DIN EN ISO/IEC 27701:2021-07

Norm für Datenschutzmanagement

Dr. Bernd Schütze

4. Fachtagung „Datenschutz im Gesundheitswesen“, 2022-05-12

HEALTHCARE SOLUTIONS

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)
- Bundesverband Gesundheits-IT e. V (bvitg)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.

Agenda

Was möchte ich vorstellen?

- (Kurze) Darstellung der Entstehungsgeschichte
- Abgrenzung
- DIN EN ISO/IEC 27701: Was sie beinhaltet
- Fazit/Zusammenfassung
- Literatur

Entstehungsgeschichte

Entstehungsgeschichte

Wie alles begann...

- 2016-04
  - WG 5 (Identity management and privacy technologies) schlug dem
  - Subcommittee JTC 1/SC 27 (Information security, cybersecurity and privacy protection) von ISO/IEC
  - auf Initiative von Experten des französischen nationalen Gremiums des JTC 1/SC 27 Thema vor
  - Entwicklung des Projektes erfolgte unter der Nummer ISO/IEC 27552
- 2018-02: British Standards Institution (BSI) veröffentlichte erste CD (Committee Draft)
- 2018-08: Zweite CD veröffentlicht
- 2019-01,03: DIS (Draft International Standard) veröffentlicht
- 2019-04: Beendigung der Arbeit am Standard ISO/IEC 27552
- 2019-07: Umnummerierung gemäß der Entschließung 39/2019 des ISO/Technical Management Board in ISO/IEC 27701
- **2019-08**: Veröffentlichung des Standards ISO/IEC 27701:2019
- 2021-04: CEN veröffentlicht EN ISO/IEC 27701:2021
- **2021-07**: DIN veröffentlicht deutsche Fassung DIN EN ISO/IEC 27701:2021-07

Abgrenzung

Abgrenzung

Was die DIN EN ISO/IEC 27701 nicht ist...

- Die DIN EN ISO/IEC 27701beschreibt ein Datenschutz-Management-System, welches zertifiziert werden kann
- Die DIN EN ISO/IEC 27701ist daher **keine Zertifizierung im Sinne von Art. 42 DS-GVO**
- Art. 42 DS-GVO:
  - Abs. 1: „[...] datenschutzspezifischen Zertifizierungsverfahren [...], die dazu dienen, nachzuweisen, dass diese Verordnung **bei Verarbeitungsvorgängen** von Verantwortlichen oder Auftragsverarbeitern **eingehalten wird**.
  - Abs. 2:“Zusätzlich [...] können auch datenschutzspezifische Zertifizierungsverfahren [...] vorgesehen werden, um nachzuweisen, dass [...] im Rahmen der Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen [...] geeignete Garantien bieten.

DIN EN ISO/IEC 27701: Was die Norm beinhaltet

Für die Eiligen

Die wichtigsten Fragen in aller Kürze

- DIN EN ISO/IEC 27701 :=
  Globales Datenschutz Managementsystem für mehr Sicherheit
- Ist eine Zertifizierung mit der DIN EN ISO/IEC 27701 möglich?
  - Ja, aber...
    - ➢ Die eigentliche Zertifizierung erfolgt gemäß DIN EN ISO/IEC 27001
    - ➢ Dabei wird die 27001 um die Anforderungen der 27701 ergänzt
  - Nein
    - ➢ Als alleinstehende Norm
- Können mit der DIN EN ISO/IEC 27701Anforderungen der DS-GVO adressiert werden?
  - Ja ! ☺

Aufbau der Norm

Inhalt der Norm

Der Aufbau der Norm entspricht dem anderer Normen, d.h.

