Risiko und Rechenschaftspflicht – Anforderungen der DSGVO in die Praxis übersetzen

Dr. h.c. Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein, DE

Vortrag auf der Jahrestagung der Datenschutzbeauftragten
am 04.05.2023 in Graz

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

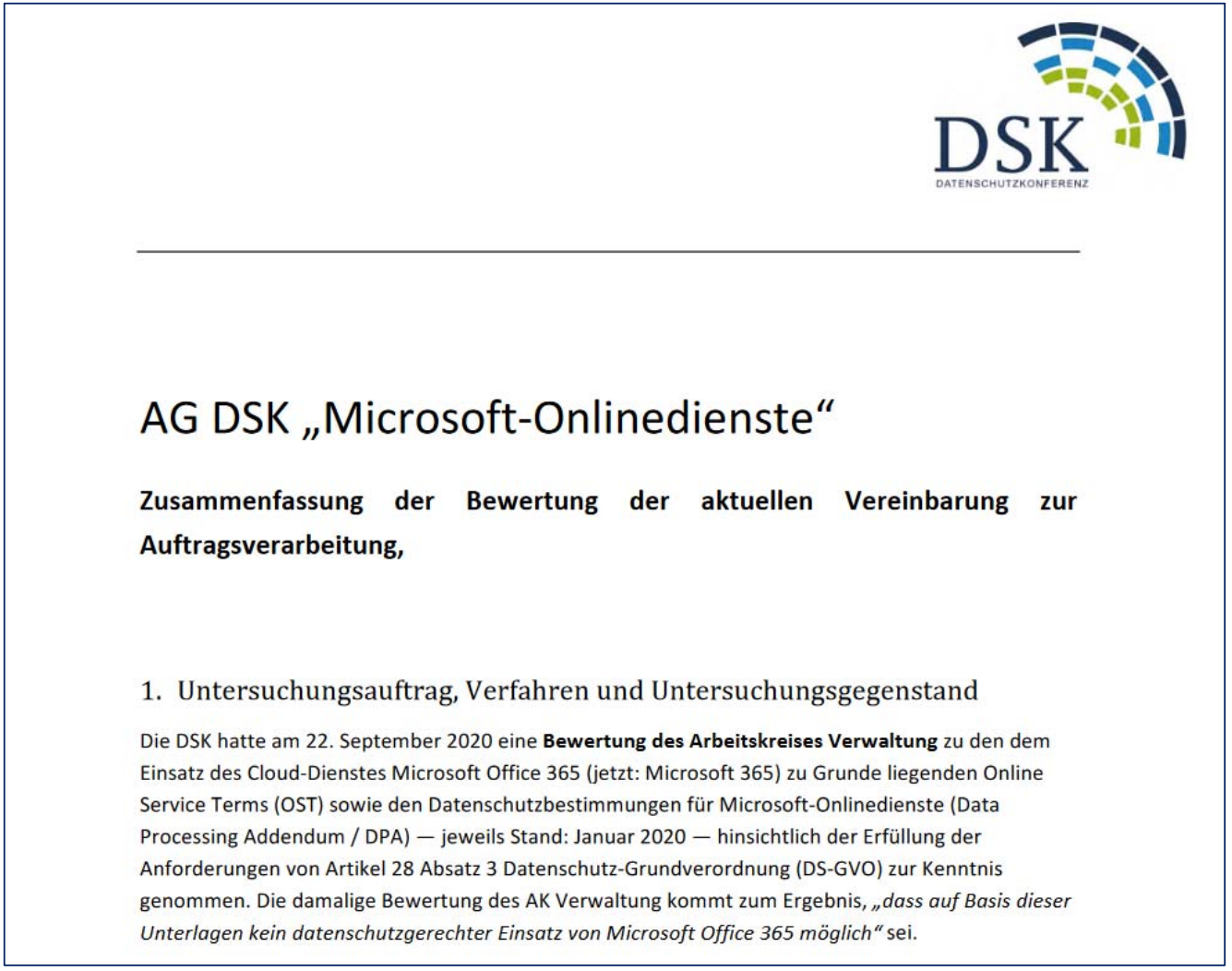
 Bild: Gerd Altmann via Pixabay

Überblick

- Warum das Thema?
- Was bedeutet die Rechenschaftspflicht?
- Gibt es einen Zusammenhang mit dem Risiko?
- Was ist zu tun?
- Hilfestellungen
- Fazit

Motivation

- Prüfung / Diskussion „Microsoft-Onlinedienste“
- 09/2020-11/2022
- Zahlreiche Gespräche
- Zahlreiche Veränderungen



DSK
DATENSCHUTZKONFERENZ

AG DSK „Microsoft-Onlinedienste“

Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung,

1. Untersuchungsauftrag, Verfahren und Untersuchungsgegenstand

Die DSK hatte am 22. September 2020 eine **Bewertung des Arbeitskreises Verwaltung** zu den dem Einsatz des Cloud-Dienstes Microsoft Office 365 (jetzt: Microsoft 365) zu Grunde liegenden Online Service Terms (OST) sowie den Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) — jeweils Stand: Januar 2020 — hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) zur Kenntnis genommen. Die damalige Bewertung des AK Verwaltung kommt zum Ergebnis, *„dass auf Basis dieser Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich“* sei.

https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

Zentrale und wiederkehrende Fragestellung der Gesprächsreihe war es, in welchen Fällen Microsoft als Auftragsverarbeiter tätig ist und in welchen als Verantwortlicher. Dies konnte nicht abschließend geklärt werden.

Verantwortliche müssen jederzeit in der Lage sein, ihrer **Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO** nachzukommen. Beim Einsatz von Microsoft 365 lassen sich hierbei auf Grundlage des „Datenschutznachtrags“ weiterhin Schwierigkeiten erwarten, da Microsoft nicht vollumfänglich offenlegt, **welche Verarbeitungen im Einzelnen stattfinden.** Zudem legt Microsoft weder vollständig dar, welche Verarbeitungen im Auftrag des Kunden noch welche zu eigenen Zwecken stattfinden. **Die Vertragsunterlagen sind in der Hinsicht nicht präzise** und erlauben im Ergebnis nicht abschließend bewertbare, ggf. sogar umfangreiche Verarbeitungen auch zu eigenen Zwecken.

https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

Zentrale und wiederkehrende Fragestellung der Gesprächsreihe war es, in welchen Fällen Microsoft als Auftragsverarbeiter tätig ist und in welchen als Verantwortlicher. Dies konnte nicht abschließend geklärt werden.

