Dokumentationspflichten unter der DS-GVO

Dr. Bernd Schütze

Fachtagung Datenschutz im Gesundheitswesen: Workshop Dokumentationspflichten

VITA

HEALTHCARE SOLUTIONS

Deutsche Telekom Healthcare and Security Solutions GmbH
Dr. Bernd Schütze
Senior Experte Medical Data Security

☎ +49 (160) 9566 - 3145
Bernd.Schuetze@T-Systems.com

Studium

- Informatik (FH-Dortmund)
- Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
- Jura (Fern-Uni Hagen)

Ergänzende Ausbildung

- Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
- Datenschutz-Auditor (TüV Süd)
- Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)

Berufserfahrung

- Über 10 Jahre klinische Erfahrung
- Mehr als 20 Jahre IT im Krankenhäusern
- > 20 Jahre Datenschutz im Gesundheitswesen

Mitarbeit in wiss. Fachgesellschaften

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
- Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
- Gesellschaft für Informatik (GI)

Mitarbeit in Verbänden

- Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
- Berufsverband Medizinischer Informatiker e.V. (BVMI)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.
- HE Deutschland e.V.

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

- Verantwortliche muss Nachweis erbringen können, dass Verarbeitung gemäß Vorgaben DS-GVO erfolgt
- Maßnahmen, die Einhaltung der Grundsätze von Art. 5 sicherstellen, muss ggf. überprüft und aktualisiert werden

→ Vorschrift fordert umfassende Dokumentation sämtlicher Maßnahmen zur Sicherstellung des Datenschutzes*

* Roßnagel Art. 5 Rn. 181. in Simitis / Hornung / Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

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

Rechtmäßigkeit der Verarbeitung

Artt. 6,9 DS-GVO

- Verarbeitung zur Vertragserfüllung (Stichwort Behandlungsvertrag)
- Nicht jede Verarbeitung ist erlaubt, sondern nur die **zur Vertragserfüllung erforderlichen**
- Erforderlich: sowohl Hauptleistung als auch Nebenleistungen, die mit Hauptleistung zusammenhängen* (z.B. gesetzliche Aufbewahrungsfristen)
- Frage: Wie weisen sie nach, welche Daten/Verarbeitungen zur Erfüllung des Behandlungsvertrages erforderlich sind?

* Roßnagel Art. 5 Rn. 181. in Simitis / Hornung / Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

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

Korrekturen der Dokumentation (Art. 16 DS-GVO)

Kann/darf man alles „korrigieren“?

- Korrekturanspruch gilt grundsätzlich auch auf Daten in Patientenakten (siehe auch ErwGr.63 DS-GVO)
- Berichtigungen können nur verlangt werden, wenn die Unrichtigkeit zweifelsfrei festgestellt werden kann

→ Verdachtsdiagnosen eines Arztes sind somit davon nicht betroffen, da kaum nachweisbar sein dürfte, dass der Arzt einen anderen Verdacht hatte

→ Medizinische Bewertungen oder Aufzeichnungen durch Fachpersonal (Pflegekräfte, Ärzte usw.) sind subjektive Dokumentationen, die nicht berichtigt werden können

- (Aber ggf. die in der Dokumentation beschriebenen „Tatsachen“, welche zu den Bewertungen/Aufzeichnungen führten)

→ Diagnosen, die zum Zeitpunkt der Erstellung dem medizinischen Kenntnisstand entsprachen, dürfen nicht nachträglich korrigiert werden, wenn sich im Laufe der Zeit der medizinische Erkenntnisstand ändert

Korrekturen der Dokumentation (Art. 16 DS-GVO)

Kann/darf man alles „korrigieren“?

Aber Korrekturwünsche des Patienten, Entscheidungen bzgl. der Korrektur und die Begründung der Entscheidung müssen dokumentiert werden

–

–

→

→ te,

→

entsprachen, dürfen nicht nachträglich korrigiert werden, wenn sich im Laufe der Zeit der medizinische Erkenntnisstand ändert

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

Etablierung eines Prozesses

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 Krankenhausgesellschaft NRW

- 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

Umsetzungsvorschlag

Stand heute: Kein umfassendes Doku-System

Elektronische Dokumentation: Mehr als ein System erforderlich

- Mehrfacherfassung
- Beispiel: Welcher Zweck gilt bei abweichender Beschreibung in verschiedenen Systemen?