1. Anwendungsbereich
2. Normative Verweisungen
3. Begriffe
4. Allgemeines
5. PIMS-spezifische Anforderungen in Bezug auf ISO/IEC 27001
   (PIMS = Privacy Information Managementsystem)
6. PIMS-spezifische Leitlinien in Bezug auf ISO/IEC 27002
7. Zusätzliche Leitlinie für verantwortliche Stellen nach ISO/IEC 27002
8. Zusätzliche Leitlinie für Auftragsverarbeiter nach ISO/IEC 27002

Aufbau der Norm

Inhalt der Norm

Ergänzt durch Anhänge

Anhang A: PIMS-spezifische Referenzmaßnahmenziele und –Maßnahmen (verantwortliche Stelle)

Anhang B: PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen (Auftragsverarbeiter)

Anhang C: Zuordnung zu ISO/IEC 29100

Anhang D: Zuordnung zur Datenschutz-Grundverordnung

Anhang E: Zuordnung zu ISO/IEC 27018 und ISO/IEC 29151

Anhang F: Anwendung von ISO/IEC 27701 auf ISO/IEC 27001 und ISO/IEC 27002

Inhalte: Eher Allgemeines

Anwendungsbereich

1. Anwendungsbereich
   - Leitlinie für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Managementsystems für Informationen zum Datenschutz (PIMS)
   - Erweiterung der ISO/IEC 27001 und ISO/IEC 27002 um Datenschutzaspekte
2. Normative Verweisungen
   - DIN EN ISO/IEC 27000 (Informationssicherheitsmanagementsysteme - Überblick und Terminologie)
   - DIN EN ISO/IEC 27001(Informationssicherheitsmanagementsysteme – Anforderungen)
   - DIN EN ISO/IEC 27002 (Leitfaden für Informationssicherheitsmaßnahmen)
   - DIN EN ISO/IEC 29100 (Rahmenwerk für Datenschutz)

Inhalte: Eher Allgemeines

Anwendungsbereich

3. Begriffe
   - Verweis auf Begriffe nach ISO/IEC 27000; ISO/IEC 29100
   - Ergänzt um
     - gemeinsame verantwortliche Stelle
     - Managementsystem für Datenschutzinformationen (PIMS)
4. Allgemeines
   - Beschreibung der Aufbau der Norm
   - Anwendung der Anforderungen der ISO 27001sowie 27002
   - Einordnung der Begrifflichkeit „Kunde“

5. PIMS-spezifische Anforderungen in Bezug auf ISO/IEC 27001

5.2 Kontext der Organisation, 5.3 Führung

DIN EN ISO/IEC 27001	DIN EN ISO/IEC 27701
4.4 Informationssicherheitsmanagementsystem – Die Organisation muss entsprechend den Anforderungen dieser Internationalen Norm ein Informationssicherheitsmanagementsystem aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern. 5.1 Führung und Verpflichtung – Die oberste Leitung muss in Bezug auf das Informationssicherheitsmanagementsystem Führung und Verpflichtung zeigen, indem sie: a) ...	5.2.4 Managementsystem für Informationssicherheit – Die Organisation muss ein PIMS in Übereinstimmung mit den Anforderungen der ISO/IEC 27001:2013 [...] einrichten, umsetzen, aufrechterhalten und fortlaufend verbessern. 5.3.1 Führung und Verpflichtung – Es gelten die in ISO/IEC 27001:2013, 5.1, genannten Anforderungen sowie die in 5.1 festgelegte Interpretation.

6. PIMS-spezifische Leitlinien in Bezug auf ISO/IEC 27002

6.2.1.1 Richtlinien für die Informationssicherheit

DIN EN ISO/IEC 27002	DIN EN ISO/IEC 27701

- Die DIN EN ISO/IEC 27701 verweist immer wieder auf die DIN EN ISO/IEC 27001 bzw. 27002
- Die Anforderungen der DIN EN ISO/IEC 27701 können daher nur in Kenntnis der anderen Normen richtig interpretiert und umgesetzt werden