Verantwortliche müssen jederzeit in der Lage sein, ihrer **Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO** nachzukommen. Beim
„Datenschutznachtrags“ we
offenlegt, **welche Verarbeit**
dar, welche Verarbeitunger
Vertragsunterlagen sind in
bewertbare, ggf. sogar umf

3.5. Löschung und Rückgabe personenbezogener Daten

Microsoft hat der Arbeitsgruppe die einzelnen Löschprozesse erläutert. Die Erläuterungen zeigen mit Ausnahme des Sonderfalls der Verarbeitung auftragsgegenständlicher Daten zu Zwecken der „Cyberabwehr“, dass auch Verarbeitungen für Geschäftszwecke von Microsoft die Löschfristen für personenbezogene Daten nicht verlängern sollten. Zudem haben sich im Zuge der Umgestaltung des „Datenschutznachtrags“ auch Änderungen in Bezug auf Löschung ergeben, die allerdings auch Unklarheiten und Widersprüche mit sich bringen.

Nach Bewertung der Arbeitsgruppe genügt die Ausgestaltung der Rückgabe- und Löschverpflichtung **nicht in jedem Fall den gesetzlichen Anforderungen** aus Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe g DSGVO. Verantwortliche können wegen der Unklarheit der Regelungen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 i.V.m. Art. 5 Abs. 1 Buchstabe a DSGVO nicht nachkommen.

https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

InfoCuria
Rechtsprechung

Deutsch (de)

Sprache des Dokuments : Deutsch ECLI:EU:C:2023:373 Ausdrucken

URTEIL DES GERICHTSHOFS (Fünfte Kammer)

4. Mai 2023(*)

„Vorlage zur Vorabentscheidung – Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten – Verordnung (EU) 2016/679 – Art. 5 – Grundsätze für die Verarbeitung – Rechenschaftspflicht im Hinblick auf die Verarbeitung – Art. 6 – Rechtmäßigkeit der Verarbeitung – Von einer Verwaltungsbehörde erstellte elektronische Akte über einen Asylantrag – Übermittlung an das zuständige nationale Gericht über ein elektronisches Postfach – Verstoß gegen Art. 26 und 30 – Keine Vereinbarung zur Festlegung der gemeinsamen Verantwortlichkeit und kein Führen eines Verzeichnisses von Verarbeitungstätigkeiten – Folgen – Art. 17 Abs. 1 – Recht auf Löschung (Recht auf ‚Vergessenwerden') – Art. 18 Abs. 1 – Recht auf Einschränkung der Verarbeitung – Begriff ‚unrechtmäßige Verarbeitung' – Berücksichtigung der elektronischen Akte durch ein nationales Gericht – Keine Einwilligung der betroffenen Person"

In der Rechtssache C-60/22

betreffend ein Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht vom Verwaltungsgericht Wiesbaden (Deutschland) mit Beschluss vom 27. Januar 2022, beim Gerichtshof eingegangen am 1. Februar 2022, in dem Verfahren

Bild: Gerd Altmann via Pixabay

Überblick

- Warum das Thema?
- Was bedeutet die Rechenschaftspflicht?
- Gibt es einen Zusammenhang mit dem Risiko?
- Was ist zu tun?
- Hilfestellungen
- Fazit

22. „betroffene Aufsichtsbehörde“ eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

a) der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,

b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder

c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

23. „grenzüberschreitende Verarbeitung“ entweder

a) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder

b) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

24. „maßgeblicher und begründeter Einspruch“ einen Einspruch gegen einen Beschlussentwurf im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder ob beabsichtigte Maßnahmen gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen;

25. „Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates (1);

26. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

KAPITEL II

Grundsätze

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

(1) Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

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“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Artikel 6

Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

Blick in die DSGVO

Art. 5 Abs. 2 DSGVO

Accountability calls for documentation

- Anforderung der Rechenschaftspflicht
- Art. 5 (2) DSGVO

- „Demonstrate compliance" – wie?

Artikel 5 (2) DSGVO

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Article 5 (2) GDPR

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Artikel 42

Zertifizierung

(1) Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen wird Rechnung getragen.

(2) Zusätzlich zur Einhaltung durch die unter diese Verordnung fallenden Verantwortlichen oder Auftragsverarbeiter können auch datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen, die gemäß Absatz 5 des vorliegenden Artikels genehmigt worden sind, vorgesehen werden, um nachzuweisen, dass die Verantwortlichen oder Auftragsverarbeiter, die gemäß Artikel 3 nicht unter diese Verordnung fallen, im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen nach Maßgabe von Artikel 46 Absatz 2 Buchstabe f geeignete Garantien bieten. Diese Verantwortlichen oder Auftragsverarbeiter gehen mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung ein, diese geeigneten Garantien anzuwenden, auch im Hinblick auf die Rechte der betroffenen Personen.

(3) Die Zertifizierung muss freiwillig und über ein transparentes Verfahren zugänglich sein.

Blick in die DSGVO

Art. 42 DSGVO: Zertifizierung

EuGH zur Rechenschaftspflicht: Urteil vom 24.02.2022 – C-175/20, Rn. 77 ff.

Vorlagefrage 9
„Anhand welcher Kriterien ist zu prüfen, ob die Steuerverwaltung als für die Verarbeitung Verantwortliche sicherstellt, dass die Datenverarbeitung im Einklang mit den Anforderungen nach Art. 5 Abs. 1 der Verordnung 2016/679 erfolgt (Rechenschaftspflicht)?"

77 In diesem Zusammenhang ist darauf hinzuweisen, dass der für die Verarbeitung Verantwortliche nach dem in Art. 5 Abs. 2 der Verordnung 2016/679 verankerten Grundsatz der Rechenschaftspflicht nachweisen können muss, dass er die in Abs. 1 dieses Artikels festgelegten Grundsätze für die Verarbeitung personenbezogener Daten einhält.

78 Folglich obliegt es der lettischen Steuerverwaltung, nachzuweisen, dass sie gemäß Art. 25 Abs. 2 dieser Verordnung versucht hat, die Menge der zu erhebenden personenbezogenen Daten so gering wie möglich zu halten.

81 Wie sich oben aus Rn. 77 ergibt, obliegt die Beweislast insoweit der lettischen Steuerverwaltung.

https://curia.europa.eu/juris/document/document.jsf?text=&docid=254583&pageIndex=0&doclang=DE

EuGH zur Rechenschaftspflicht: Urteil vom 04.05.2023 – C-60/22, Rn. 53 ff.

38 Unter diesen Umständen hat das Verwaltungsgericht Wiesbaden beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. 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?

https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&doclang=DE

EuGH zur Rechenschaftspflicht: Urteil vom 04.05.2023 – C-60/22, Rn. 53 ff.