Bestimmen, was Bestimmbar ist

Vorab definieren, was gebrauct wird: Sammlung von Items

- Allgemeine Dokumentation
  - Verantwortlicher / Name/Kontaktdaten Verantwortlicher, wenn vorhanden auch Datenschutzbeauftragter
  - Zweck(e) / Zweckbindung
  - Betroffene (Kategorien)
  - Daten (Kategorien)
  - Datenminimierung / Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
  - Art. 5 (Rechtmäßigkeit, Transparenz, Richtigkeit, Löschfristen / Speicherbegrenzung
  - Systematische Beschreibung der geplanten Verarbeitungsvorgänge
  - Gewährleistung Rechte Betroffener
  - Ggf. die vom Verantwortlichen verfolgten berechtigten Interessen
  - Empfänger
  - Drittland-Verarbeitung
  - Auftragsverarbeitung (Kriterien für Auswahl, Vertrag, …)

Bestimmen, was Bestimmbar ist

Vorab definieren, was gebraucht wird: Sammlung von Items

- Sicherheit der Verarbeitung
  - Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
  - Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird
  - Privacy by Design/Default
  - Inhalte gemäß Art. 32 DS-GVO
  - TOMs
  - Verletzung des Schutzes personenbezogener Daten
- Im Nachfolgenden werden in Gruppen einige Punkte beispielhaft bearbeitet und hinterher besprochen
  - Wenn die Ergebnisse der Gruppenarbeit zur Verfügung gestellt wird, werden diese (anonym) zusammen mit der Präsentation auf der Veranstaltungshomepage bereitgestellt

Aufgabe: Welche Daten von wem werden zu welchen Zwecken verarbeitet?

Zwecke: bitte beachten

Der Zweck der Erhebung muss klar und eindeutig festgelegt werden: Sie muss detailliert genug sein, um festzustellen, welche Art von Verarbeitung vorliegt und welche nicht, und um zu ermöglichen, dass die Einhaltung des Gesetzes bewertet und Datenschutzgarantien angewendet werden können. Aus diesen Gründen wird ein vager oder allgemeiner Zweck, wie z.B. "Verbesserung der Benutzerfreundlichkeit", "Marketingzwecke", "IT-Sicherheitszwecke" oder "Zukunftsforschung", in der Regel - ohne weitere Einzelheiten - nicht den Kriterien der "Spezifität" entsprechen.*

* EDSA: Leitlinien 2/2019 (Draft) , Ziff. 16 (S.6). 2019-04-09
Art-29-Gruppe: WP 203, S. 15/16. 2013-04-02

Betroffenenkategorien

- Nicht nur an Patienten denken
- Datenschutz gilt für alle im Krankenhaus
  - Beschäftigte
  - Lieferanten
  - Geschäftspartner
  - ...

Aufgabe (15 Min.): Welche Daten von wem werden zu welchen Zwecken verarbeitet?

Zwecke	Betroffenenkategorien
– 1	– 1

Aufgabe: Welche Datenarten werden verarbeitet, welche Empfänger sind vorhanden?

Datenarten

- Hinreichend genau, damit betroffene Person weiß, um was es geht
- Aber nicht zu detailliert, damit die Transparenz (Art. 12) in der Menge an Informationen nicht verlorengeht

Empfänger

- Bitte auch an Auftragsverarbeiter denken

Aufgabe (15 Min.): Welche Datenarten werden verarbeitet, welche Empfänger sind vorhanden?

Datenarten	Empfänger
– 1	– 1

Aufgabe: Existiert eine Drittlandverarbeitung? Nach welchen Kriterien werden Auftragsverarbeiter ausgewählt?

Auftragsverarbeitung

- **Hinreichende Garantien**, dass „geeignete TOMs so durchgeführt werden, dass Verarbeitung **im Einklang mit den Anforderungen der DS-GVO erfolgt und Schutz betroffener Personen gewährleistet ist**“

Drittlandverarbeitung

- An Wartung von IT-Systemen denken: setzt Auftragsverarbeiter ggf. Unterauftragnehmer in Drittländern ein?
- Welche Rechtsgrundlage?
- Bei Standardvertragsklauseln: Wie wird Patient informiert?

