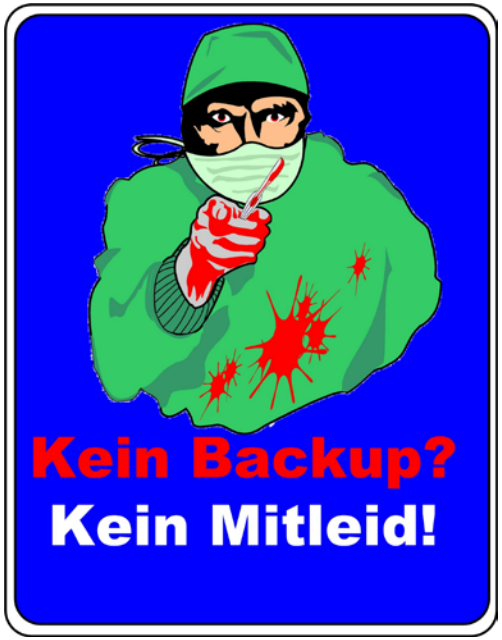


Die Sicherheit der Verarbeitung

Anforderungen aus Art. 32 DS-GVO

Dr. Bernd Schütze

Seminar Datenschutz-Grundverordnung (DS-GVO)

HEALTHCARE SOLUTIONS

Agenda

Worum geht es eigentlich?

- Sicherheit der Verarbeitung
- Technisch-organisatorische Maßnahmen
- Checklisten: Haben sie noch eine Zukunft?

Sicherheit der Verarbeitung

Sicherheit der Verarbeitung

Rechtliche Anforderungen

- Treffen geeigneter technisch-organisatorische Maßnahmen (Art. 32 Abs. 1)
  - um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
- unter Berücksichtigung (Art. 32 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
- Hinweis: Genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor zum Nachweis der Anforderungen dienen

Sicherheit der Verarbeitung

Inhalt der Pflicht

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

Sicherheit der Verarbeitung

Technisch-organisatorische Maßnahmen (TOM) gefordert

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 (Art. 32 Abs. 1 DS-GVO)

Sicherheit der Verarbeitung

Angemessene Maßnahmen

Die Beurteilung der Angemessenheit ist eine Abwägung beinhaltend

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Eintrittswahrscheinlichkeit
- Schwere des Risikos für die persönlichen Rechte und Freiheiten

Sicherheit der Verarbeitung

Ergänzend: § 22 Abs. 2 BDSG n.F.

§ 22 Verarbeitung besonderer Kategorien personenbezogener Daten

(2) In den Fällen des Absatzes 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. 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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. [...],
2. **Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind**,
3. **Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,**
4. **Benennung einer oder eines Datenschutzbeauftragten**,
5. **Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern**,
6. [...] oder
7. **spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.**

– Anforderung 1, 6-9: zu Art. 32 DS-GVO praktisch identische Anforderungen

– Aber: Sämtliche Maßnahmen von Abs. 2 müssen bzgl. Notwendigkeit und Angemessenheit geprüft werden*

* Weichert T: § 22 BDSG Rn. 18 in Kühling/Buchner. DS-GVO · BDSG. Verlag C.H.Beck. ". Auflage, ISBN 978-3-406-71932-5

Technisch-organisatorische Maßnahmen (TOM)

Technisch-organisatorische Maßnahmen (TOM)

Ziele der TOMs

Wahrung Datenschutzgrundsätze, d. h. per „Voreinstellung“ 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

→ Sicherheit der Verarbeitung gefordert

Technisch-organisatorische Maßnahmen (TOM)

TOM: Vorgabe durch Art. 32 Abs. 1 lit. a DS-GVO

Diese Maßnahmen schließen u.a. Folgendes ein:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- [...]

