Dokumentation im Datenschutz-
Anforderungen der Datenschutz-Grundverordnung

Agenda

Was möchte ich vorstellen?

- Pflicht zur Dokumentation
- Spezielle Vorgaben zur Dokumentation
- Umsetzungsvorschlag

Dokumentationspflicht

Dokumentationspflicht inkl. Auditierung

DS-GVO verpflichtet zur Dokumentation sowie zur Prüfung der DS-GVO-Einhaltung

- Art. 5 Abs. 2 DS-GVO
  Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen **Einhaltung nachweisen**
- Art. 24 DS-GVO
  Verantwortliche setzt technische und organisatorische Maßnahmen zum Schutz der von der Verarbeitung betroffenen Person um; diese **Maßnahmen werden erforderlichenfalls überprüft und aktualisiert**.

Spezielle Vorgaben zur Dokumentation

Rechenschaftspflicht nach Art. 5 DS-GVO

Verantwortliche muss nachweisen

- Rechtmäßigkeit
- Transparenz (inkl. Drittland-Verarbeitung)
- Verantwortlicher
- Zweck(e) / Zweckbindung
- Datenminimierung
- Richtigkeit
- Betroffene (Kategorien)
- Daten (Kategorien)
- Empfänger (Kategorien)
- Löschfristen / Speicherbegrenzung
- Integrität, Vertraulichkeit

Nachweis bzgl. Einwilligung gem. Art. 7 DS-GVO

Verantwortliche muss nachweisen

- Art. 7 DS-GVO
  [...] muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat
- Beinhaltet
  - Freiwilligkeit
    (Ohne Zwang, „echte“ Alternativmöglichkeiten sind vorhanden)
  - Für den bestimmten Fall (= Zweckbindung)
  - Informiertheit
    (Insbesondere in Kenntnis der Sachlage, z.B. auch Berücksichtigung Artt. 12, 13,14 DS-GVO)
  - unmissverständlich abgegebene Willensbekundung
    (in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung)
  - Ausdrückliche Willenserklärung
    (Eindeutig: „Ich will“)

Informationspflichten (Artt. 13, 14 DS-GVO)

Verantwortliche muss nachweisen

- Art. 13 Abs. 1 DS-GVO
  Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit
- Art. 14 DS-GVO
  Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit

→ Verstoß gegen Informationspflicht bußgeldbewehrt

→ Wie weist der Verantwortliche nach, dass den Pflichten nachgekommen wurde?

→ Prozess dokumentieren, Prozess regelmäßig prüfen, Prüfung und Ergebnis Prüfung dokumentieren

Privacy by Design/Default (Art. 25 DS-GVO)

Privacy by Design/Default betrifft vollständigen Daten-Lebenszyklus

- Art. 25 Abs. 1 Ds-GVO
  [...] trifft der Verantwortliche **sowohl zum Zeitpunkt der Festlegung der Mittel** für die Verarbeitung als auch **zum Zeitpunkt der eigentlichen Verarbeitung** geeignete technische und organisatorische Maßnahmen [...]
- Zielsetzung (Art. 25 abs. 1 DS-GVO)
  [...] die **Datenschutzgrundsätze** [...] **wirksam umzusetzen** und die **notwendigen Garantien** in die Verarbeitung aufzunehmen, um den **Anforderungen dieser Verordnung zu genügen** und die **Rechte der betroffenen Personen zu schützen**

→ Anforderung zur Dokumentation ergibt sich indirekt aus Art. 25 Abs. 3 DS-GVO

Auftragsverarbeitung (Art. 28 DS-GVO)