Aufgabe (15 Min.): Existiert eine Drittlandverarbeitung? Nach welchen Kriterien werden Auftragsverarbeiter ausgewählt?

Auftragsverarbeitung	Drittlandverarbeitung
– 1	– 1

Normen als Umsetzungshilfe: Datenschutzkonzept

ISO/IEC 29100 „Privacy framework“: die Rahmenbedingungen

- definiert die einschlägige Terminologie
  - anonymity, anonymization, anonymized data, consent, ...
- spezifiziert die Akteure und ihre Interaktionen bei der Verarbeitung personenbeziehbarer Daten
  - Akteure: principals, controllers, processors, Third parties
  - Interaktionen: Datenfluss zwischen einzelnen Akteuren
- beschreibt beim Schutz der Privatsphäre zu berücksichtigende Aspekte und entsprechende technische Ansätze
  - Identifiers, Legal and regulatory factors, Business factors, ...
- liefert Verweise wesentliche Datenschutzgrundsätze für die Informationstechnologie
  - consent, Purpose legitimacy, Collection limitation, Data minimization,...

Normen als Umsetzungshilfe: Zweckbestimmung

DIN CEN ISO/TS 14265

- „Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen“
- Vorgeschlagene Zwecke
  - Klinische Versorgung einer zu behandelnden Person
  - Notfallbehandlung einer zu behandelnden Person
  - Unterstützung von Gesundheitsversorgungsmaßnahmen innerhalb der Dienstleistungsorganisation für eine einzelne behandelte Person
  - Ermöglichung der Bezahlung von für eine einzelne behandelte Person erbrachten Gesundheitsdienstleistungen
  - Management und Qualitätssicherung von Gesundheitsdienstleistungen
  - Aus- und Weiterbildung
  - Überwachung der öffentlichen Gesundheit, Krankheitsbekämpfung
  - Öffentlicher Sicherheitsnotfall
  - Forschung
  - Marktstudien
  - Juristische Verfahren
  - ...

Normen als Umsetzungshilfe: Datenschutz-Folgenabschätzung

ISO/IEC DIS 29134 „Privacy impact assessment - Guidelines“

- Wann ist PIA erforderlich?
- Einbindung der Stakeholder
- Durchführung
- Follow-Up /Reporting
- Anhang, z. B. beispielhafte Darstellung definierter Risiken bei Hardware, Software oder auch Personen

Normen als Umsetzungshilfe: Datenschutz-Folgenabschätzung

ISO/IEC DIS 29134 „Privacy impact assessment - Guidelines“

- Wann ist
- Einbindu
- Durchfüh
- Follow-U
- Anhang, Personer

Supporting assets	Action	Privacy risk	Examples of threats
Hardware	Abnormal use	Disappearances of PII	Storage of personal files; personal use, etc.
Hardware	Abnormal use	Illegitimate accesses to the PII	Use of USB flash drives or disks that are ill-suited to the sensitivity of the information; use or transportation of sensitive hardware for personal purposes, etc.
Software	Loss	Disappearances of PII	Non-renewal of the license for software used to access data, etc.
Software	Modification	Disappearances of PII	Errors during updates, configuration or maintenance; infection by malware; replacement of components, etc.
Computer channels	Espionage	Illegitimate accesses to the PII	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.
Computer channels	Loss	Disappearances of PII	Theft of copper cables, etc.
Individuals	Abnormal use	Unwanted changes in the PII	Influence (rumor, disinformation, etc.), etc.
Individuals	Loss	Illegitimate accesses to the PII	Employee poaching; assignment changes; takeover of all or part of the organization, etc.
Paper documents	Damage	Disappearances of PII	Aging of archived documents; burning of files during a fire, etc.
Paper documents	Modification	Unwanted changes in the PII	Changes to figures in a file; replacement of an original by a forgery, etc.

ler auch

Normen als Umsetzungshilfe: Sicherheit der Verarbeitung

Nutzung von Normen zur Umsetzung der Anforderungen von Art. 32 DS-GVO

- DIN EN ISO 27799 „Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002“
  - Verweis auf andere Norm
- DIN ISO/IEC 27002 „Leitfaden für Informationssicherheits-Maßnahmen“
  - Anleitung zur Umsetzung der 27001
- DIN ISO/IEC 27001“Informationssicherheits-Managementsysteme – Anforderungen“

Normen als Umsetzungshilfe: Sicherheit der Verarbeitung: Und die Praxis?