→ D.h. Pseudonymisierung und Verschlüsselung gefordert

→ Begründung erforderlich, wenn darauf verzichtet wird

Technisch-organisatorische Maßnahmen (TOM)

TOM: Pseudonymisierung

Bundesdatenschutzgesetz	EU Datenschutzgrundverordnung
§3 Abs. 6a: Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die **Bestimmung des Betroffenen auszuschließen** oder **wesentlich zu erschweren**	Art. 4 Abs. 5: "Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen **nicht mehr einer spezifischen betroffenen Person zugeordnet werden können**, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden
§3 Abs. 6: „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse **nicht mehr** oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder **bestimmbaren natürlichen Person zugeordnet werden können**	-

Technisch-organisatorische Maßnahmen (TOM)

Abgrenzung: Pseudonym vs. Anonym

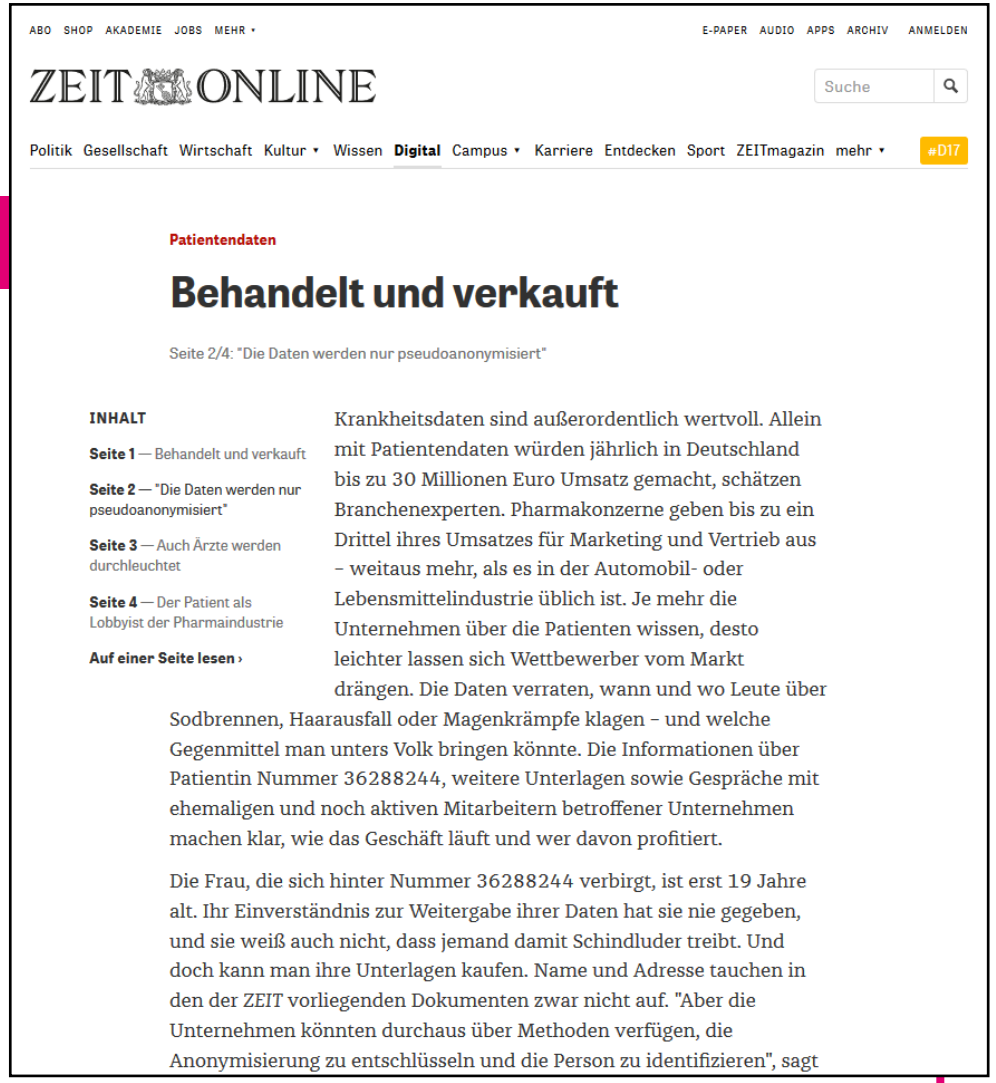
Wann sind Daten als „anonym“ anzusehen, wann als pseudonym?