38 Unter diesen Umständen hat das Verwaltungsgericht Wiesbaden beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. 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?

https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&doclang=DE

EuGH zur Rechenschaftspflicht: Urteil vom 04.05.2023 – C-60/22, Rn. 53 ff.

38 Unter diesen Umständen hat das Verwaltungsgericht Wiesbaden beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende Fragen zur Vorabentscheidung vorzulegen:

1. Führt eine fehlende bzw. unterlassene oder unvollständige Rechenschaftspflicht eines V
z. B. durch ein fehlendes od
Verarbeitungstätigkeiten nac
Vereinbarung über ein geme
dazu, dass die Datenverarbe
Abs. 1 Buchst. d DS-GVO un
dass ein Löschungs- bzw. Be
besteht?

53 Nach dem Wortlaut von Abs. 2 des Art. 5 der DS-GVO ist der Verantwortliche nach dem in dieser Bestimmung verankerten Grundsatz der „Rechenschaftspflicht" für die Einhaltung des Abs. 1 dieses Artikels verantwortlich und muss nachweisen können, dass jeder der dort genannten Grundsätze eingehalten worden ist; mithin obliegt ihm hierfür die Beweislast (vgl. in diesem Sinne Urteil vom 24. Februar 2022, Valsts ieņēmumu dienests [Verarbeitung personenbezogener Daten für steuerliche Zwecke], C-175/20, EU:C:2022:124, Rn. 77, 78 und 81).

54 Hieraus folgt, dass der Verantwortliche nach Art. 5 Abs. 2 in Verbindung mit Art. 5 Abs. 1 Buchst. a der DS-GVO sicherstellen muss, dass die von ihm durchgeführte Datenverarbeitung „rechtmäßig" ist.

https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&doclang=DE

EuGH zur Rechenschaftspflicht: Urteil vom 04.05.2023 – C-60/22, Rn. 53 ff.

58 Da die Art. 7 bis 11 der DS-GVO, die genau wie die Art. 5 und 6 dieser Verordnung in deren Kapitel II stehen, das die Grundsätze betrifft, zum Ziel haben, den Umfang der dem Verarbeiter nach Art. 5 Abs. 1 Buchst. a und Art. 6 Abs. 1 dieser Verordnung obliegenden Pflichten näher zu bestimmen, ist die Verarbeitung personenbezogener Daten, wie sich aus der Rechtsprechung des Gerichtshofs ergibt, zudem nur rechtmäßig, wenn sie diese anderen Bestimmungen des genannten Kapitels einhält, die im Wesentlichen die Einwilligung, die Verarbeitung besonderer Kategorien sensibler personenbezogener Daten und die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten betreffen […]

59 […] festzustellen, dass die Einhaltung der in Art. 26 der DS-GVO vorgesehenen Pflicht zum Abschluss einer Vereinbarung zur Festlegung der gemeinsamen Verantwortung und der in Art. 30 dieser Verordnung verankerten Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu führen, nicht zu den in Art. 6 Abs. 1 Unterabs. 1 genannten Gründen für die Rechtmäßigkeit der Verarbeitung zählen.

https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&doclang=DE

EuGH zur Rechenschaftspflicht: Urteil vom 04.05.2023 – C-60/22, Rn. 53 ff.

58 Da die Art. 7 bis 11 der DS-GVO, die genau wie die Art. 5 und 6 dieser Verordnung in deren Kapitel II stehen, das die Grundsätze betrifft, zum Ziel haben, den Umfang der dem Verarbeiter nach Art. 5 Abs. 1 Buchst. a und Art. 6 Abs. 1 dieser Verordnung obliegenden Pflichten näher zu b
Daten, wie sich aus der Rechtsp
rechtmäßig, wenn sie diese and
die im Wesentlichen die Einwilli
sensibler personenbezogener Da
Daten über strafrechtliche Verur

59 […] festzustellen, dass die Einha
zum Abschluss einer Vereinbaru
und der in Art. 30 dieser Verord
Verarbeitungstätigkeiten zu führ
genannten Gründen für die Rech

60 Darüber hinaus besteht das Ziel der Art. 26 und 30 der DS-GVO im Unterschied zu den Art. 7 bis 11 dieser Verordnung nicht darin, den Umfang der in Art. 5 Abs. 1 Buchst. a und Art. 6 Abs. 1 der Verordnung genannten Anforderungen näher zu bestimmen.

61 Daher lässt sich aus dem Wortlaut von Art. 5 Abs. 1 Buchst. a und Art. 6 Abs. 1 Unterabs. 1 der DS-GVO ableiten, dass ein Verstoß des Verarbeiters gegen die in den Art. 26 und 30 dieser Verordnung vorgesehenen Pflichten keine „unrechtmäßige Verarbeitung“ im Sinne von Art. 17 Abs. 1 Buchst. d und Art. 18 Abs. 1 Buchst. b der Verordnung darstellt, die sich aus einem Verstoß des Verarbeiters gegen den in Art. 5 Abs. 2 der DS-GVO genannten Grundsatz der „Rechenschaftspflicht“ ergeben würde.

https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&doclang=DE

Bild: Gerd Altmann via Pixabay

Überblick

- Warum das Thema?
- Was bedeutet die Rechenschaftspflicht?
- Gibt es einen Zusammenhang mit dem Risiko?
- Was ist zu tun?
- Hilfestellungen
- Fazit