Nutzung von Normen zur Umsetzung der Anforderungen von Art. 32 DS-GVO

DIN 27799

Contents Page

© ISO 2016 – All rights reserved

 © ISO 2016 – All rights reserved

Normen als Umsetzungshilfe:
Sicherheit der Verarbeitung: Und die Praxis?

Nutzung von Normen zur Umsetzung der Anforderungen von Art. 32 DS-GVO

DIN 27799

DIN EN ISO 27799
ISO 27799

Contents

© ISO 2016 – All rights reserved

6.2.2 Teleworking

Control

ISO/IEC 27002:2013, 6.2.2, applies.

Verweis auf DIN 27002

Implementation guidance

ISO/IEC 27002:2013, 6.2.2, applies.

Health-specific implementation guidance

Spez. Hinweise Health Care

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should:

a) prepare policy on the precautions to be taken when teleworking;

b) ensure that teleworking users of health information systems abide by this policy.

Some national jurisdictions (e.g. in Germany) have already placed restrictions on teleworking by health professionals.

It is important to consider that in healthcare, teleworking can cross jurisdictional borders and can even take place on board planes and ships situated beyond any national jurisdiction. Physicians already routinely e-mail medical images, etc. across boundaries to obtain specialist opinions. International teams involved in disaster relief may, in future, rely upon health information systems in jurisdictions other than their home jurisdiction. The legal and ethical considerations of doing this need to be taken into account in the design and deployment of health information systems (especially national systems) that may be used in this manner.

Other information

ISO/IEC 27002:2013, 6.2.2, applies.

© ISO 2016 – All rights reserved

Normen als Umsetzungshilfe:
Sicherheit der

Nutzung von Normen

DIN 27799

Contents

© ISO 2016 – All rights reserved

DIN 27002

6.2.2 Telearbeit

Maßnahme

Eine Richtlinie und unterstützende Sicherheitsmaßnahmen zum Schutz von Information, auf die von Telearbeitsplätzen aus zugegriffen wird oder die dort verarbeitet oder gespeichert werden, sollten umgesetzt sein.

Anleitung zur Umsetzung

Organisationen, die Telearbeit erlauben, sollten eine Richtlinie zur Definition von Bedingungen und Einschränkungen für die Nutzung von Telearbeit erlassen. Soweit erforderlich und gesetzlich zulässig, sollten folgende Themen berücksichtigt werden:

a) die bestehende physische Sicherheit des Telearbeitsstandortes unter Berücksichtigung der physischen Sicherheit des Gebäudes und der lokalen Umgebung;

b) die vorgeschlagene physikalische Telearbeitsumgebung;

c) die Sicherheitsanforderungen für die Kommunikation, unter Berücksichtigung des notwendigen Fernzugriffs auf interne organisationseigene Systeme, die Sensibilität der Information auf die zugegriffen und die über Telekommunikationsverbindungen weitergegeben wird sowie die Empfindlichkeit der internen Systeme;

d) die Bereitstellung von virtuellen Desktop-Zugriffen, der Verarbeitung und Speicherung von Information auf privaten Geräten unterbindet;

e) die Gefahr des unbefugten Zugriffs auf Information durch andere Personen in derselben Unterkunft, z. B. Familie und Freunde;

f) die Verwendung von Heimnetzwerken und Anforderungen und Beschränkungen der Konfiguration von drahtlosen Netzwerkdiensten;

g) Richtlinien und Verfahren, um Streitigkeiten über Rechte an geistigem Eigentum zu verhindern, das auf privaten Geräten erarbeitet wurde;

h) Zugang zu Geräten in Privateigentum (um die Sicherheit der Maschine zu überprüfen oder während einer Untersuchung), der von Gesetzes wegen verhindert werden könnte;

i) Software-Lizenzvereinbarungen, die dergestalt sind, dass Organisationen für die Lizenzierung von Client-Software auf privaten Arbeitsgeräten von Beschäftigten oder sonstiger Benutzer, die zu externen Parteien gehören verantwortlich werden könnten;

j) Anforderungen an Schadsoftwareschutz und Firewall.