- Definition „Pseudonym“ der EU DS-GVO beinhaltet, was Stand heute in Deutschland als „faktisch anonym“ angesehen wird
- Artikel-29-Datenschutzgruppe*
  - „Ein häufiger Irrtum liegt in der Annahme, dass pseudonymisierte Daten mit anonymisierten Daten gleichzusetzen seien“
  - „Pseudonymisierung verringert die Verknüpfbarkeit eines Datenbestands mit der wahren Identität einer betroffenen Person und stellt somit eine sinnvolle Sicherheitsmaßnahme, aber kein Anonymisierungsverfahren dar“
  - Häufiger Fehler: „Annahme, dass ein pseudonymisierter Datenbestand anonymisiert ist...“
  - „... Ergebnis der Anonymisierung ... so dauerhaft sein sollte wie eine Löschung ... es darf nicht möglich sein, die personenbezogenen Daten weiter zu verarbeiten“

* Quelle: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

Technisch-organisatorische Maßnahmen (TOM)

Abgrenzung: Pseudonym vs. Anonym



ABO SHOP AKADEMIE JOBS MEHR ▾ E-PAPER AUDIO APPS ARCHIV ANMELDEN

ZEIT ONLINE

Suche

Politik Gesellschaft Wirtschaft Kultur ▾ Wissen **Digital** Campus ▾ Karriere Entdecken Sport ZEITmagazin mehr ▾ #D17

Patientendaten

Behandelt und verkauft

Seite 2/4: "Die Daten werden nur pseudoanonymisiert"

INHALT

Krankheitsdaten sind außerordentlich wertvoll. Allein mit Patientendaten würden jährlich in Deutschland bis zu 30 Millionen Euro Umsatz gemacht, schätzen Branchenexperten. Pharmakonzerne geben bis zu ein Drittel ihres Umsatzes für Marketing und Vertrieb aus – weitaus mehr, als es in der Automobil- oder Lebensmittelindustrie üblich ist. Je mehr die Unternehmen über die Patienten wissen, desto leichter lassen sich Wettbewerber vom Markt drängen. Die Daten verraten, wann und wo Leute über Sodbrennen, Haarausfall oder Magenkrämpfe klagen – und welche Gegenmittel man unters Volk bringen könnte. Die Informationen über Patientin Nummer 36288244, weitere Unterlagen sowie Gespräche mit ehemaligen und noch aktiven Mitarbeitern betroffener Unternehmen machen klar, wie das Geschäft läuft und wer davon profitiert.

Die Frau, die sich hinter Nummer 36288244 verbirgt, ist erst 19 Jahre alt. Ihr Einverständnis zur Weitergabe ihrer Daten hat sie nie gegeben, und sie weiß auch nicht, dass jemand damit Schindluder treibt. Und doch kann man ihre Unterlagen kaufen. Name und Adresse tauchen in den der ZEIT vorliegenden Dokumenten zwar nicht auf. "Aber die Unternehmen könnten durchaus über Methoden verfügen, die Anonymisierung zu entschlüsseln und die Person zu identifizieren", sagt

Zeit Online vom 31. Oktober 2013. Autorin: Anne Kunze. http://www.zeit.de/2013/45/patientendaten-marktforschung-pharmaindustrie/seite-2

Technisch-organisatorische Maßnahmen (TOM)

Was sind anonyme Daten entsprechend DS-GVO?

- Es gibt anonyme Daten (ErwGr. 26)
- Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten (=DS-GVO gilt nicht für anonyme Daten, ErwGr. 26)
- Was ist anonym? (ErwGr. 26)
  - Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen
    (von „Natur“ aus anonym)
  - Personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann
    (Verarbeitung „Anonymisierung“ durchgeführt)

Technisch-organisatorische Maßnahmen (TOM)

Verschlüsselung: Welche Algorithmen sollte man verwenden?

- Allgemein
  - BSI: Technische Richtlinie 02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen
    (https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html)
    - BSI TR-02102-1: Bewertung der Sicherheit ausgewählter kryptographischer Verfahren, ermöglicht längerfristige Auswahl geeigneter Verfahren
    - BSI TR-02102-2: Empfehlungen bzgl. Einsatz TLS
    - BSI TR-02102-3: Empfehlungen bzgl. Ipsec, und Internet Key Exchange
    - BSI TR-02102-4: Empfehlungen bzgl. SSH
- Erzeugung von Signaturschlüsseln, Hashen zu signierender Daten oder Erzeugung/Prüfung elektronischer Signaturen
  - Bundesnetzagentur: Auflistung geeigneter Algorithmen und Parameter
    - Jährliche Veröffentlichung im Bundesanzeiger
    - Online unter https://www.bundesnetzagentur.de/
      (https://www.bundesnetzagentur.de/DE/Service-Funktionen/ElektronischeVertrauensdienste/QES/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen_node.html)