Der Risiko-Begriff in der DSGVO

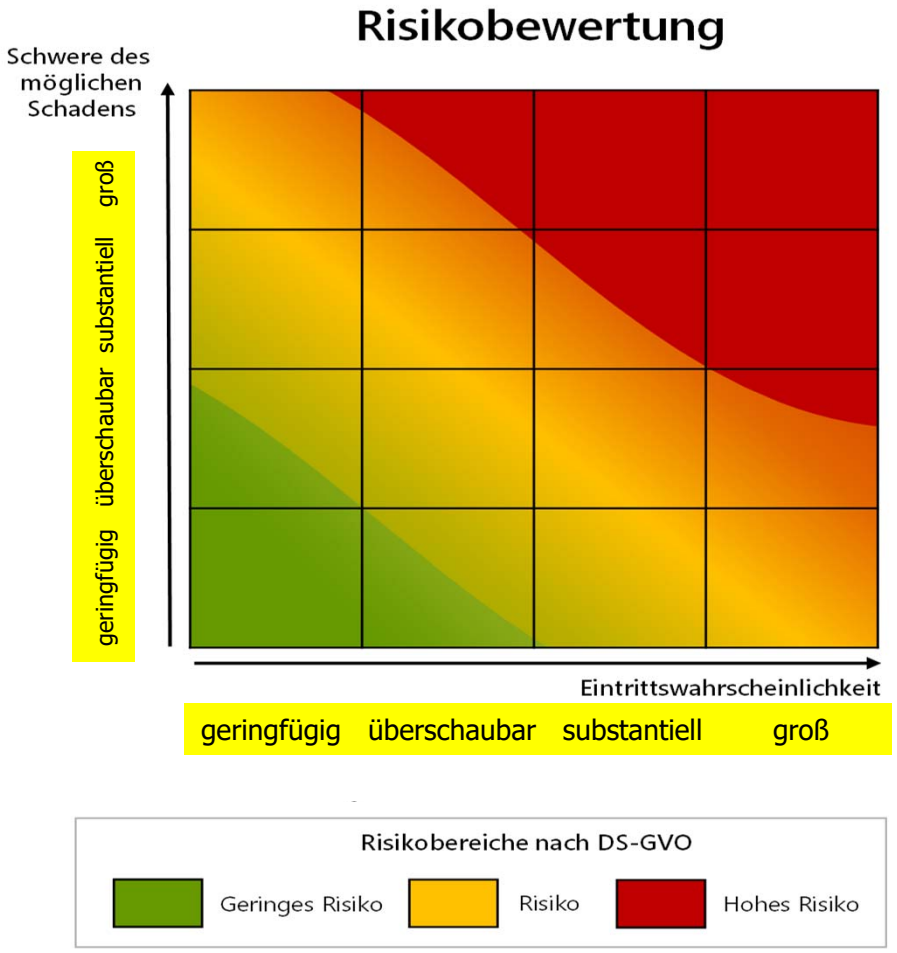
- Risiko = Schwere möglicher Schäden x Eintrittswahrscheinlichkeit
- Lässt sich nicht völlig quantifizieren
- Kann aber objektiv bestimmt werden

- Risiken müssen mit technischen und organisatorischen Maßnahmen eingedämmt werden

→ Artt. 24, 25, 32, 35 DSGVO

Risiko für die Rechte und Freiheiten natürlicher Personen
(≠ Risiken der Cybersicherheit)

https://www.datenschutzzentrum.de/artikel/1225-.html



In Art. 5 DSGVO steht doch gar nicht „Risiko"

Bild: David Mark via Pixabay

Wie genau muss die Dokumentation sein? – Nachvollziehbarkeit für die Zielgruppe

Wie genau muss der Verantwortliche die Verarbeitung und die Risiken kennen?

Zielorientiert: „can demonstrate compliance"

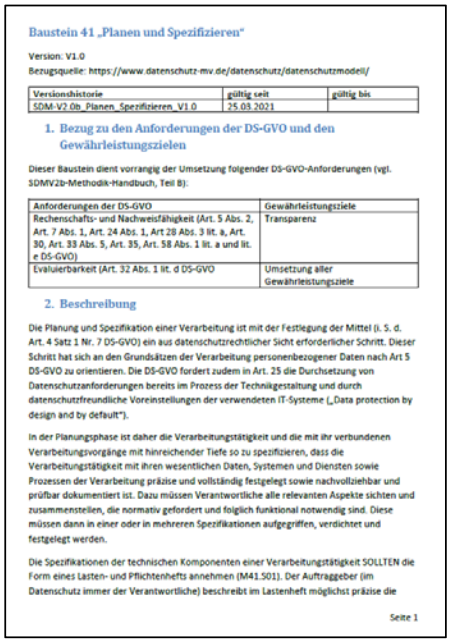
Bild: Gerd Altmann via Pixabay

Überblick

- Warum das Thema?
- Was bedeutet die Rechenschaftspflicht?
- Gibt es einen Zusammenhang mit dem Risiko?
- Was ist zu tun?
- Hilfestellungen
- Fazit

Dokumentation – eigentlich ein Oberbegriff

Planen und Spezifizieren



Baustein 41 „Planen und Spezifizieren“

Version: V1.0
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Versionshistorie	gültig seit	gültig bis
SDM-V2.0b_Planen_Spezifizieren_V1.0	25.03.2021	

1. Bezug zu den Anforderungen der DS-GVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO-Anforderungen (vgl. SDMV2b-Methodik-Handbuch, Teil B):

Anforderungen der DS-GVO	Gewährleistungsziele
Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2, Art. 7 Abs. 1, Art. 24 Abs. 1, Art 28 Abs. 3 lit. a, Art. 30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e DS-GVO)	Transparenz
Evaluierbarkeit (Art. 32 Abs. 1 lit. d DS-GVO	Umsetzung aller Gewährleistungsziele

2. Beschreibung

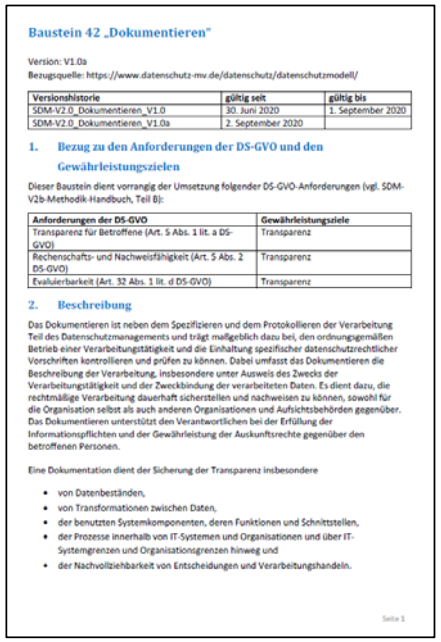
Die Planung und Spezifikation einer Verarbeitung ist mit der Festlegung der Mittel (i. S. d. Art. 4 Satz 1 Nr. 7 DS-GVO) ein aus datenschutzrechtlicher Sicht erforderlicher Schritt. Dieser Schritt hat sich an den Grundsätzen der Verarbeitung personenbezogener Daten nach Art 5 DS-GVO zu orientieren. Die DS-GVO fordert zudem in Art. 25 die Durchsetzung von Datenschutzanforderungen bereits im Prozess der Technikgestaltung und durch datenschutzfreundliche Voreinstellungen der verwendeten IT-Systeme („Data protection by design and by default“).

In der Planungsphase ist daher die Verarbeitungstätigkeit und die mit ihr verbundenen Verarbeitungsvorgänge mit hinreichender Tiefe so zu spezifizieren, dass die Verarbeitungstätigkeit mit ihren wesentlichen Daten, Systemen und Diensten sowie Prozessen der Verarbeitung präzise und vollständig festgelegt sowie nachvollziehbar und prüfbar dokumentiert ist. Dazu müssen Verantwortliche alle relevanten Aspekte sichten und zusammenstellen, die normativ gefordert und folglich funktional notwendig sind. Diese müssen dann in einer oder in mehreren Spezifikationen aufgegriffen, verdichtet und festgelegt werden.