Die zu berücksichtigen Richtlinien und Regelungen sollten enthalten:

a) die Bereitstellung geeigneter Geräte und Aufbewahrungsmöbel für Telearbeitstätigkeiten, dort wo der Einsatz von privaten, nicht unter der Aufsicht der Organisation stehenden Geräten untersagt ist;

VO

2

se Health Care

essing personal health

olicy.

teleworking by health

l borders and can even
on. Physicians already
pinions. International
ystems in jurisdictions
this need to be taken
ially national systems)

Normen als Umsetzungshilfe: Berechtigungskonzept

Nutzung von Normen zur Umsetzung der Anforderungen der DS-GVO

- DIN EN ISO 22600-1 „Privilegienmanagement und Zugriffssteuerung“, Teil 1: Übersicht und Policy-Management
- DIN EN ISO 22600-2 „Privilegienmanagement und Zugriffssteuerung“, Teil 2: Formale Modelle
- DIN EN ISO 22600-3 „Privilegienmanagement und Zugriffssteuerung“, Teil 3: Implementierungen

Normen als Umsetzungshilfe: Berechtigungskonzept: Nutzung der DIN 22600

Privilegienmanagement und Zugriffssteuerung

a. **Teil 1**
   - Zieldefinition
   - Definitionen, z.B.
     - Authentifizierung
     - Policy-Repository
   - Aufbau einer Policy-Vereinbarung
   - Beispiel einer Textschablone für die Dokumentation
   - Grundlegende Checklisten, z.B.

Normen als Umsetzungshilfe:

Bere

Privile

a. Tei

–

–

A.3.2.1	Verfahren zum Nachweis der Identität des Patienten	Ist-Zustand	Vereinbart
	1. Patientenname		
	2. Patientenkennzahl		
	3. Patientenname und Kennzahl		
	4. Sonstiges (beschreiben):		

A.3.2.2	Verfahren zum Nachweis der Identität des Mediziners	Ist-Zustand	Vereinbart
	1. Name		
	2. Kennzahl		
	3. Name und Kennzahl		
	4. Sonstiges (beschreiben):		

–

–

A.3.2.3	**Patientenzustimmungsverfahren** (in diesem Abschnitt des Anhangs ist nur das Klassifizierungsschema festgelegt. Zur Beschreibung der Zustimmung müssen Informationen über Rolle, Maßnahme, Zweck, Kontext und Umgebungsbedingungen usw. festgelegt werden.)	Ist-Zustand	Vereinbart
	1. Keine Zustimmung des Patienten erforderlich		
	2. Zustimmung des Patienten ist erforderlich		
	3. Die Zustimmung des Patienten wird vom Patienten verlangt und überprüft		
	4. Sonstiges (beschreiben):		

Normen als Umsetzungshilfe: Berechtigungskonzept: Nutzung der DIN 22600

Privilegienmanagement und Zugriffssteuerung

a. **Teil 1**

b. **Teil 2**

- Darstellung der verschiedenen Modelle wie beispielsweise
  - Domainenmodell
  - Dokumentenmodell
  - Policy-Modell
- Darstellung von funktionellen Rollen, z.B.
  - Person, die etwas ver- oder vorschreibt
  - Unterzeicner
- Darstellung von strukturellen Rollen, z.B.
  - Ärztliche Direktorin / Ärztlicher Direktor
  - Chefärztin / Chefarzt
- Beispiel für strukturelle Rollen entspr. ASTM E-1986

Normen als Umsetzungshilfe:
Berechtigungskonzept: Nutzung der DIN 22600

Tabelle B.1 — ASTM E-1986 lizenziertes Gesundheitswesen Personal, das sich unterscheidende Stufen von Access garantiert, kontrolliert

