ds²

Integrierter Datenschutz

Rechenschaftspflicht

ds² Unternehmensberatung GmbH & Co. KG

Rechenschaftspflicht in der DSGVO

European Data Protection Supervisor:

"Eine der wichtigsten Neuerungen der neuen Datenschutzverordnung ist die Einbeziehung des **Grundsatzes der Rechenschaftspflicht,** der im Wettbewerbsrecht gut etabliert, im Datenschutzrecht jedoch relativ neu ist."

https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf

Rechenschaftspflicht in der DSGVO

Umsetzung der datenschutzrechtlichen Rechenschaftspflicht – Was bedeutet das im Detail?

©fotomek - stock.adobe.com

Rechenschaftspflicht in der DSGVO

Prüfung des BayLDA 2018

Start: 01.10.2018 Ende: offen

Kurzbeschreibung	Die DS-GVO verlangt vom Verantwortlichen, dass die Einhaltung der DS-GVO nachgewiesen wird (Art. 5 Abs. 2 DS-GVO). Diese "Rechenschaftspflicht" stellt vom Grundsatz her eine "Nachweislast-Umkehr" dar, was bedeutet, dass die Einhaltung der gesetzlichen Anforderungen der Aufsichtsbehörde bei einer Kontrolle dargestellt werden muss. Konkret bedeutet dies, dass sowohl die Aufbauorganisation bei großen Unternehmen so gestaltet ist, dass neben dem betrieblichen Datenschutzbeauftragten weitere Akteure (z.B. Rechts-/Complianceabteilung oder IT-Sicherheit) sich mit datenschutzrechtlichen Anforderungen beschäftigen. Des Weiteren müssen in der sogenannten Ablauforganisation drei Kernprozesse im Unternehmen wirksam ausgestaltet sein: 1. Datenschutzkonforme Verarbeitung 2. Umgang mit Betroffenenrechten 3. Umgang mit Datenschutzverletzungen Ziel der Prüfung ist vereinfacht gesprochen, die Einhaltung der Datenschutzgrundverordnung im Unternehmensalltag bei großen Unternehmen, festzustellen.
Prüfgrundlage	Art. 5 Abs. 2 DS-GVO Art. 24 DS-GVO
Zielgruppe	(Groß-)Konzerne und Datengetriebene Unternehmen

https://www.lda.bayern.de/de/kontrollen.html

Rechenschaftspflicht in der DSGVO

Die **Grundsätze für die Verarbeitung personenbezogener Daten** finden sich in **Art. 5 Abs. 1 DS-GVO**:

a) Rechtmäßigkeit, Treu und Glauben, Transparenz

b) Zweckbindung

c) Datenminimierung

d) Datenrichtigkeit

e) Speicherbegrenzung

f) Sicherheit der Verarbeitung

Der Verantwortliche ist für die Einhaltung dieser Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können. **(„Rechenschaftspflicht“), Art. 5 Abs. 2 DS-GVO**

Rechenschaftspflicht in der DSGVO

Worin besteht also ist die Herausforderung?

→ auf Nachfrage der Aufsichtsbehörde belegen können,

dass die Vorgaben der DSGVO erfüllt werden.