Die Spezifikationen der technischen Komponenten einer Verarbeitungstätigkeit SOLLTEN die Form eines Lasten- und Pflichtenhefts annehmen (M41.501). Der Auftraggeber (im Datenschutz immer der Verantwortliche) beschreibt im Lastenheft möglichst präzise die

Seite 1

Dokumentieren



Baustein 42 „Dokumentieren“

Version: V1.0a
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Versionshistorie	gültig seit	gültig bis
SDM-V2.0_Dokumentieren_V1.0	30. Juni 2020	1. September 2020
SDM-V2.0_Dokumentieren_V1.0a	2. September 2020	

1. Bezug zu den Anforderungen der DS-GVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO-Anforderungen (vgl. SDM-V2b-Methodik-Handbuch, Teil B):

Anforderungen der DS-GVO	Gewährleistungsziele
Transparenz für Betroffene (Art. 5 Abs. 1 lit. a DS-GVO)	Transparenz
Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2 DS-GVO)	Transparenz
Evaluierbarkeit (Art. 32 Abs. 1 lit. d DS-GVO)	Transparenz

2. Beschreibung

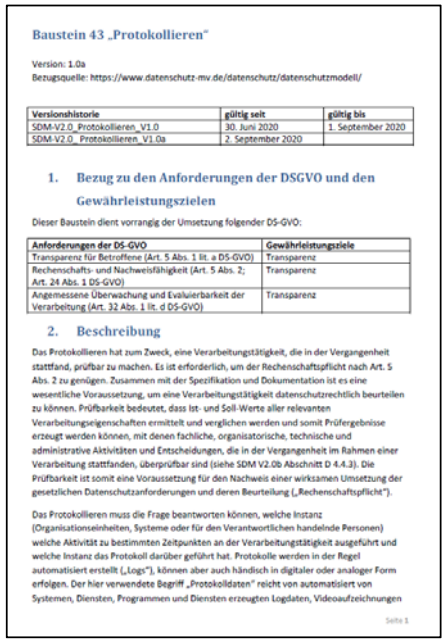
Das Dokumentieren ist neben dem Spezifizieren und dem Protokollieren der Verarbeitung Teil des Datenschutzmanagements und trägt maßgeblich dazu bei, den ordnungsgemäßen Betrieb einer Verarbeitungstätigkeit und die Einhaltung spezifischer datenschutzrechtlicher Vorschriften kontrollieren und prüfen zu können. Dabei umfasst das Dokumentieren die Beschreibung der Verarbeitung, insbesondere unter Ausweis des Zwecks der Verarbeitungstätigkeit und der Zweckbindung der verarbeiteten Daten. Es dient dazu, die rechtmäßige Verarbeitung dauerhaft sicherstellen und nachweisen zu können, sowohl für die Organisation selbst als auch anderen Organisationen und Aufsichtsbehörden gegenüber. Das Dokumentieren unterstützt den Verantwortlichen bei der Erfüllung der Informationspflichten und der Gewährleistung der Auskunftsrechte gegenüber den betroffenen Personen.

Eine Dokumentation dient der Sicherung der Transparenz insbesondere

- von Datenbeständen,
- von Transformationen zwischen Daten,
- der benutzten Systemkomponenten, deren Funktionen und Schnittstellen,
- der Prozesse innerhalb von IT-Systemen und Organisationen und über IT-Systemgrenzen und Organisationsgrenzen hinweg und
- der Nachvollziehbarkeit von Entscheidungen und Verarbeitungshandeln.

Seite 1

Protokollieren



Baustein 43 „Protokollieren“

Version: 1.0a
Bezugsquelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Versionshistorie	gültig seit	gültig bis
SDM-V2.0_Protokollieren_V1.0	30. Juni 2020	1. September 2020
SDM-V2.0_Protokollieren_V1.0a	2. September 2020	

1. Bezug zu den Anforderungen der DSGVO und den Gewährleistungszielen

Dieser Baustein dient vorrangig der Umsetzung folgender DS-GVO:

Anforderungen der DS-GVO	Gewährleistungsziele
Transparenz für Betroffene (Art. 5 Abs. 1 lit. a DS-GVO)	Transparenz
Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2; Art. 24 Abs. 1 DS-GVO)	Transparenz
Angemessene Überwachung und Evaluierbarkeit der Verarbeitung (Art. 32 Abs. 1 lit. d DS-GVO)	Transparenz

2. Beschreibung

Das Protokollieren hat zum Zweck, eine Verarbeitungstätigkeit, die in der Vergangenheit stattfand, prüfbar zu machen. Es ist erforderlich, um der Rechenschaftspflicht nach Art. 5 Abs. 2 zu genügen. Zusammen mit der Spezifikation und Dokumentation ist es eine wesentliche Voraussetzung, um eine Verarbeitungstätigkeit datenschutzrechtlich beurteilen zu können. Prüfbarkeit bedeutet, dass Ist- und Soll-Werte aller relevanten Verarbeitungseigenschaften ermittelt und verglichen werden und somit Prüfergebnisse erzeugt werden können, mit denen fachliche, organisatorische, technische und administrative Aktivitäten und Entscheidungen, die in der Vergangenheit im Rahmen einer Verarbeitung stattfanden, überprüfbar sind (siehe SDM V2.0b Abschnitt D 4.4.3). Die Prüfbarkeit ist somit eine Voraussetzung für den Nachweis einer wirksamen Umsetzung der gesetzlichen Datenschutzanforderungen und deren Beurteilung („Rechenschaftspflicht“).

