TOMs unter der DS-GVO: Wie sehen zukünftig Checklisten aus?

Dr. Bernd Schütze

36. Sitzung der GMDS-AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

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

Einsatz von Checklisten unter der DS-GVO

- Geänderte Rahmenbedingungen
- Bedeutung für Checklisten
- Prüfung des Auftragsverarbeiters
- Fazit

Geänderte Rahmenbedingungen

BDSG und Checklisten

Anlage zu § 9 S. 1 BDSG

- Checklisten prüfen i.d.R. die Umsetzung von § 9 S. 1 BDSG, d.h.
  - Zutrittskontrolle
  - Zugangskontrolle
  - Zugriffskontrolle
  - Weitergabekontrolle
  - Eingabekontrolle
  - Auftragskontrolle
  - Verfügbarkeitskontrolle
  - Mandantentrennung

- Anders ausgedrückt: Sie dienen der Prüfung der technisch-organisatorischen Maßnahmen (TOM) aus der Anlage (zu § 9 Satz 1) BDSG

Anforderungen aus der DS-GVO bzgl. IT-Sicherheit

Art. 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

- Treffen geeigneter technisch-organisatorische Maßnahmen (Art. 25 Abs. 2)
  - zur Umsetzung der Datenschutzgrundsätze
  - zur Durchsetzung der Betroffenenrechte
- unter Berücksichtigung (Art. 25 Abs. 1)
  - des Stands der Technik
  - der Implementierungskosten
  - der Art, Umfang, Umstände und Zwecke
  - der Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen

➔ Beschränkung der Verarbeitung durch Voreinstellung auf das Erforderliche:

- Beschränkung auf den oder die Verarbeitungszweck(e)
- Beschränkung der Datenmenge
- Beschränkung des Verarbeitungsumfangs
- Beschränkung der Speicherfristen
- Beschränkung der Zugänglichkeit

Anforderungen aus der DS-GVO bzgl. IT-Sicherheit

Art. 32: Sicherheit der Verarbeitung

Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten

geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten

IT-Sicherheit und DS-GVO

Technische und organisatorische Maßnahmen in der DS-GVO

- Die für Checklisten genutzte Aufzählung der technisch-organisatorischen Maßnahmen fehlt in der DS-GVO
- Konzept der Datensicherheit :
  - Risikoanalyse und
  - ein dem Risiko angemessenes Schutzniveau

IT-Sicherheit und DS-GVO

Technische und organisatorische Maßnahmen in der DS-GVO

Wahrung Datenschutzgrundsätze, d. h. per „Voreinstellung“ gem. Art. 25 DS-GVO grundsätzlich nur Verarbeitung

- für den jeweiligen bestimmten Verarbeitungszweck
- nur die Menge an Daten und
- den Verarbeitungsumfang
- unter Beachtung der erforderliche Speicherfrist
- und wahren nur der erforderlichen Zugänglichkeit

→ Anforderungen von Art. 5 einhalten

→ Gewährleistung Sicherheit der Verarbeitung gefordert

IT-Sicherheit und DS-GVO

Technische und organisatorische Maßnahmen in der DS-GVO

Art. 32 DS-GVO: TOM **schließen** u.a. Folgendes **ein**:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer **sicherzustellen**;
- die Fähigkeit, die **Verfügbarkeit** der Daten und den **Zugang** zu ihnen bei einem physischen oder technischen **Zwischenfall rasch wiederherzustellen**;
- ein **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

IT-Sicherheit und DS-GVO

Technische und organisatorische Maßnahmen in der DS-GVO

D.h. Art. 32 DS-GVO fordert u.a.

- Maßnahmen
  - Pseudonymisierung
  - Verschlüsselung
- Fähigkeiten
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Belastbarkeit
  - Wiederherstellbarkeit
  - Notallmanagement
- Verfahren
  - Überprüfbarkeit
  - Bewertung
  - Evaluierung

Unter Berücksichtigung

→ Stand der Technik

→ Implementierungskosten

→ Art, Umfang, Umstände und Zwecke der Verarbeitung

→ Risiko der Verarbeitung

IT-Sicherheit entsprechend DS-GVO

Anforderungen der DS-GVO

IT-Sicherheit gemäß DS-GVO prüfen heißt:

- Risikoevaluierung und –beurteilung
- Darstellung eines Maßnahmenkatalogs zur Risikominimierung
- (Interne) Audits inkl. Managementbewertung
- Verfahren zur Korrektur/Anpassung von ergriffenen Maßnahmen („PDCA-Zyklus“)

➔ IT-Sicherheits-Managementsystem inkl.