Aktuelle Standardliste von lizenzierten Anbietern des Gesundheitswesens	Empfohlene erweiterte Liste von lizenzierten Anbietern im Gesundheitswesen
Arzt (Dr. med./Allopath, Osteopath, Chiropraktiker, Naturheilkundler, Homöopath)	Arzt (mit Unterkategorien:) Chiropraktiker (ehemals „Chiropraktik“) Homöopath Dr. med./Allopath Naturheilkundler Osteopath Pathologe (neue empfohlene Rolle) Psychiater (neue empfohlene Rolle) Radiologe (neue empfohlene Rolle)
Arztassistent	Arztassistent
Staatlich geprüfte spezialisierte Krankenschwester (NP, NM, CAN, CNS)	Krankenschwester (mit Unterkategorien:) Krankenschwester mit klinischer Spezialisierung (CNS) (ehemals „CNS“) Staatlich geprüfte Anästhesie-Krankenschwester (CRNA) (ehemals „CAN“) Lizenzierte Berufskrankenschwester (LVN)/Lizenzierte praktische Krankenschwester (LPN) (ehemals „Lizenzierte Berufskrankenschwester (LVN)“) Hebammenschwester (NM) (ehemals „Hebammen“ und „NM“) Fachpfleger, Fachpflegerin (NP) (ehemals „NP“) Staatlich geprüfte Krankenschwester (RN)
Hebammen	Siehe Krankenschwester
Staatlich geprüfte Krankenschwester (RN)	Siehe Krankenschwester
Lizenzierte Berufskrankenschwester (LVN)	Siehe Krankenschwester
Pharmazeut (DV)	Pharmazeut (mit Unterkategorien) Pharmazeut, Apotheker (neue empfohlene Rolle) Pharmazeut, klinisch (neue empfohlene Rolle)
Anbieter für nicht-westliche Medizin	Anbieter für nicht-westliche Medizin (mit Unterkategorien) Akupunkteur (neue empfohlene Rolle) Heilmasseur (neue empfohlene Rolle)
Nebenleistungsanbieter	Empfohlen wird die Streichung von „Nebenleistungsanbieter“ und der Ersatz durch detaillierte Anbieterrollen: Audiologe (neue empfohlene Rolle) Zahnmediziner (neue empfohlene Rolle) Diätetiker (neue empfohlene Rolle) Psychologe (neue empfohlene Rolle) Sprachpathologe (neue empfohlene Rolle) Tierarzt, Veterinär (DVM) (neue empfohlene Rolle)
Ergotherapie	Therapeut (mit Unterkategorien:) Audiotherapeut (neue empfohlene Rolle) Bildungstherapeut (neue empfohlene Rolle) Kinesiotherapeut (neue empfohlene Rolle) Musiktherapeut (neue empfohlene Rolle) Berufsbeschäftigungstherapeut (war „Berufstherapie“) Krankengymnast (war „physische Therapie“) Freizeittherapeut (neue empfohlene Rolle) Atemtherapeut (war „Atemtherapie“) Logopäde (war „Sprachtherapie“) Berufstherapeut (neue empfohlene Rolle)
Physiotherapie	Siehe Therapeut
Sprachtherapie	Siehe Therapeut
Atemtherapie	Siehe Therapeut
Techniker	Techniker (mit Unterkategorien:) Kardiologietechniker (neue empfohlene Rolle) Laborant (neue empfohlene Rolle) Pharmazeutisch-technischer Assistent (neue empfohlene Rolle) Prothesentechniker Radiologietechniker (neue empfohlene Rolle)
CAST-Techniker	Empfohlen wird die Streichung. Siehe Techniker
Prothesentechniker	Siehe Techniker
(keine)	Technologe (mit Unterkategorie) (neue empfohlene Rolle) Labortechniker (neue empfohlene Rolle)

Normen als Umsetzungshilfe: Berechtigungskonzept: Nutzung der DIN 22600

Privilegienmanagement und Zugriffssteuerung

a. **Teil 1**
b. **Teil 2**
c. **Teil 3**
   - Umgang mit Zugriffssteuerungsinstrumenten (ACI)
     - Initiator-ACI, Benutzer-ACI
     - Ziel-ACI
     - Aktions-ACI
     - Kontextuelle-ACI
   - Infrastrukturdienste
     - X.509-basierte Zertifikatsspezifikationen
     - XACML-basierte Rollenzuweisung