Das Protokollieren muss die Frage beantworten können, welche Instanz (Organisationseinheiten, Systeme oder für den Verantwortlichen handelnde Personen) welche Aktivität zu bestimmten Zeitpunkten an der Verarbeitungstätigkeit ausgeführt und welche Instanz das Protokoll darüber geführt hat. Protokolle werden in der Regel automatisiert erstellt („Logs“), können aber auch händisch in digitaler oder analoger Form erfolgen. Der hier verwendete Begriff „Protokolldaten“ reicht von automatisiert von Systemen, Diensten, Programmen und Diensten erzeugten Logdaten, Videoaufzeichnungen

Seite 1

Planung → Implementierung → Betrieb

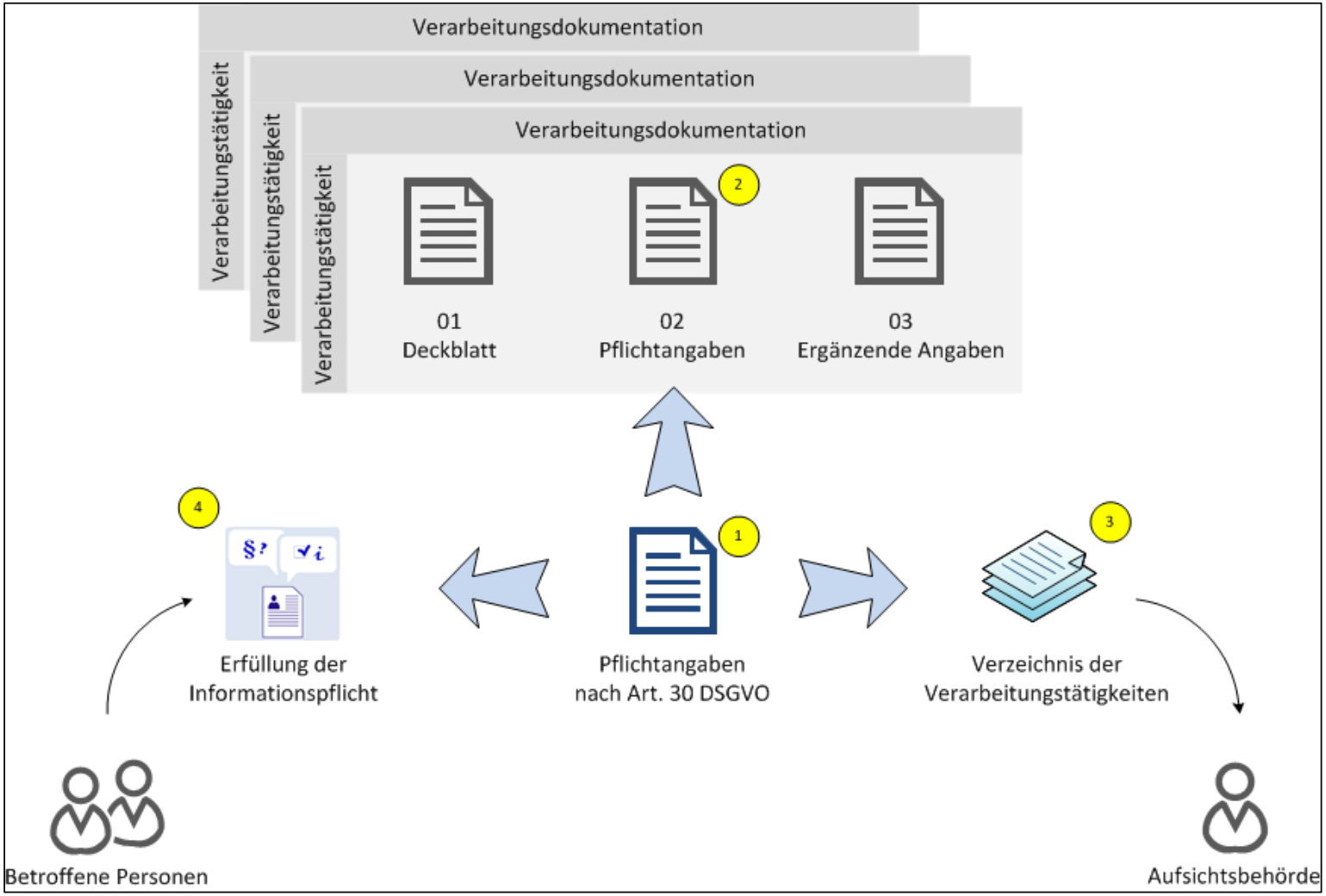
Dokumentation – für wen?

Non scholae sed vitae discimus.

Bild: Tumisu via Pixabay

- Nicht für die Aufsichtsbehörde, sondern …
- Ja, für wen dokumentiert der Verantwortliche?
- Für sich? Für betroffene Personen? Für ein Gericht?
- Davon hängt auch ab, wie dokumentiert wird.