- Datenschutzkonzept
- IT-Sicherheitskonzept

Bedeutung für Checklisten

Checklisten unter der DS-GVO

Abbildung der Anforderungen der DS-GVO gefordert

- Checklisten nicht länger eine Abbildung der Anlage zu § 9 BDSG
  - → DS-GVO fordert weder Mandantentrennung noch eine andere bisher geprüfte Vorgabe der Anlage
- Checklisten müssen individuell entsprechend der jeweiligen Risikoanalyse aufgebaut sein
  - → Die *Risikoanalyse* kann auch eine Mandantentrennung erfordern.
    (Oder jede andere der bisherigen Vorgaben der Anlage zu § 9 BDSG)

➔ Die bisherigen Maßnahmen sind natürlich nicht obsolet, denn die Technik ändert sich ja nicht mit dem Gesetz

➔ Geprüft werden muss jedoch, ob eine der bisherigen Maßnahmen **angemessen** ist

- → Oder nur gefordert wurde, um dem Katalog zur Anlage zu § 9 BDSG zu genügen
- → In diesem Fall ist die Maßnahme nicht länger zu fordern und muss aus der Checkliste entfernt werden

Checklisten unter der DS-GVO

Abbildung der Anforderungen der DS-GVO gefordert

Art. 32 DS-GVO fordert die Berücksichtigung („*schließen ein*“)

- Maßnahmen
  - Pseudonymisierung
  - Verschlüsselung
- Fähigkeiten
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Belastbarkeit
  - Wiederherstellbarkeit
  - Notallmanagement
- Verfahren
  - Überprüfbarkeit
  - Bewertung
  - Evaluierung

1. In Checkliste darstellen
2. Prüfen, ob im jeweiligen Fall erforderlich zur Gewährleistung eines angemessenen Schutzniveaus
   a) Falls nicht erforderlich: in Checkliste Begründung aufnehmen
   b) Falls erforderlich: in Checkliste darstellen, wie abgebildet

Prüfung des Auftragsverarbeiters

Auswahl des Auftragsverarbeiters

Anforderungen der DS-GVO

- Art. 28 DS-GVO
  - (1) „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet“
  - (3) [...] Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter
    - c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;
- Der Verantwortliche muss den Auftragsverarbeiter auch dahingehend prüfen, ob das von Artt. 32 DS-GVO geforderte Schutzniveau
  - eingehalten werden kann (vor Auftragsvergabe) und
  - eingehalten wird (während der Auftragsverarbeitung)

Auswahl des Auftragsverarbeiters

Prüfung des Auftragsverarbeiters

- Art. 28 DS-GVO

  (5) „Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann **als Faktor** herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.“

➔ Nachweis erfolgt nicht alleine basierend auf genehmigte Verhaltensregel oder eine Zertifizierung

➔ Beides sind ggf. Faktoren, um hinreichende Garantien nachzuweisen

➔ Zertifizierung alleine evtl. nicht ausreichend

Auswahl des Auftragsverarbeiters

Was ist eine Zertifizierung?

- „Als Zertifizierung [...] bezeichnet man ein Verfahren, mit dessen Hilfe die Einhaltung bestimmter Anforderungen nachgewiesen wird.
  Zertifizierung ist ein Teilprozess der Konformitätsbewertung.“ (Quelle: Wikipedia*)
- Zertifizierung: Prüfung auf Konformität zu Anforderungen, bzw. auf Einhaltung der Anforderungen
- Zertifizierung letztlich nichts anderes als Überprüfung einer (mehr oder weniger komplexen) Checkliste

➔ Checklisten auch unter der DS-GVO akzeptiertes Mittel

➔ Ggf. zum Nachweis der Konformität zu Art. 32 DS-GVO Zertifizierung um individuelle Checkliste ergänzen

* https://de.wikipedia.org/wiki/Zertifizierung

Fazit

Fazit

Was kann man mitnehmen? Was ist zu tun?