Normen als Umsetzungshilfe: Schutz der Daten

ISO/IEC DIS 29151: Leitfaden für den Schutz personenbezogener Daten

- Zielsetzung:
  - Etablierung von Kontrollmöglichkeiten bzgl. der Datennutzung
  - Darstellung der hierfür notwendigen Anforderungen
- Ergänzung zu 29134 PIA: Praktische Umsetzung des Schutzes PII
  - Information Security Policies
  - Organisationsstrukturen
    - Umgang mit Behörden und anderen an den Daten interessierten Gruppen
    - Mobilgeräte
    - Telearbeit
  - Geräteverwaltung
  - Zugriffskontrolle
  - ...

Normen als Umsetzungshilfe: Archivierungskonzept

ISO 15489-1 „Records management“

- Records Management („Schriftgutverwaltung“)
  - Part 1: Concepts and principles
  - Part 2: Guidelines
- Steuert
  - Erzeugung/Erhebung
  - Ggfs. Empfang bei einer Übermittlung
  - Nutzung
  - Aufbewahrung
  - Aussonderung/Löschung

  von Records
- Kernaufgabe: Gewährleistung von Aufbewahrungs- und Aussonderungsvorschriften unter Berücksichtigung von
  - Mindestaufbewahrungsfristen (z.B. BTM-Gesetz, RöV)
  - Maximale Aufbewahrungsmöglichkeit (z.B. Haftungsrecht)

Normen als Umsetzungshilfe: Pseudonymisierung

DIN EN ISO 25237 „Pseudonymisierung“

- Stark am Gesundheitswesen orientiert
- Kategorien betroffener Personen dargestellt
- Datenarten besprochen
- Pseudonymisierungsverfahren vorgestellt
- Anhang: Szenarien im Gesundheitswesen