Technisch-organisatorische Maßnahmen (TOM)

TOM: Vorgabe durch Art. 32 Abs. 1 lit. a DS-GVO

Diese Maßnahmen schließen gegebenenfalls 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

Technisch-organisatorische Maßnahmen (TOM)

Apropos Belastbarkeit

- Art. 32 (1d), dt.
  - die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit [...]
- Art. 32 (1d), engl.
  - the ability to ensure the ongoing confidentiality, integrity, availability and resilience [...}
- „Belastbarkeit“ = „resilience“
  - Übersetzung „resilience“ in dt. IT-Fachliteratur*: „Widerstandsfähigkeit“ oder „Ausfallsicherheit“

* Siehe z. B. Wagner SM, Bode C. Empirische Untersuchung von SC-Risiken und SC-Risikomanagement in Deutschland. In: Vahrenkamp/ Siepermann (Hrsg.) Risikomanagement in Supply Chains: Gefahren abwehren, Chancen nutzen, Erfolg generieren..Erich Schmidt Verlag. 2007 ISBN 978-3503100415

Technisch-organisatorische Maßnahmen (TOM)

Art. 32 Abs. 1 fordert...

- Maßnahmen u.a.
  - Pseudonymisierung
  - Verschlüsselung
- Fähigkeiten
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Belastbarkeit/Ausfallsicherheit
  - Wiederherstellbarkeit
  - Notfallmanagement
- Verfahren
  - Überprüfbarkeit
  - Bewertung
  - Evaluierung

Unter Berücksichtigung

→ Stand der Technik

→ Implementierungskosten

→ Art, Umfang, Umstände und Zwecke der Verarbeitung

→ Risiko der Verarbeitung

Technisch-organisatorische Maßnahmen (TOM)

TOM: Vorgabe durch Art. 32 Abs. 1 lit. a DS-GVO

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

Technisch-organisatorische Maßnahmen (TOM)

Ergänzend: § 22 Abs. 2 Ziff. 3,4 BDSG n.F

- Anforderung bzgl. organisatorischer Maß nahmen
  - Sensibilisierung der an Verarbeitungsvorgängen Beteiligten, z.B.
    - Schulungsmaßnahmen
    - Regelmäßige Informationen
      - Z.B. per E-Mail – Frage hat jede Reinigungskraft bei Ihnen eine Mailadresse?
      - Reinigung der Patientenzimmer – Kenntnisnahme der Patientenaufkleber auf Betten, OP-Programm; Verarbeitung halt
    - ...
- Pflicht zur Benennung einer oder eines Datenschutzbeauftragten
  - Bestärkung von Art. 37 Abs. 1 lit. a,c DS-GVO*
  - Ergänzende Anforderung bzgl. § 38 BDSG n.F. *

* Weichert T: § 22 BDSG Rn. 35 in Kühling/Buchner. DS-GVO · BDSG. Verlag C.H.Beck. ". Auflage, ISBN 978-3-406-71932-5

Technisch-organisatorische Maßnahmen (TOM)

Ergänzend: § 22 Abs. 2 Ziff. 3,4 BDSG n.F

- Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind
  - § 630f Abs. 1 BGB: „Der Behandelnde ist verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Dies ist auch für elektronisch geführte Patientenakten sicherzustellen.“

→ Vollständige Dokumentationshistorie gefordert!

- Umfassende Dokumentation der eingesetzten Verfahren erforderlich
- Protokollierung der konkreten Verarbeitungsmaßnahmen
- Vollprotokollierung aller Eingaben, Änderungen, Löschungen
- Löschfristen der Protokolldaten sind vorab an Hand einer Risikobewertung festzulegen, Mindestfrist für die Aufbewahrung von Protokolldaten: 1 Jahr*

* Weichert T: § 22 BDSG Rn. 33 in Kühling/Buchner. DS-GVO · BDSG. Verlag C.H.Beck. ". Auflage, ISBN 978-3-406-71932-5

Technisch-organisatorische Maßnahmen (TOM)

Ergänzend: § 22 Abs. 2 Ziff. 3,4 BDSG n.F

- Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern

→ Art. 32 DS-GVO fordert Vertraulichkeit

→ § 203 StGB:

- berufsmäßig tätigen Gehilfen, Vorbereitung auf den Beruf tätige Personen, sonstige Personen
- soweit dies für die Inanspruchnahme der Tätigkeit erforderlich ist

→ Worauf hat wer Zugang? Ggf. Berechtigungskonzepte sowie deren Umsetzung prüfen!