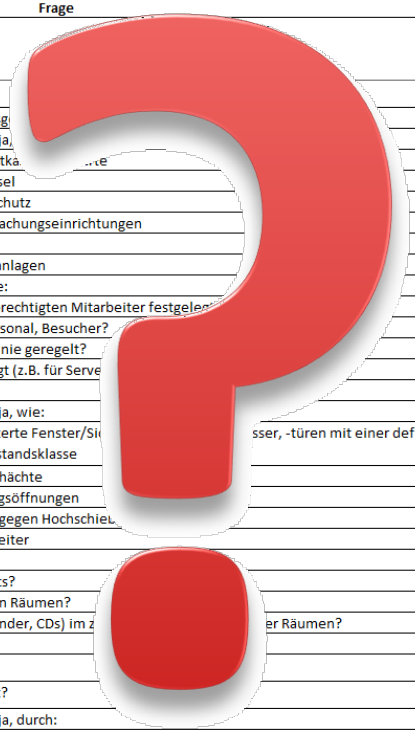
- Checklisten bleiben wichtiges Hilfsmittel
- Auch unter DS-GVO können bisherige Anforderungen wie
  - Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Mandantentrennung

  gefordert sein – wenn die Risikoanalyse hier Handlungsbedarf ergibt
- „Starre“ Checklisten unter Risikoansatz der DS-GVO nicht mehr zielführend
- Künftige Checklisten müssen
  - Pseudonymisierung und Verschlüsselung
  - Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit, Notallmanagement
  - Überprüfbarkeit, Bewertung, Evaluierung

  berücksichtigen
- Sollte unsere AG eine Beispiele bzgl. der neuen Anforderungen erarbeiten?

Diskussion

	A	B	C	D	E	F	G
1		Frage		Vom AN auszufüllen		Vom AG auszufüllen	
2	Kategorie	Kernfrage		Ja (x, leeres Feld)	Nein (x, leeres Feld)	Trifft nicht zu (x, leeres Feld)	Gewichtung (Wert zwischen 1 und 10)
50		**TOMs 1: Zutrittskontrolle**					
51	TOMs1	Erfolgt eine Zutrittskontrolle für den Zutritt zum Betriebsg					
52	TOMs1		Wenn ja,				
53			Magnetka…te				
54			Schlüssel				
55			Werkschutz				
56			Überwachungseinrichtungen				
57			Video				
58			Alarmanlagen				
59			Andere:				
60	TOMs1	Existiert ein Zutrittskontrollsystem, in dem die zutrittsberechtigten Mitarbeiter festgele…					
61	TOMs1	Bestehen Regelungen für Fremdpersonal, Reinigungspersonal, Besucher?					
62	TOMs1	Ist die Begleitung von Gästen im Gebäude in einer Richtlinie geregelt?					
63	TOMs1	Sind differenzierte Sicherheitsbereiche/-zonen festgelegt (z.B. für Serve…					
64	TOMs1	Ist der Rechenzentrums (RZ) Zutritt gesichert?					
65	TOMs1		Wenn ja, wie:				
66			Vergitterte Fenster/Si… sser, -türen mit einer definierten Widerstandsklasse				
67			Lichtschächte				
68			Lüftungsöffnungen				
69			Rollos gegen Hochschie…				
70			Feuerleiter				
71	TOMs1	Sind die Server in abschließbaren Serverschränken?					
72	TOMs1	Sind Datenträger Bestandteil eines Zutrittsschutzkonzepts?					
73	TOMs1	Sind gelagerte Notebooks unter Verschluss in gesicherten Räumen?					
74	TOMs1	Erfolgt die Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im z… er Räumen?					
75	TOMs1	Liegt eine Anweisung zur Ausgabe von Schlüsseln vor?					
76		**TOMs 2: Zugangskontrolle**					
77	TOMs2	Wird die unbefugte Nutzung von IT-Systemen verhindert?					
78	TOMs2		Wenn ja, durch:				
79			User-ID				



Kontakt: Bernd.Schuetze@T-Systems.com