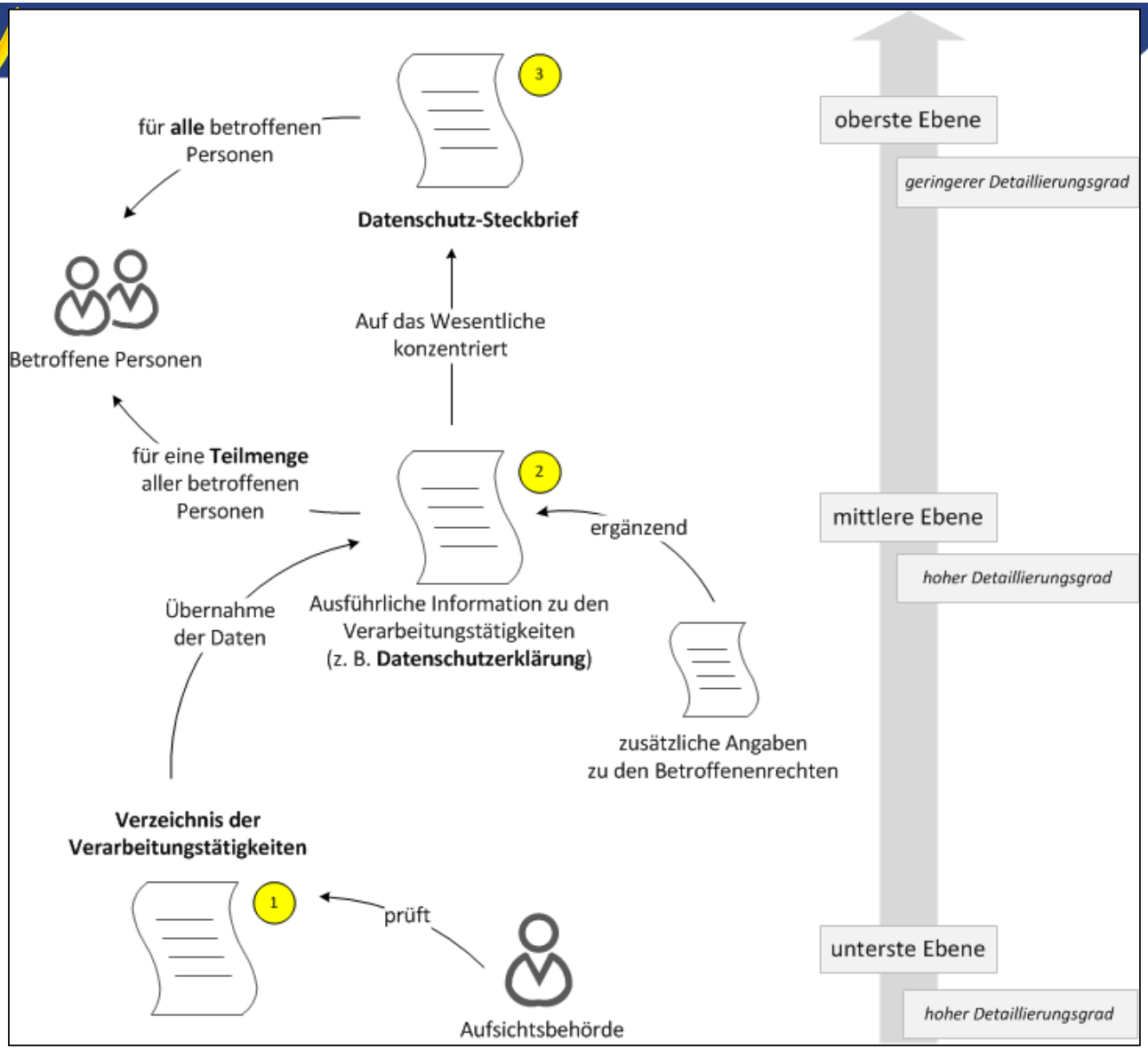
Verschiedene Zielgruppen



Am besten (auch wenn laut EuGH nicht Teil der Rechenschaftspflicht):

Startpunkt:
Art. 30 DSGVO

Verschiedene Zielgruppen



Ziel: adäquate Nachvollziehbarkeit für andere Personen

- Betroffene Personen
- Prüfinstanzen (bDSB, Aufsichtsbehörde)
- Administrator:innen, Entwickler:innen

https://www.datenschutzzentrum.de/dokumentation

In Hoch-Risiko-Situationen ist mehr nötig

BAYERN

Quellcodeüberprüfung von Palantir für Polizei verzögert sich

Sicherheitsforscher sollen den Quellcode von Palantirs Analysesoftware für die Polizei überprüfen. Das verzögert sich.

in Pocket speichern | merken

5. Januar 2023, 9:31 Uhr, Lennart Mühlenmeier

(Bild: Sophie Louisnard/Unsplash-Lizenz)

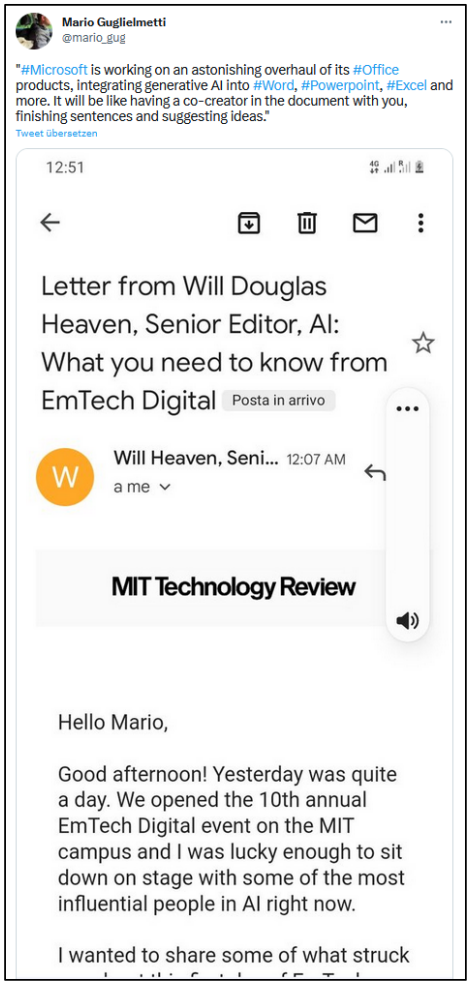
Palantirs Software soll Beziehungsgeflechte zwischen Objekten durchsuchbar machen.

https://www.golem.de/news/bayern-quellcodeueberpruefung-von-palantir-fuer-polizei-verzoegert-sich-2301-170965.html

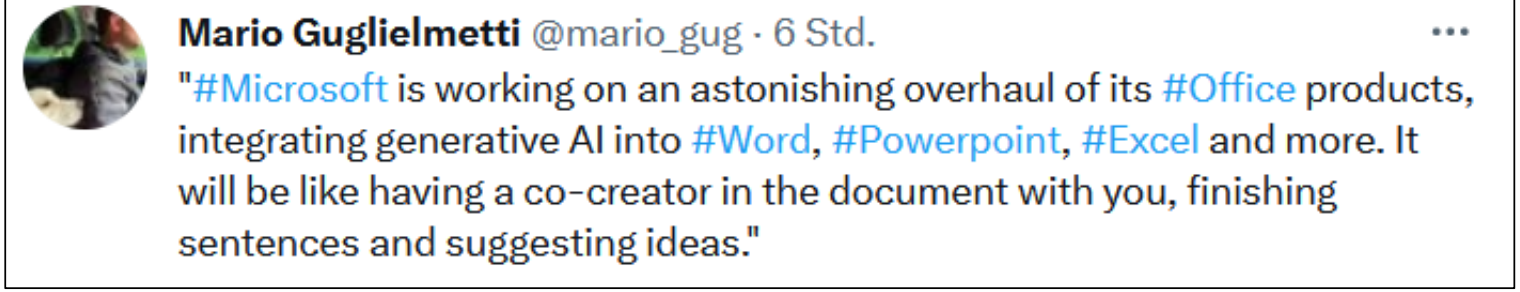
6.49. The court finds that it is unable to assess the correctness of the position of the State of the precise nature of SyRI because the State has not disclosed the risk model and the indicators of which the risk model is composed or may be composed. In these proceedings the State has also not provided the court with objectively verifiable information to enable the court to assess the viewpoint of the State on the nature of SyRI. The reason the State gives for this is that citizens could then adjust their conduct accordingly. This is a deliberate choice of the State. That choice also coincides with the starting point of the legislator regarding the provision of information on SyRI. The SyRI legislation does not show how the decision model of SyRI functions and which indicators are or can be used in a SyRI project (see 4.23 above for the terms decision model and indicators), i.e. which factual data make or can make the presence of a certain situation plausible.

