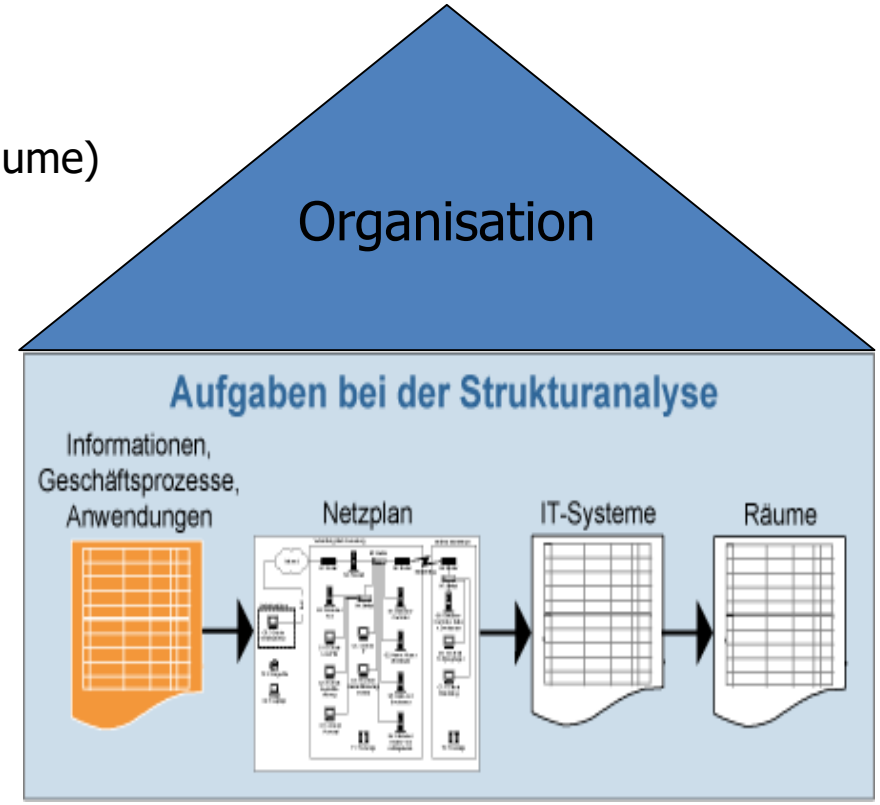
	Audit	Kontrolle Prüfung	Sicherheits-check
DSGVO überwachen	X	X	
Festlegung des Gegenstands	X	X	X
Dokumenten- und Vorortprüfung	X	X	
Einhaltung von Regelungen/ Vorschriften	X	X	
Soll-Ist-Abgleich	X	X	X
Prozessüberprüfung	X	X	X
Methodischer Ansatz	X	X	
Einbeziehung der Leitungsebene	X	X	
Positiver Ansatz	X		
Gutachten/Bericht	X		
Zertifizierung / Zertifikat	X		
Prüfbericht		X	
Konsequenzen bei Abweichungen		X	

Bestandsaufnahme – Strukturanalyse

Überblick: Welche Daten werden mit welchen IT-Komponenten an welchem Ort verarbeitet?

- Regelungen und Vorschriften
- Aufgaben, Prozesse, Fachanwendungen, Daten
- Datenkommunikation
- Infrastruktur (Gebäude, Räume)
- Hard- und Software
- Vernetzung

Quelle: https://pixabay.com/



Quelle: www.bsi.bund.de/

Auditgegenstand – Scope

Beispiele: Was kann ich im Rahmen eines Audits überwachen?