Normen als Umsetzungshilfe: Pseudonymisierung

DIN EN ISO 25237 „Pseudonymisierung“

- Stark
- Kateg
- Date
- Pseu
- Anha

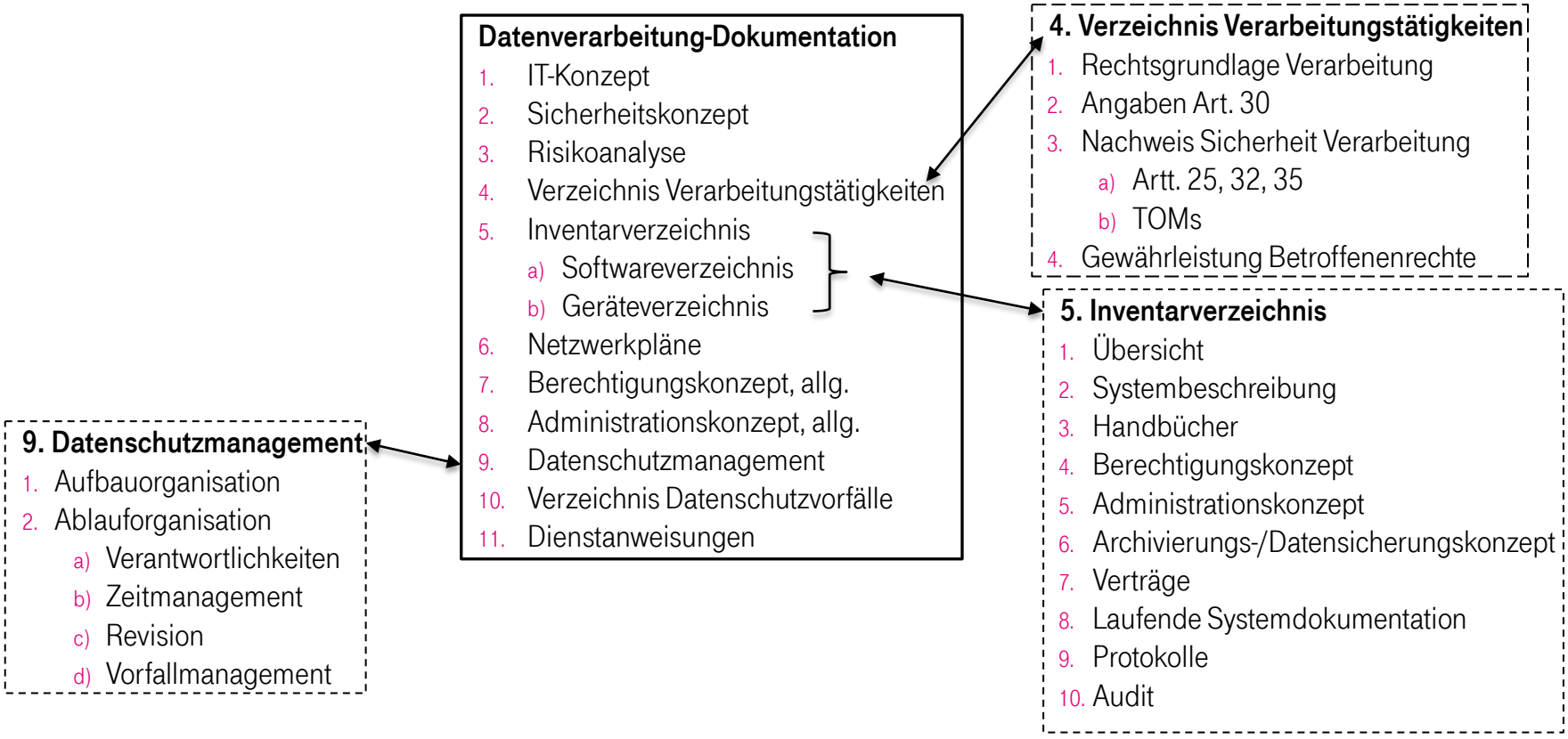
Normen als Umsetzungshilfe: Biometrie als Zugang z.B. zum Rechenzentrum

ISO/IEC 24745: Biometric information protection

- Begriffsdefinitionen
  - biometric characteristic, biometric data, biometric information privacy, unlinkability, ...
- Vorstellung von biometrischen Systemen
- Sicherheitsanforderungen
  - Vertraulichkeit, Integrität, Erneuerbarkeit und Widerrufbarkeit
  - Gefahrenpotential#
  - Sicherheit bei Stand-alone-Datenbanken wie auch bei verteilten Datenbanksystemen
- Management des Datenschutzes in biometrischen Systemen
- Diverse Anhänge
  - Nutzbare kryptographische Algorithmen
  - Pseudonymisierung biometrischer Daten
  - ...

Anforderungen zur Dokumentation in der DS-GVO

Aufbau und Struktur*



* Angelehnt an: Angelika Martin (ULD): DSVO – Handreichung für Datenschutzbeauftragte., S.2 (2007-07-22)

Das Datenschutzkonzept: Dreh- und Angelpunkt

Datenschutzkonzept muss jeder haben: nur der Umfang wird unterschiedlich ausfallen

- Datenschutzkonzept: Wie wird Datenschutz im Unternehmen umgesetzt?
- Ohne Datenschutzkonzept kaum ein Nachweis bzgl. Einhaltung möglich:
  - Wenn nicht im Datenschutzkonzept beschrieben wird, wie Datenschutz im Unternehmen auszusehen hat
  - wie sollen dann Beschäftigte die Vorgaben umsetzen?
- Umfang muss der Verarbeitung angemessen sein
  - Unternehmen, die große Mengen an Daten mit vielen unterschiedlichen Verfahren verarbeiten, benötigen ggf. umfangreiche Dokumentationen als andere Unternehmen
  - Sprich: Datenschutzkonzept wird im Krankenhaus anders aussehen als in der Arztpraxis
- Frage, ob man es „Datenschutzkonzept“ oder „Prozessdokumentation“ oder „…“ nennt, weniger relevant, wie der Inhalt
- Siehe Beispiel: Was braucht man immer, auf was kann man ggf. verzichten?

Diskussion / Fragen

Kontakt: Bernd.Schuetze@T-Systems.com