7. Zusätzliche Leitlinie für verantwortliche Stellen nach ISO/IEC 27002

Keine Entsprechungen in der DIN EN ISO/IEC 27002

- DIN EN ISO/IEC 27701 enthält natürlich diverse Anforderungen, die in den Normen zur IT-Sicherheit so nicht vorhanden sind: Die datenschutzspezifischen Anforderungen
- Zum Beispiel
  - 7.2.1 Identifizieren und Dokumentieren des Zwecks
    - Maßnahme
      Die Organisation sollte die spezifischen Zwecke, für die die personenbezogenen Daten verarbeitet werden, identifizieren und dokumentieren.
  - 7.2.4 Einholung und Aufzeichnung der Einwilligung
    - Maßnahme
      Die Organisation sollte die Einwilligung der betroffenen Personen nach den dokumentierten Prozessen einholen und aufzeichnen.

8. Zusätzliche Leitlinie für Auftragsverarbeiter nach ISO/IEC 27002

Keine Entsprechungen in der DIN EN ISO/IEC 27002

- DIN EN ISO/IEC 27701 enthält natürlich diverse Anforderungen, die in den Normen zur IT-Sicherheit so nicht vorhanden sind: Die datenschutzspezifischen Anforderungen
- Zum Beispiel: Verarbeitung personenbezogener Daten im Auftrag
  - 8.2.4 Verstoßende Anweisung
    - Maßnahme
      Die Organisation sollte den Kunden informieren, wenn ihrer Meinung nach eine Verarbeitungsanweisung gegen geltende Gesetze und/oder Vorschriften verstößt.
  - 8.2.6 Aufzeichnungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten
    - Maßnahme
      Die Organisation sollte die notwendigen Aufzeichnungen zum Nachweis der Einhaltung ihrer Verpflichtungen (wie im anwendbaren Vertrag festgelegt) für die Verarbeitung von personenbezogenen Daten, die im Namen eines Kunden durchgeführt wird, festlegen und führen.

Warum die DIN EN ISO/IEC 27701 auch ohne 27001/27002 interessant sein kann: Anhang D

Anhang D: Zuordnung zur Datenschutz-Grundverordnung

– In Anhang D werden die Anforderungen der Norm den Anforderungen der Artt. Der DS-GVO zugeordnet

Tabelle D.1 — Zuordnung der Struktur von ISO/IEC 27701 auf die Artikel der DSGVO

Unterabschnitt dieses Dokuments	Artikel der DSGVO
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)
6.4.2.2	(39)(1)(b)
6.5.2.1	(5)(1)(f), (32)(2)
6.5.2.2	(5)(1)(f)
6.5.3.1	(5)(1)(f), (32)(1)(a)
6.5.3.2	(5)(1)(f)
6.5.3.3	(5)(1)(f), (32)(1)(a)
6.6.2.1	(5)(1)(f)
6.6.2.2	(5)(1)(f)
6.6.4.2	(5)(1)(f)
6.7.1.1	(32)(1)(a)

DS-GVO trifft DIN EN ISO/IEC 27701

Da kann einem schon mal etwas bekannt vorkommen...

Datenschutz-Grundverordnung	DIN EN ISO/IEC 27701
Art. 7 Abs. 3 – Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Art. 15 Abs. 3 – Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung.	7.3.4 Bereitstellung eines Mechanismus zur Änderung oder zum Widerruf der Einwilligung – Die Organisation sollte einen Mechanismus zur Verfügung stellen, mit dem betroffene Personen ihre Einwilligung ändern oder widerrufen können. 7.3.8 Bereitstellung einer Kopie der verarbeiteten personenbezogenen Daten – Die Organisation sollte in der Lage sein, eine Kopie der personenbezogenen Daten, die auf Anfrage der betroffenen Person verarbeitet werden, zur Verfügung zu stellen.

DS-GVO trifft DIN EN ISO/IEC 27701

Da kann einem schon mal etwas bekannt vorkommen...