Technisch-organisatorische Maßnahmen (TOM)

Ergänzend: § 22 Abs. 2 Ziff. 3,4 BDSG n.F

- **spezifische** Verfahrensregelungen, die im Fall
  - einer Übermittlung oder
  - Verarbeitung für andere Zwecke

  die Einhaltung der Vorgaben des BDSG n.F. sowie der DS-GVO sicherstellen
- Übermittlung, z.B.
  - Externe Qualitätssicherung
  - Auditierung / Zertifizierung
- Verarbeitung andere Zwecke, z.B.
  - Interne Qualitätssicherung
  - Forschung
- Wie sehen bei Ihnen die spezifischen Verfahren aus?

  Beispiele*:
  - Protokollierung
  - Kontrolle/Evaluierung der Datensätze bzgl. Zweck, Berechtigung
  - Hinweis auf Zweckbindung bei den Weiter-Verarbeitern

* Weichert T: § 22 BDSG Rn. 41 in Kühling/Buchner. DS-GVO · BDSG. Verlag C.H.Beck. ". Auflage, ISBN 978-3-406-71932-5

Technisch-organisatorische Maßnahmen (TOM)

§ 22 BDSG n.F. und andere nationale Regelung: Was gilt wann?

- Spezifische nationale Regelungen können als lex specialis dem BDSG n.F. vorgehen
  - Beispiel: SGB X
- Voraussetzungen*
  a) Regelung ist an DS-GVO „angepasst
  b) Andere Regelung muss „spezifischer“ sein
    - Soweit lediglich Aussagen zur materiell-rechtlichen Zulässigkeit enthalten sind → § 22 Abs. 2 BDSG ist ergänzend anzuwenden
    - Werden bereichsspezifische Garantien geregelt, gehen diese dem §22 BDSG vor, verdrängen diese aber nicht

* Weichert T: § 22 BDSG Rn. 45 in Kühling/Buchner. DS-GVO · BDSG. Verlag C.H.Beck. ". Auflage, ISBN 978-3-406-71932-5

Checklisten: Haben sie noch eine Zukunft?

Checklisten

Es existieren viele Checklisten, z.B.

- Ergänzende Checklisten zum Muster-ADV-Vertrag für das Gesundheitswesen (https://gesundheitsdatenschutz.org/doku.php/adv-mustervertrag-2015)
- Checkliste GDD
  - GDD Ratgeber „Datenschutz-Prüfung von Rechenzentren“ (https://www.gdd.de/downloads/praxishilfen/GDD-Ratgeber_Datenschutz-Pruefung_von_Rechenzentren_2015.pdf)
  - Datenschutz im Unternehmen (https://www.gdd.de/downloads/praxishilfen/datenschutz-im-unternehmen-2)
- Checkliste Datenschutz-Wiki (https://www.datenschutz-wiki.de/Checkliste_TOM_Auftragskontrolle oder https://www.datenschutz-wiki.de/Checkliste_TOM_Verf%C3%BCgbarkeitskontrolle)
- Baustein B 1.5 Datenschutz BSI (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01005.html sowie Tabelle http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/ErgaenzendeDoks/MassnahmeGS-Kat.pdf?__blob=publicationFile)
- Anhang A der ISO 27001
- Checklisten der Aufsichtsbehörden
  - Bayern (https://www.inte.de/BayLDA.pdf)
  - Niedersachsen (http://www.lfd.niedersachsen.de/download/32309/Orientierungshilfe_Fremd-_und_Fernwartung_LfD_Niedersachsen_.pdf)
  - Orientierungshilfen der Aufsichtsbehörden, insbesondere
    - Orientierungshilfe Krankenhausinformationssysteme https://www.datenschutzzentrum.de/artikel/1107-OH-KIS-Orientierungshilfe-Krankenhausinformationssysteme.html)
- ...