- **Organisation:** Zuständigkeiten und Aufgaben, Datenschutzmanagement
- **Infrastruktur:** Büroräume, Technikräume, Verkabelung, USV, Homeoffice, Schließsystem, Zutrittsberechtigung, Aktenaufbewahrung, Archive, Papierentsorgung, Gebäudeleittechnik
- **Dokumentation, Nachweise:** Konzepte, Richtlinien, TOMs, AV, Verfahrens-dokumentation, Test- und Freigabe, Verzeichnis der Verarbeitungstätigkeiten, DSFA
- **Berechtigungsmanagement:** Benutzerkonten- und Rechteverwaltung, Active-Directory, NTFS-Rechte auf Ordner und Dateiebene
- **Netzkommunikation:** Netzstrukturen, Netzsegmentierung, DMZ, Netzschnittstellen, Firewall, Switches, Router, VPN, WLAN, WAN
- **IT-Systeme:** Client- und Servermanagement mit Betriebssystemen, Fachanwendungen und Datenbanken, Virtualisierung, Mobile Systeme, MDM, GPO, USB
- **Datenschutzvorfall- und Notfallmanagement:** Datensicherung, Virenschutz, Patchmanagement
- **Kontrolle, Überwachung:** Protokollierung, Überprüfung, Ticketsysteme, Logdateien
- **Spezielle Themen:** z. B. Projektmanagement, Migration, TK-Anlage, Archivsysteme, Fernwartung, Auftragsverarbeiter

Anforderung an den Datenschutz-Auditor (DSB)

Was wird von dem Auditor verlangt?

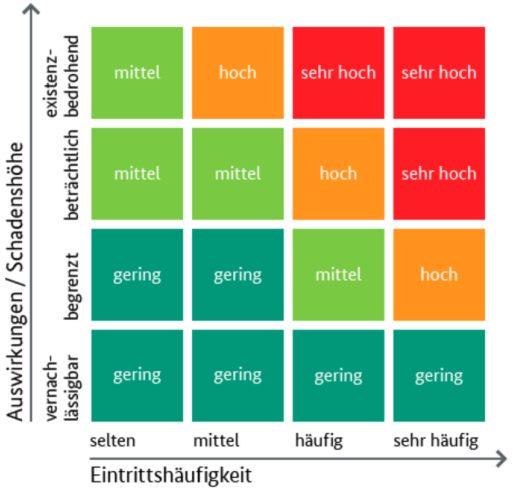
- **Rechtschaffenheit und Vertraulichkeit**
  - Er ist zur Verschwiegenheit gegenüber Dritten verpflichtet
- **Fachkompetenz**
  - Der Auditor sollte über Kenntnisse im Bereich der Prüfmethoden und zentralen Prüfungsgebiete verfügen
  - Er benötigt sowohl breites als auch tiefes Wissen auf dem Gebiet des Datenschutzrechts und der Informationssicherheit
- **Objektivität und Sorgfalt**
  - Er arbeitet objektiv berichtet ausschließlich dem Verantwortlichen
  - Er unterstützt den Verantwortlichen bei der Erreichung der Ziele
  - Er erhält ein uneingeschränktes Informationsrecht und es dürfen ihm keine Informationen vorenthalten werden
- **Sachliche Darstellung**
  - Erstellung eines Berichts mit den festgestellten Sachverhalten und einer konstruktiven Bewertung der dargestellten Sachverhalte
  - Empfehlungen zur Verbesserung der Maßnahmen und Prozesse
- **Nachweise und Nachvollziehbarkeit**
  - Dokumentation des Verlaufs – Termine, Beteiligte, Prüfmethodik, Prüfbereiche

Auditaspekte und Auditziele

Werden die Regelungen der DSGVO eingehalten?

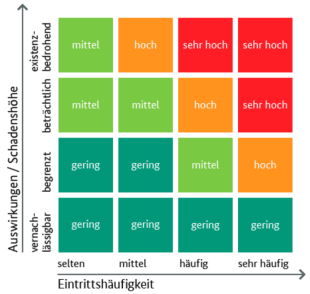
- Angemessenheit (Eignung, Zweckmäßigkeit)
- Wirksamkeit (Funktionsfähigkeit, Effektivität)
- **Rechtmäßigkeit**
- Ordnungsmäßigkeit (Compliance)
- Wirtschaftlichkeit
- **Ziele Datenschutz und Informationssicherheit**
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Intervenierbarkeit
  - Datenminimierung
  - Transparenz
  - Nichtverkettbarkeit
  - Belastbarkeit
  - Authentizität

Risikobetrachtung!
Sind die Daten ausreichend geschützt?



Der **Schutzbedarf** der Daten / Assets und somit die Auswahl der technischen und organisatorischen Maßnahmen **(TOM)** steht in Abhängigkeit zur **Eintrittswahrscheinlichkeit** und **Schwere** des **Schadens** für den Betroffenen bzw. für das Unternehme!