Vertrag zur Auftragsverarbeitung muss existieren

- Verantwortlicher muss nachweisen
  - Kriterien für die Auswahl des Auftragsverarbeiters
  - Einhaltung Vorgaben Art. 32 DS-GVO (Sicherheit Verarbeitung)
  - Gewährleistung der Rechte der betroffenen Person
  - Durchführung und das Ergebnis einer Vor-Ort-Prüfung (wenn durchgeführt)
  - Einhaltung Vertragspflichten
  - → Nachweis muss für gesamte Dauer der Verarbeitung geführt werden
- Pflicht zum Vertragsabschluss (schriftlich)
  - Inhaltliche Vorgaben aus Art. 28 Abs. 3 S. 2 lit. a-h DS-GVO (siehe auch Muster-Vertrag zur Auftragsverarbeitung für das Gesundheitswesen*)
  - Weitere Vorgaben bzgl. Verarbeitung im Auftrag nicht zwingend Vertragsbestandteil, muss aber ggf. nachgewiesen werden, z.B.
    - → Nicht in der Union niedergelassene Verantwortlichen oder Auftragsverarbeitern benötigen Vertreter in der Union
    - → Artt. 44ff DS-GVO: Verarbeitung in Drittstaaten

* Mustervertrag zur Auftragsverarbeitung, online unter http://ds-gvo.gesundheitsdatenschutz.org/html/adv-vertrag.php

Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)

Dokumentiert werden muss

- Name/Kontaktdaten Verantwortlicher, wenn vorhanden auch Datenschutzbeauftragter
- Zweck(e)
- Betroffene (Kategorien)
- Daten (Kategorien)
- Empfänger (Kategorien)
- Löschfristen
- Drittland-Verarbeitung
- TOM

Sicherheit der Verarbeitung (Art. 32 DS-GV)

Sicherheit der Verarbeitung muss nachgewiesen werden

- Verantwortliche und der Auftragsverarbeiter setzen geeignete technische und organisatorische Maßnahmen ein, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:
  - Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste auf Dauer sicherzustellen;
  - die Verfügbarkeit und Zugang der Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs
- Nachweis der Maßnahmen erforderlich
  (indirekte Pflicht resultierend aus Art. 32 Abs. 3 DS-GVO)

Datenschutz-Folgenabschätzung gem. Art. 35 DS-GVO

Dokumentation muss mindestens einhalten

- Rechtmäßigkeit
- Systematische Beschreibung der geplanten Verarbeitungsvorgänge; dies beinhaltet u.a.
  - Betroffene (Kategorien)
  - Daten (Kategorien)
  - Empfänger (Kategorien)
  - Löschfristen
  - Drittland-Verarbeitung
- Zwecke der Verarbeitung
- Ggf. die vom Verantwortlichen verfolgten berechtigten Interessen
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- Zur Bewältigung der Risiken geplanten Abhilfemaßnahmen („TOM“)
- Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird

Verletzungen des Schutzes personenbezogener Daten („Datenpannen")

Die Dokumentation der Datenpannen muss beinhalten...

- Verantwortlicher
- Name/Kontaktdaten Datenschutzbeauftragter oder sonstige Anlaufstelle
- Zweck(e)
- Betroffene (Kategorien), ungefähre Anzahl betroffener Personen
- Daten (Kategorien)
- Beschreibung der Art der Verletzung des Schutzes
- Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (Risikobetrachtung)
- Meldepflicht
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen (TOM)

Dokumentation der TOMs

Hierbei muss eingegangen werden auf

- Inhalte gemäß Art. 32 DS-GVO
- Zweck(e)
- Daten (Kategorien)
- Empfänger (Kategorien)
- Löschfristen
- Drittland-Verarbeitung
- Risikobetrachtung
- TOM: Idealerweise Gruppierung
  - Pseudonymisierung und Verschlüsselung
  - Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfügbarkeit
  - Überprüfung, Bewertung und Evaluierung der Wirksamkeit
- Ggf. Zuordnung TOM-Risiko/Risiken

Dokumentation bei Drittlandverarbeitung

Dokumentation nicht direkt erforderlich, aber ...

- Art. 44 DS-GVO
  [...] ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; [...]

→ Insbesondere gilt auch die Nachweispflicht aus Art. 5 DS-GVO (Accountability)

- Art. 44 DS-GVO
  Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

→ Es ist ein Nachweis erforderlich, wie das Schutzniveau erhalten bleibt

Auch der Datenschutzbeauftragte "darf " dokumentieren

Dokumentation nicht direkt erforderlich, aber ...

- Art. 39 Abs. 1 DS-GVO
  Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:
  - b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen
- Wie weist der Datenschutzbeauftragte die Erfüllung seiner Aufgaben nach?
  Dokumentation

Anforderungen zur Dokumentation in der DS-GVO

Aber was ist zu dokumentieren?