Checklisten

Checklisten müssen „passen“

- Basieren meist auf den Anforderungen resultierend aus der Anlage zu § 9 S. 1 BDSG (resp. Anlage zu § 78a SGB X)
- DS-GVO verfolgt risikobasierten Ansatz, gibt (kaum) Maßnahmen vor
- Maßnahmen aus bisherigen TOMs werden nicht obsolet, müssen geprüft und ggf. angepasst werden
  - Erforderliche Maßnahmen, die durch eine Risikovalidierung identifiziert wurden und bisher nicht in der Checkliste enthalten sind
  - Erforderliche Maßnahmen, die in einer Checkliste enthalten sind und durch eine Risikovalidierung identifiziert wurden
  - Maßnahmen, die in einer Checkliste enthalten sind und nicht durch eine Risikovalidierung identifiziert wurden
- Erfahrungsgemäß werden Maßnahmen entsprechend „Einfachheit“ umgesetzt, nicht entsprechend Wichtigkeit
  - DS-GVO fordert Risikoadaptiertheit
  - Dementsprechend hier Umdenken erforderlich

Checklisten

Anforderung „persönliche“ Checkliste/Maßnahmenkatalog

Checkliste

- muss branchenspezifisch Risiken adressieren
  - (Banken haben andere Risiken als Arztpraxen),
- muss die identifizierten Risiken adressieren und
- sollte nur die Maßnahmen enthalten, die vom Verantwortlichen umsetzbar sind,
- muss für die Umsetzenden und Auditierenden gut dokumentiert sein.
- Abgebildet sein muss
  - Erforderlichkeit der Maßnahme
  - Reicht die Maßnahme zur Anforderungserfüllung aus
  - Ja/Nein der bisherigen Checklisten wohl nicht ausreichend zur Erfüllung der aus Art. 5 resultierenden Nachweispflicht

Checklisten

Reifegrad im Datenschutz: ISO/IEC 29190

- ISO/IEC 29190 „Modell zur Bestimmung des Reifegrades im Datenschutz“
- Definiert verschiedene Stufen der Tauglichkeit
  - Level 0: Unvollständiger Prozess
  - Level 1: Angewandter Prozess
  - Level 2: Managed Prozess
  - Level 3: Bewährter, alt-eingeführter Prozess
  - Level 4: Berechenbarer Prozess
  - Level 5: Neuerungen einführender Prozess
- Bewertung des Erreichens des angestrebten Ergebnisses
  - Nicht erreicht (0-15%)
  - Teilweise erreicht (>15 – 50%)
  - Weitestgehend erreicht (>50 – 85%)
  - Vollständig erreicht (>85 – 100%)

  Beachte: 100%ige Erreichbarkeit ist nicht gefordert, an 80-20-Regel denken

Checklisten

Kombination ISO/IEC 33020 mit IDO/IEC 29190

Table 1 — Applicability of process attributes to assessment of capability levels

Capability Level	Process performance process	Performance management process	Work product management process	Process definition process	Process deployment process	Quantitative analysis process	Quantitative control process	Process innovation process	Process innovation implementation
Level 0: Incomplete									
Level 1: Performed	X								
Level 2: Managed	X	X	X						
Level 3: Established	X	X	X	X	X				
Level 4: Predictable	X	X	X	X	X	X	X		
Level 5: Innovating	X	X	X	X	X	X	X	X	X

Checklisten

Branchenspezifische Maßnahmenliste

- Entsprechend ISO/IEC 29190 könnte ein Maßnahmenkatalog für das Gesundheitswesen zur Abbildung der TOMs erarbeitet werden
  - Wartung/Fernwartung
  - Verarbeitung von Patientendaten im KIS/LIS/PACS/...
  - Home-Office
- Katalog könnte z.B. im Anhang von Verhaltensregeln („Code of Conduct“) enthalten sein (Art. 40 DS-GVO)
- Verhaltensregeln können „Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten“ entwickeln
- „High Level“:
  - Mit einem XML-Modell, welches diese Kataloge abbildet, können geforderte Maßnahmen (seitens Verantwortlicher) und Reifegrad der Umsetzung (seitens Auftragsverarbeiter) automatisch ausgetauscht werden
- Adressaten zur Entwicklung könnten sein
  - DKG, bvitg, GDD, GMDS, ...
- Idealerweise onzipert als Verhaltensregeln i.S.v. Art. 40 DS-GVO