Gefährdungen – Risiken – Maßnahmen



DATEN – ASSETS
z. B. Personaldaten

↓

Anforderungen/Schutzbedarf
DSGVO, z. B. ISO 27001

Gefährdungen ⟷ **Maßnahmen (TOM)**

z. B. Vireninfizierung mit Ransomeware

z. B. Antivirenschutzsoftware reduziert Gefährdung und Risiko

↓ ↓

Risiko hoch = Eintrittswahrscheinlichkeit/Schadenshöhe = Risiko gering

---

Ziel: Datenschutz (und Informationssicherheit) sollen gewährleistet werden!

- Aus den festgestellten **Gefährdungen** werden die Risiken ermittelt
- Die **Maßnahmenauswahl/-gewichtung** ergibt sich jeweils aus der **Risikokritikalität**
- Je höher die **Schadensauswirkung**, desto **belastbarer** müssen die Maßnahmen sein
- Die Maßnahmen dokumentieren die **Umsetzung der Anforderungen** und den Schutz der Daten

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"

Strategie – Auditablauf

Wie gehe ich vor, was will ich fragen?

- Abfrage von Regelungen über eine zugestellte **Checkliste**
- Analyse der angeforderten **Dokumentation**
- Durchsicht von **Inventarlisten**, Konfigurations- und/oder Protokolldateien
- Aufnahme von **Beständen**, z. B. Schlüsselbestandsbuch, Datensicherungsbänder
- **Begehung** von Gebäuden, Büros, Keller, Dachböden, Server- und Technikräume
- Analyse von **Abläufen/Prozessen**, z. B. Löschen von Daten oder Papierentsorgung
- Umsetzung von **Interviews** mit Beschäftigten der Fachabteilungen
- Untersuchung / **Analyse von IT-Systemen**
- Analyse von Daten/Informationen am System, z. B. **Fachanwendungen**
- Überprüfung von **Zweigstellen** oder Auftragsverarbeitern
- …

Bewertungsmaßstab, Gesetze und Richtlinien

Was muss die Organisation beachten?

- Gesetze und interne **Vorschriften** beachten, DSGVO etc.
- Ggf. Einhaltung von **IT-Sicherheitsstandards** (z. B. BSI-Grundschutz, ISO 27001)
- **Dokumentation** (SOLL) in Abhängigkeit zum **Auditgegenstand**
  - Geschäftsverteilungsplan, Organigramm
  - Konzept über den Einsatz der **technischen Komponenten**
  - Software, **Fachanwendungen mit Daten**
  - Datensicherungskonzept
  - Virenschutzkonzept
  - Netzkonzept, Netzplan
  - Dienstanweisungen
  - Leitlinien zur Informationssicherheit und zum Datenschutz
  - Schutzbedarfsfeststellung
  - Risikoanalyse
  - **Technische und organisatorische Maßnahmen**
  - **Verzeichnis der Verarbeitungstätigkeiten**
  - Verfahrens- und Prozessbeschreibungen eingesetzter Software
  - Bestellungsurkunde und Aufgabenjahresplan DSB (Audit beim Auftragsverarbeiter)
  - Verträge / Vereinbarungen zur Auftragsverarbeitungen

Auditbericht

Was schreibe ich auf und wie gliedere ich den Auditbericht?

1. **Gegenstand** des Audits (Scope)
2. **Zeitraum** und beteiligte Personen
3. **Sachverhaltsdarstellung**
   - Objektiv
   - Rechtliche Bewertung
   - Verstöße gegen Gesetze
   - Abweichungen von internen Regelungen
4. **Verbesserungsvorschläge**
5. **Handlungsnotwendigkeit** mit Priorität

Gliederungsbeispiel:

Auditbeispiel 1 - Datenlöschung

1. **Vorbereitung**
   - Abgrenzung des Audits: Welche Fachanwendungen und Speichermedien will ich prüfen?
   - Erstellung eines Auditplans mit Checkliste
   - Um welche Gefährdungen, Risiken geht es? Welche Sensibilität haben die Daten?
   - Wie werden Daten gelöscht? Gibt es Löschungsfristen? Wie werden Datenträger entsorgt?
   - Welche Regelungen sind festgelegt worden bzw. sind zu beachten, TOMs?
2. **Auftaktgespräch**
   - Einladung der Verantwortlichen „Fachbereichsverantwortliche, IT-Abteilung"
   - Darstellung des Prüfplans und des Prüfungsablaufs
   - Fragen an Fachbereiche über vorhandene Prozesse und der organisatorischen Umsetzung
3. **Vor-Ort-Audit**
   - Analyse zweier Arbeitsplätze mit sensiblen Daten, Interview mit Beschäftigten
   - Analyse ausgewählter Fachwendungen in Bezug auf Löschfunktionen
   - Interview mit Beschäftigten der IT-Abteilung über die Datenlöschung
   - Begehung der Räume mit ausgesonderten IT-Komponenten
4. **Abschlussgespräch**
   - Kurze Darstellung der festgestellten Sachverhalte
   - Darstellung von Abweichungen, ggf. Empfehlung von Maßnahmen zur Beseitigung der Abweichungen
5. **Auditbericht**
   - Kurzer Auditbericht mit Sachverhalten, Bewertungen und Empfehlungen

Auditbeispiel 2 - Kennwortsicherheit

1. **Vorbereitung**
   - Abgrenzung des Audits: Welche Bereiche/Systeme mit Kennwörtern will ich prüfen?
   - Erstellung eines Auditplans mit Checkliste
   - Um welche Gefährdungen, Risiken geht es? Wer könnte zu Schaden kommen?
   - Gibt es Kennwortrichtlinien? Besteht eine Dienstanweisung über die Kennwortvergabe?
2. **Auftaktgespräch**
   - Einladung der Verantwortlichen „Fachbereichsverantwortliche, IT-Abteilung"
   - Fragen an IT-Abteilung über den Prozess der Kennwortverwaltung
   - Analyse über den Umgang mit Kennwörtern bei Beschäftigten der Fachabteilungen
   - Abfrage der Kennwortrichtlinien (Kennwortkomplexität, Falscheingabe etc.)
3. **Vor-Ort-Audit**
   - Analyse der Systemeinstellungen (AD-Gruppenrichtlinien, Fachanwendungen)
   - Ggf. Prüfen der Umsetzung einer Zweifaktor-Authentifizierung für z. B. die Administration
   - Prüfen des Prozesses für die Beantragung eines Benutzerkontos und des Kennworts
   - Verwendung und Verwaltung der Kennwörter im administrativen Bereich (IT-Abteilung)
   - Behandlung von Kennwörtern für Standard-Administrationskonten der IT-Komponenten
4. **Abschlussgespräch**
   - Kurze Darstellung der festgestellten Sachverhalte
   - Empfehlung über den Einsatz einer Software für die professionelle Verwaltung von administrativen Kennwörtern (z. B. KeePass, Pleasant Passwort Server)
5. **Auditbericht**
   - Kurzer Auditbericht mit Sachverhalten, Bewertungen und Empfehlungen

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 mit sensiblen Daten (Datenschutz-Folgenabschätzung) • Mitwirkung/Beratung der Verantwortlichen bei der Umsetzung der DSFA • Unterstützung bei der Dokumentation und der Erstellung der Risikoanalyse • Mitwirkung bei der Nutzung des Tools PIA (privacy impact assessment) CNIL für die DSF	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*

Berufsverband der Datenschutzbeauftragten

BvD e.V.

DATENSCHUTZ GESTALTEN

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/berufsbild/

ARTIKEL-29-DATENSCHUTZGRUPPE

Der Europäische Datenschutzausschuss – EDSA

16/DE
WP 243 rev.01

Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“)

angenommen am 13. Dezember 2016

zuletzt überarbeitet und angenommen am 5. April 2017

Inhaltsverzeichnis

Quelle: https://www.datenschutzkonferenz-online.de/media/wp/20170405_wp243_rev01.pdf

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

Christian-Albrechts-Universität zu Kiel

Vorlesung Datenschutz SS 2024

13. Mai 2024

Vielen Dank für Ihre Aufmerksamkeit!

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