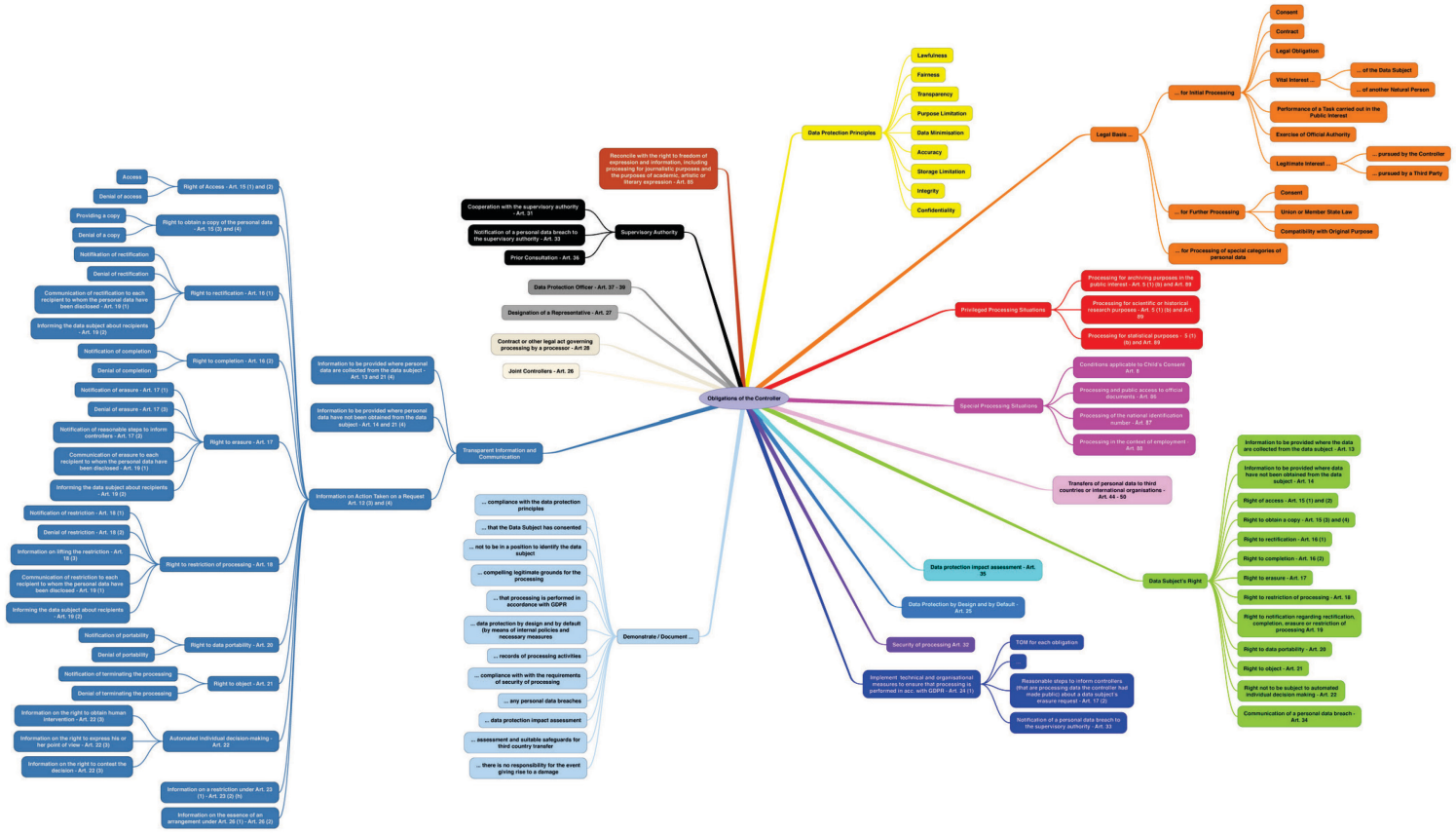
©fotomek - stock.adobe.com

Rechenschaftspflicht in der DSGVO

Bedeutet **Rechtmäßigkeit,** dass Verstöße gegen die DS-GVO die Rechtmäßigkeit der Verarbeitung insgesamt in Frage stellen?

Rechenschaftspflicht in der DSGVO

Pflichten in der DS-GVO



https://dataprotection-landscape.com/file/mindmap_o.02.jpg

Dialogfelder | Recht | DSGVO:Pflichten Kachel 2

Rechenschaftspflicht in der DSGVO

Rechtmäßigkeit nach Art. 5 Abs. 1 a) DS-GVO

→ Vorlagefrage an den EuGH In der Rechtssache C-60/22

*„**Führt eine fehlende bzw. unterlassene oder unvollständige Rechenschaftspflicht** eines Verantwortlichen nach Art. 5 der DS-GVO, **z. B.** durch ein fehlendes oder unvollständiges Verzeichnis der Verarbeitungstätigkeiten **nach Art. 30 DS-GVO oder** eine fehlende Vereinbarung über ein gemeinsames Verfahren **nach Art. 26 DS-GVO** dazu, **dass die Datenverarbeitung unrechtmäßig im Sinne der Art. 17 Abs. 1 Buchst. d DS-GVO und Art. 18 Abs. 1 Buchst. b DS-GVO ist**, so dass ein Löschungs- bzw. Beschränkungsanspruch des Betroffenen besteht?“*

©fotomek - stock.adobe.com

Rechenschaftspflicht in der DSGVO

Rechtmäßigkeit nach Art. 5 Abs. 1 a) DS-GVO

Antwort auf die Vorlagefrage an den EuGH vom 04.05.2023

- aus der Struktur und Systematik der DS-GVO geht eindeutig hervor, dass sie zwischen den „Grundsätzen“(Art. 5 - 11) und den „allgemeinen Pflichten“ unterscheidet
- Unterscheidung spiegelt auch bei der Regelung zu den Sanktionen in Kapitel VIII der DS-GVO wider
- Ziel der DS-GVO besteht insbesondere darin, ein hohes Niveau des Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen – insbesondere ihres in Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union und in Art. 16 Abs. 1 AEUV verankerten Rechts auf Privatleben – bei der Verarbeitung personenbezogener Daten zu gewährleisten
- Verstoß gegen einzelne Pflicht reicht „für sich genommen nicht aus, um nachzuweisen, dass ein Verstoß gegen das Grundrecht auf den Schutz personenbezogener Daten vorliegt“ (Rn 65).