Datenschutz-Grundverordnung	DIN EN ISO/IEC 27701
Art. 28 Abs. 3 lit. a – die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen [...] verarbeitet	8.2.2 Ziele der Organisation – Die Organisation sollte sicherstellen, dass personenbezogene Daten, die im Namen eines Kunden verarbeitet werden, nur für die Ziele verarbeitet werden, die in den dokumentierten Anweisungen des Kunden zum Ausdruck kommen.
Art. 28 Abs. 3 lit. e – [...] nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen	8.3.1 Verpflichtungen gegenüber betroffenen Personen – Die Organisation sollte dem Kunden die Mittel zur Verfügung stellen, um seinen Verpflichtungen in Bezug auf betroffene Personen nachzukommen.

Warum die DIN EN ISO/IEC 27701 auch ohne 27001/27002 interessant sein kann: Anhang A

Anhang A: PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen

– Die Liste in Anhang A kann als Checkliste für den Verantwortlichen dienen

Tabelle A.1 — Maßnahmenziele und Maßnahmen

A.7.2 Bedingungen für die Erhebung und Verarbeitung Zielsetzung: Bestimmen und Dokumentieren, dass die Verarbeitung rechtmäßig ist, mit einer rechtlichen Grundlage nach den geltenden Rechtssystemen und mit klar definierten und legitimen Zwecken.		
A.7.2.1	Identifizieren und Dokumentieren des Zwecks	*Maßnahme* Die Organisation muss die spezifischen Zwecke, für die die personenbezogenen Daten verarbeitet werden, identifizieren und dokumentieren.
A.7.2.2	Identifizieren der rechtmäßigen Grundlage	*Maßnahme* Die Organisation muss die geeignete rechtmäßige Grundlage für die Verarbeitung von personenbezogenen Daten für die identifizierten Zwecke bestimmen, dokumentieren und einhalten.
A.7.2.3	Bestimmen, wann und wie die Einwilligung einzuholen ist	*Maßnahme* Die Organisation muss ein Verfahren festlegen und dokumentieren, mit dem sie nachweisen kann, ob, wann und wie die Einwilligung zur Verarbeitung von personenbezogenen Daten von den betroffenen Personen eingeholt wurde.
A.7.2.4	Einholung und Aufzeichnung der Einwilligung	*Maßnahme* Die Organisation muss die Einwilligung der betroffenen Personen nach den dokumentierten Prozessen einholen und aufzeichnen.
A.7.2.5	Datenschutz-Folgenabschätzung	*Maßnahme* Die Organisation muss immer dann, wenn eine neue Verarbeitung von personenbezogenen Daten oder Änderungen an der bestehenden Verarbeitung von personenbezogenen Daten geplant ist, die Notwendigkeit einer Datenschutz-Folgenabschätzung bewerten und gegebenenfalls umsetzen.

Warum die DIN EN ISO/IEC 27701 auch ohne 27001/27002 interessant sein kann: Anhang B