Instantie	Rechtbank Den Haag
Datum uitspraak	05-02-2020
Datum publicatie	06-03-2020
Zaaknummer	C-09-550982-HA ZA 18-388 (English)
Rechtsgebieden	Civiel recht
Bijzondere kenmerken	Bodemzaak,Eerste aanleg - meervoudig
Inhoudsindicatie	see: ECLI:NL:RBDHA:2020:865 (https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2020:865) (Dutch version) SyRI legislation in breach of European Convention on Human Rights The Hague District Court has delivered a judgment today in a case about the Systeem Risico Indicatie, or SyRI. SyRI is a legal instrument used by the Dutch government to detect various forms of fraud, including social benefits, allowances, and taxes fraud. The court has ruled that the legislation regulating the use of SyRI violates higher law. The court has decided that this legislation does not comply with Article 8 of the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life, home and correspondence.

https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:1878



Nochmal zurück zum Start: Microsoft-Onlinedienste



- „co-creator in the document“
  - In Behörden?
  - In Arztpraxen?
  - In Rechtsanwaltskanzleien?
- Und wie funktioniert es genau?

Tweet vom 04.05.2023 von Mario Guglielmetti mit Zitat von Will Douglas Heaven zur Integration von KI in Office-Produkte: https://twitter.com/mario_gug/status/1653895387478999040

Bild: Gerd Altmann via Pixabay

Überblick

- Warum das Thema?
- Was bedeutet die Rechenschaftspflicht?
- Gibt es einen Zusammenhang mit dem Risiko?
- Was ist zu tun?
- Hilfestellungen
- Fazit

Hilfestellungen

- Standard-Datenschutzmodell, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/
  - Baustein „Planen und Spezifizieren", https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0b_Planen_Spezifizieren_V1.0.pdf
  - Baustein „Dokumentieren", https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Dokumentieren_V1.0a.pdf
  - Baustein „Protokollieren", https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Protokollieren_V1.0a.pdf

- EDSB:
  - Rechenschaftspflicht in der Praxis: Leitfaden für Organe, Einrichtungen und Agenturen der Union über die Dokumentierung von Verarbeitungsvorgängen – Zusammenfassung, https://edps.europa.eu/system/files/2021-07/19-07-17_summary_accountability_guidelines_en_95_de.pdf
  - Rechenschaftspflicht in der Praxis Teil I: Verzeichnisse, Register und Erfordernis einer Datenschutz-Folgenabschätzung, https://edps.europa.eu/system/files/2021-07/19-07-17_accountability_on_the_ground_part_i_en_48_de.pdf

Bearbeitungsschritte zur vollständigen Dokumentation

Bearbeitungsschritt		ggf. Bemerkung
Datenschutzbeauftragte/r beteiligt	☐	
Personal-/Betriebsrat beteiligt	☐	
Zweck der Verarbeitung beschrieben	☐	
Rechtmäßigkeit geprüft/beschrieben	☐	
Betroffenenkategorien definiert	☐	
Datenkategorien definiert	☐	
Datenübermittlungen beschrieben	☐	
Löschfristen beschrieben/definiert	☐	
Zuständigkeiten definiert	☐	
Benutzerberechtigungen definiert	☐	
Administrationsberechtigungen definiert	☐	

Bearbeitungsschritte zur vollständigen Dokumentation

Bearbeitungsschritt		ggf. Bemerkung
Verfahren zur Protokollierung festgelegt	☐	
Prüfungs-/Kontrollprozesse festgelegt	☐	
Auftragsverarbeitung (falls vorhanden) geprüft und dokumentiert	☐	
Prozess (Informationspflicht für betroffene Personen, Artt. 13 und 14 DSGVO) definiert	☐	
Prozess (Betroffenenrechte, Artt. 16 bis 18 DSGVO) definiert	☐	
Datenschutz „by Design" und „by Default" (Art. 25 DSGVO) geprüft und dokumentiert	☐	
Sicherheit der Verarbeitung (Art. 32 DSGVO) bewertet, technische und organisatorische Maßnahmen definiert und dokumentiert	☐	

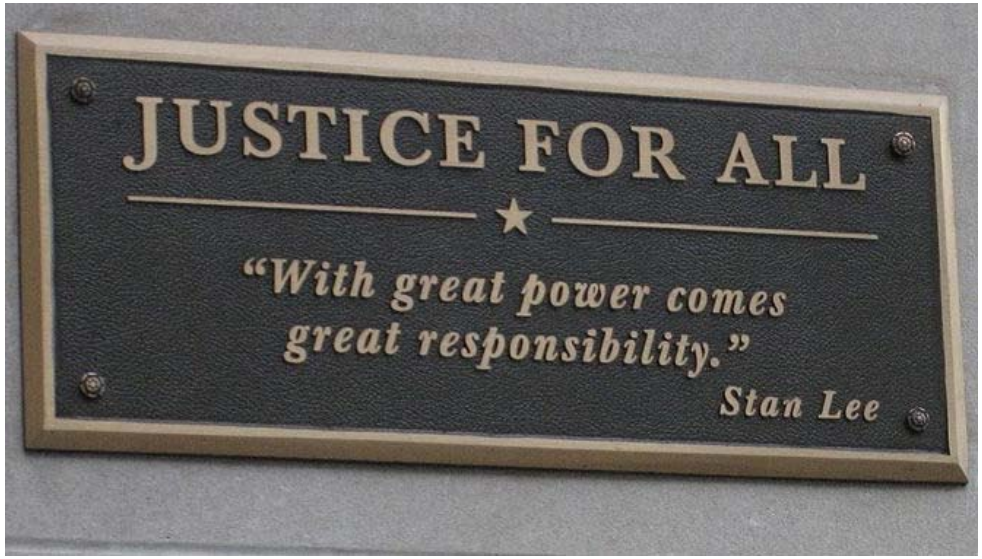
Bearbeitungsschritte zur vollständigen Dokumentation

Bearbeitungsschritt		ggf. Bemerkung
Notwendigkeit einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) geprüft und dokumentiert	☐	
Verarbeitungstätigkeit getestet	☐	
Verarbeitungstätigkeit freigegeben	☐	
Verarbeitungstätigkeit ins Verzeichnis der Verarbeitungstätigkeiten aufgenommen	☐	
Verarbeitungstätigkeit in die IT-Dokumentation aufgenommen	☐	
Verarbeitungstätigkeit in die Sicherheitsdokumentation aufgenommen	☐	

Überblick

- Warum das Thema?
- Was bedeutet die Rechenschaftspflicht?
- Gibt es einen Zusammenhang mit dem Risiko?
- Was ist zu tun?
- Hilfestellungen
- Fazit

Fazit



- Generell:
  - Zerlegung in Module
  - Schrittweises Vorgehen
  - Nötige Informationen einfordern – alle haben dasselbe Problem
  - Bewusstsein über das Risiko
- Als ständige Aufgabe im Datenschutzmanagementsystem
- Rechenschaftspflicht und KI?