An vielen Stellen müssen dieselben Angaben gemacht werden, z.B.

	Rechenschaftspflicht	Einwilligung	Tätigkeitsverzeichnis	Datenschutz-Folgenabschätzung	Dokumentation TOMs	Datenpannen
Rechtmäßigkeit	X			X		
Verantwortlicher	X	X	X			X
Zweck(e)	X	X	X	X	X	X
Betroffene (Kategorien)	X		X	X		X
Daten (Kategorien)	X	X	X	X	X	X
Empfänger (Kategorien)	X	X	X	X	X	
Löschfristen	X	X	X	X	X	
Drittland-Verarbeitung	X	X	X	X	X	
Risikobetrachtung				X		X
TOM		X	X	X	X	X

Umsetzungsvorschlag

Umsetzung, z.B. durch

Datenschutz-Management als PDCA-Zyklus

- Plan
  Planung der Verarbeitung inkl. Risikomanagement
- Do
  Umsetzung geeigneter technisch-organisatorischer Maßnahmen
- Check
  Überwachung/Monitoring der Maßnahmen hinsichtlich der Wirksamkeit bzgl. der Risiken (inkl. Ggf. neu aufgetretener Risiken)
- Act
  Anpassung/Aktualisierung Maßnahmen

Umsetzung, z.B. durch

Datenschutz-Management, d.h.

- Prozessbeschreibung inkl. Verfahrens-/Arbeitsanweisungen
- Regelmäßige Prüfung der Prozesse sowie Dokumentation der Prüfungsergebnisse
- Dokumente Reaktion auf bei Prüfungen festgestellte Abweichungen

Beispiel: Umgang mit Anfragen betroffener Personen

Erforderlich: Etablierung strukturierter Prozesse

1. Annahme einer Anfrage

- Darstellung, *wo* Anfragen im Unternehmen eingehen können
  - Identifizierung der „Entry-Points“ wie Telefonzentrale, Kontaktformular Internet, E-Mail-Kommunikationsadressen des Unternehmens, z. B. Impressum, ...
- Schulung der die Anfragen entgegennehmenden Personen
  - Welche Informationen müssen erfragt werden?
  - An wen wird die Anfrage weitergeleitet?

Beispiel: Umgang mit Anfragen betroffener Personen

Erforderlich: Etablierung strukturierter Prozesse

2. Umgang mit einer Anfrage

2.1 Eingangsprüfung

- Überprüfung, ob es sich tatsächlich um eine datenschutzrechtliche Anfrage handelt
- Erfassung der Anfrage in einem geeigneten Dokumentationssystem
- Überprüfung, worum es sich handelt (Auskunftsersuchen, Korrekturanfrage, Löschungsersuchen, ...)
- Versendung einer Eingangsbestätigung an den Antragssteller
- Prüfung der Identität des Antragsstellers
- Prüfung, ob
  - unbegründete Antrag i.S.v. Art. 12 Abs. 5 DS-GVO
  - exzessiven Anträgen einer betroffenen Person vorliegen
- Kann Antrag nicht sofort bearbeitet werden: Information betroffene Person ohne Verzögerung

Beispiel: Umgang mit Anfragen betroffener Personen

Erforderlich: Etablierung strukturierter Prozesse

2. Umgang mit einer Anfrage

2.2 Inhaltliche Prüfung

- Prüfung, ob personenbezogene Daten der betroffenen Person verarbeitet werden/wurden
- Wenn keine Daten vorhanden sind:
  Negativmitteilung an den Betroffenen versenden !
- Wenn Daten vorhanden sind: Abarbeiten

Beispiel: Umgang mit Anfragen betroffener Personen

Erforderlich: Etablierung strukturierter Prozesse

2. Umgang mit einer Anfrage

2.3 Beantwortung

- Auskunftsersuchen:
  - Zusammenstellung
  - Unverzügliche Beantwortung
    a) Innerhalb eines Monats
    b) Wenn auf Grund Komplexität nicht innerhalb von einem Monat möglich
       - Innerhalb von 3 Monaten nach Antragstellung zwingend umzusetzen
       - Person muss innerhalb der ersten Monats über Verzögerung informiert werden
  - Beachten: Elektronische Antragstellung = Unterrichtung auch elektronisch, wenn betroffene Person nichts anderes verlangt
- Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit
  - Weiterleitung an entsprechende Stellen zwecks Umsetzung
  - Sobald Umsetzung erfolgt → Information betroffene Person (siehe Auskunftsersuchen)