Anhang A: PIMS-spezifische Referenzmaßnahmenziele und -Maßnahmen

– Die Liste in Anhang B kann als Checkliste bei Verarbeitung in Auftrag dienen

Tabelle B.1 — Maßnahmenziele und Maßnahmen

B.8.2 Bedingungen für die Erhebung und Verarbeitung Zielsetzung: Bestimmen und Dokumentieren, dass die Verarbeitung rechtmäßig ist, mit einer rechtlichen Grundlage nach den geltenden Rechtssystemen und mit klar definierten und legitimen Zwecken.		
B.8.2.1	Kundenvereinbarung	*Maßnahme* Die Organisation muss, wo dies relevant ist, sicherstellen, dass der Vertrag zur Verarbeitung von personenbezogenen Daten bei der Rolle der Organisation durch Hilfestellung bei den Verpflichtungen des Kunden ansetzt (unter Berücksichtigung der Art der Verarbeitung und der der Organisation zur Verfügung stehenden Informationen).
B.8.2.2	Ziele der Organisation	*Maßnahme* Die Organisation muss sicherstellen, dass personenbezogene Daten, die im Namen eines Kunden verarbeitet werden, nur für die Ziele verarbeitet werden, die in den dokumentierten Anweisungen des Kunden zum Ausdruck kommen.
B.8.2.3	Verwendung für Marketing und Werbung	*Maßnahme* Die Organisation darf personenbezogene Daten, die im Rahmen eines Vertrags verarbeitet werden, nicht für Marketing- und Werbezwecke verwenden, ohne nachzuweisen, dass die vorherige Einwilligung der jeweiligen betroffenen Person eingeholt wurde. Die Organisation darf die Erteilung einer solchen Einwilligung nicht zur Bedingung für den Erhalt der Dienstleistung machen.
B.8.2.4	Verstoßende Anweisung	*Maßnahme* Die Organisation muss den Kunden informieren, wenn ihrer Meinung nach eine Verarbeitungsanweisung gegen geltende Gesetze und/oder Vorschriften verstößt.

Fazit

Fazit

DIN EN ISO/IEC 27701 stellt bei der Umsetzung eines DSMS eine gute Unterstützung dar

- DIN EN ISO/IEC 27701 ist keine Zertifizierung nach Art. 42 DS-GVO, richtig
- Aber die DIN EN ISO/IEC 27701
  - stellt ein international anerkanntes Datenschutz Management System dar
  - kann in andere (ISO) Management Systeme integriert werden
  - kann den Aufwand bzgl. des Nachweises, dass geeignete technische und organisatorische Maßnahmen im Sinne der DS-GVO umgesetzt wurden, deutlich reduzieren
  - kann eine eventuelle Prüfung durch die Datenschutz-Aufsichtsbehörde oder durch andere Dritte wie Kunden erleichtern
  - kann eine Art. 42 Zertifizierung unterstützen
- Die 31 Controls aus Anhang A sowie 18 Controls aus Anhang B bieten auch ohne ISO-Zertifizierung eine gute Leitplanke für die Umsetzung der Anforderungen der DS-GVO

Literatur

Literatur

DIN EN ISO/IEC 27701: Eine sehr subjektive Auswahl an Literatur

- Standard selbst
  - DIN: Beuth, als pdf, Kosten 164,10 Euro
  - ISO/IEC: ISO, als pdf (englisch, dafür inkl. epub), Kosten 178 CHF (ca. 164 Euro)
- Zeitschriften
  - Maier N, Pawlowska IM, Lins S, Sunyaev A. (2020) Die Zertifizierung nach der DS-GVO. ZD: 445-449
  - Maier-Reinhardt N. (2021) Vergleich nationaler Akkreditierungsanforderungen nach Art. 43 Abs. 3 i.V.m. 57 Abs. 1 lit. p DS-GVO. ZD-Aktuell: 05169
  - Rehfeld S. (2021) Add-on für den Datenschutz. ISO 27701 – Blaupause für einen systematischen und compliancekonformen Datenschutz. <kes> 3:73-75
  - Rost M, Sowa A. (2020) Die ISO 27701 und das SDM-V2 im Lichte der Umsetzung der DSGVO. DuD: 659-662
- Bücher
  - Shipman A, Watkins S. (2020) ISO/IEC 27701 2019: An Introduction to Privacy Information Management . IT Governance Publishing. ISBN 978-1787781993
- Und natürlich ist im Internet einiges zu finden, vor allem Werbung ;-) Aber z.B.
  - ISACA: Implementierungsleitfaden ISO/IEC 27001:2013. Stand: Mai 2016. Online unter https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf
  - Lachaud E. 2020) ISO/IEC 27701: Threats and Opportunities for GDPR Certification. Online unter https://www.researchgate.net/publication/338676835_ISOIEC_27701_Threats_and_Opportunities_for_GDPR_Certification

Diskussion / Fragen

Kontakt: schuetze@medizin-informatik.org