Rechenschaftspflicht in der DSGVO

Rechtmäßigkeit nach Art. 5 Abs. 1 a) DS-GVO

Antwort auf die Vorlagefrage an den EuGH vom 04.05.2023

„Folglich ist auf die erste Frage zu antworten, dass Art. 17 Abs. 1 Buchst. d und Art. 18 Abs. 1 Buchst. b der DS-GVO dahin auszulegen sind, ***dass der Verstoß eines Verantwortlichen gegen die Pflichten aus den Art. 26 und 30 dieser Verordnung*** *über den Abschluss einer Vereinbarung zur Festlegung der gemeinsamen Verantwortung für die Verarbeitung bzw. das Führen eines Verzeichnisses von Verarbeitungstätigkeiten* ***keine unrechtmäßige Verarbeitung darstellt****, die der betroffenen Person ein Recht auf Löschung oder auf Einschränkung der Verarbeitung verleiht, weil dieser Verstoß als solcher nicht bedeutet, dass der Verantwortliche gegen den Grundsatz der „Rechenschaftspflicht“ im Sinne von Art. 5 Abs. 2 in Verbindung mit Art. 5 Abs. 1 Buchst. a und Art. 6 Abs. 1 Unterabs. 1 der DS-GVO verstößt.“*

https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

Rechenschaftspflicht in der DSGVO

Art. 5 Abs. 1 DS-GVO Personenbezogene Daten müssen …

lit. f) in einer Weise verarbeitet werden, die eine
angemessene Sicherheit

- der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung
- durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

→ Verpflichtung angemessene Sicherheit der Verarbeitung gewährleisten

Rechenschaftspflicht in der DSGVO

Verantwortung des für die Verarbeitung Verantwortlichen (Art. 24 DSGVO)

Der Verantwortliche setzt

- unter Berücksichtigung
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen
- geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den **Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.**

Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

©fotomek - stock.adobe.com

Rechenschaftspflicht in der DSGVO

Auftragsverarbeiter (Art. 28 DSGVO)

- bietet hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet
- ist Träger von rechtlichen und vertraglichen Pflichten und für deren Einhaltung ggf. nachweispflichtig

Rechenschaftspflicht in der DSGVO

- Art. 24 Abs. 1, Art. 25 Abs. 1 und Art. 32 Abs. 1 DS-GVO enthalten Vorgaben von Rahmenbedingungen, d.h. Kriterien für die Festlegung der technischen und organisatorischen Maßnahmen
  - ➢ Vorgabe für die Umsetzung in der Praxis
- Art. 5 Abs. 1 und 2 enthalten derartige Vorgaben jedoch nicht

Rechenschaftspflicht in der DSGVO

Art. 5 Abs. 1 DS-GVO Personenbezogene Daten müssen …

lit. f) in einer Weise verarbeitet werden, die eine
angemessene Sicherheit

- der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung
- durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

→ Verpflichtung angemessene Sicherheit der Verarbeitung zu gewährleisten

- (2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können
  (= Rechenschaftspflicht)

→ Dokumentation für Nachweisbarkeit sicherstellen, aber anhand der Maßstäbe von Art. 25, 32 DS-GVO

Rechenschaftspflicht in der DSGVO

Verantwortung des für die Verarbeitung Verantwortlichen (Art. 24 DSGVO)

Der Verantwortliche setzt

- unter Berücksichtigung
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen
- geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den **Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.**

Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

©fotomek - stock.adobe.com

Rechenschaftspflicht in der DSGVO

Bayerischer Landesbeauftragter für den Datenschutz, Bayerisches Landesamt für Datenschutzaufsicht beschreibt die Anforderungen an das Datenschutzmanagement in bayerischen öffentlichen und privaten Krankenhäusern:

> *„Nachweisbarkeit bedeutet insbesondere,* ***dass die gemäß dem Risiko für die Rechte und Freiheiten ausgewählten Maßnahmen*** *(siehe vor allem Art. 24 Abs. 1 und 2, Art. 32 DSGVO)* ***so gewählt, umgesetzt, dokumentiert und auf Wirksamkeit überprüft werden****,* ***dass sie jederzeit umfassend und schnell*** *– etwa im Rahmen einer Datenschutzprüfung –* ***dargelegt werden können****.*
> *[…]*
>
> *Öffentliche wie private Krankenhäuser sollten deshalb* ***ein Datenschutzmanagement einrichten****, aus dem heraus alle Fragen des Datenschutzes schnell und umfassend behandelt werden können.“*

https://www.datenschutz-bayern.de/2/kh_leitfaden_datenschutzmanagement.pdf

Rechenschaftspflicht in der DSGVO

- Datenschutz-Managementsystem mit PDCA-Zyklus zur Erfüllung der Nachweis- und Rechenschaftspflichten implementieren
- Prozesse beschreiben

Gutes Gelingen!

©fotomek - stock.adobe.com

Integrierter Datenschutz

Herzlichen Dank für Ihre Aufmerksamkeit!

Fragen oder Anregungen? – Bitte melden Sie sich gerne:

Andrea Backer-Heuveldop
ds² Unternehmensberatung GmbH & Co. KG
Falkenstraße 10
33775 Versmold

Zentrale: +49 5423 95 993 20
andrea.heuveldop@ds-quadrat.de