Beispiel: Umgang mit Anfragen betroffener Personen

Erforderlich: Etablierung strukturierter Prozesse

2. Umgang mit einer Anfrage

2.3 Beantwortung

- Widerspruch Verarbeitung, Widerruf einer Einwilligung
  - Information der Stelle, welche
    a) die Verarbeitung (z.B. Forschung) durchführt
    b) die Einwilligung erhob
  - Verarbeitung einstellen
  - Prüfen, ob Daten gelöscht werden müssen (Art. 17 Abs. 1 lit. b,c DS-GVO)
  - Information betroffene Person über erfolgte Maßnahmen, ggf. auch über Löschung (siehe Auskunftsersuchen)

Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.

Datenschutzmanagement

- Broschüre „EU-Datenschutz-Grundverordnung (DSGVO) – Die neuen europäischen Datenschutzvorschriften: wichtige Änderungen und ihre Auswirkungen auf Wirtschaft und Verwaltung
- „Daher empfiehlt es sich ‚im Rahmen einer Unternehmensrichtlinie oder eines Handbuchs, für den Kundenkontakt oder die Personaldatenverarbeitung, **Prozesse und Ansprechpartner zu definieren**.
- Erforderlich ist auch eine **Dokumentation der IT und der Prozesse**.“
- (Siehe S. 14, letzter Absatz im Kap. Datenschutzmanagement)

Download unter https://www.awv-net.de/fachergebnisse/schriftenverzeichnis/rechtsaspekte-der-it/dsgvo-bdsg-neu-printausgabe.html
bzw. Direkt pdf-Datei unter https://www.awv-net.de/upload/online-dokumente/04651_Broschre_zur_DSGVO.pdf

Datenschutz-Management-System

Anforderungen zur Dokumentation in der DS-GVO

Elektronisches Dokumentationssystem wird benötigt

- Benötigt wird elektr. Doku-System
  - Information an einer Stelle dokumentiert
  - Steht überall, wo benötigt zur Verfügung
- Problem
  - Derzeit kein Doku-System auf dem Markt, welches alle Anforderungen abdeckt
- Andere Herausforderungen
  - Finanzierung eines Datenschutz-Doku-Systems durch Krankenhäuser
  - Diverse notwendige Finanzierungen konkurrieren im Krankenhaus miteinander, da zu wenig Geld vorhanden
  - Wie ein DS-Doku-System finanzieren?

Anforderungen zur Dokumentation in der DS-GVO

Idee

- Open-Source Entwicklung eines speziell auf das Gesundheitswesen zugeschnittenen IT-Systems zur Datenschutz-Dokumentation
  - Initialentwicklung:
    Student(en) der FH Dortmund im Rahmen Bachelor-/Master-Arbeit
  - Pflege:
    KG-NRW

Anforderungen zur Dokumentation in der DS-GVO

Idee

- Open-Source Entwicklung eines speziell auf das Gesundheitswesen zugeschnittenen IT-Systems zur Datenschutz-Dokumentation
- Datenschutzexperten erheben Anforderungen, z.B.
  - Grundlegende Anforderungen wie
    - Mandantenfähigkeit (Krankenhaus, MVZ, Tochtergesellschaften)
    - Rechtemanagement (Dokumentieren müssen DSB, aber auch Mediziner, Itler, …)
  - Anforderungen bzgl. Dokumentation
    - Was ist zu dokumentieren? (Stammdaten, …)
  - Fragenkataloge, die durch Dokumentation führen
  - Arbeitslisten
  - Gesundheitsspezifische Nachschlagespalten, z.B. Rechtsgrundlagen, Zwecke, Datenarten/-kategorien, Erhebungsquellen, Empfänger

Anforderungen zur Dokumentation in der DS-GVO