Verzeichnis der Verarbeitungstätigkeiten

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

Wer braucht ein „Verzeichnis der Verarbeitungstätigkeiten“?

Das Verzeichnis von Verarbeitungstätigkeiten muss aufgestellt werden, wenn

- das Unternehmen mindestens 250 Mitarbeiter hat

oder

- Daten mit Risiken für die Rechte und Freiheiten der betroffenen Personen verarbeitet werden

oder

- eine Verarbeitung **besonderer Datenkategorien** erfolgt

oder

- eine Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen durchgeführt wird

oder

- die Datenverarbeitung nicht nur gelegentlich erfolgt.

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

Wer ist verantwortlich?

- Verantwortlich für
  - die Erstellung bzw.
  - das Vorhandensein des Verzeichnisses sowie
  - der entsprechenden Aktualisierungen

  „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“
- Letztlich: Führung des Unternehmens / Organisation (Geschäftsführer, Vorstand, ...)
- Cave Auftragsverarbeitung:
  - Gilt für Verantwortlichen aber auch für Auftragsverarbeiter

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

Wozu dient dieses Verzeichnis?

- Primäres Ziel
  - Aufsichtsbehörde Möglichkeit bieten, „die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse“ kontrollieren zu können
- Sekundär: Arbeitshilfe für den Datenschutzbeauftragten
  - Übersicht der im Unternehmen eingesetzten Verarbeitungsvorgänge, bei denen personenbezogene Daten verarbeitet werden

→ Primäres Ziel verlangt, dass im Verzeichnis **alle Verfahren** geführt werden müssen

→ Umfasst neben den automatisierten Verarbeitungen auch **manuelle**

Art. 30: „Verzeichnis von Verarbeitungstätigkeiten“

Unterschiede zum Verfahrensverzeichnis nach BDSG a.F.

- DS-GVO kennt diese Einschränkungen des BDSG a.F. nicht!!!
- DS-GVO fordert in Art. 30, dass in dem Verzeichnis **alle** Verarbeitungstätigkeiten aufgeführt werden müssen
- BDSG: keine Sanktion für ein fehlendes Verfahrensverzeichnis
  - Nur eine fehlende Meldung entsprechend § 4d Abs. 1 BDSG konnte sanktioniert werden; Meldepflicht entfiel jedoch, wenn Datenschutzbeauftragter bestellt
- DS-GVO: Bußgeld vorhanden

Verzeichnis von Verarbeitungstätigkeiten

Inhalte

(Mindest-) Angaben

- Namen und Kontaktdaten des Verantwortlichen (Ggfs. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten)
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder *noch* offengelegt *werden*, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- Ggfs. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich Angabe des Drittlands oder der Organisation, sowie die Dokumentierung geeigneter Garantien
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Verantwortlicher: Überwiegend wie gehabt …

§ 4e BDSG	Art. 30 DS-GVO
– Name oder Firma der verantwortlichen Stelle – Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter – Anschrift der verantwortlichen Stelle	Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen
Die mit der Leitung der Datenverarbeitung beauftragten Personen,	Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten
Zweckbestimmungen der Datenerhebung, -verarbeitung oder –nutzung	Zwecke der Verarbeitung
Beschreibung der betroffenen Personengruppen	Beschreibung der Kategorien betroffener Personen
Beschreibung der Daten oder Datenkategorien	Beschreibung der Kategorien personenbezogener Daten
Empfänger oder Kategorien von Empfängern	Kategorien von Empfängern [...], einschließlich Empfänger in Drittländern oder internationalen Organisationen
Regelfristen für die Löschung der Daten	die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
Geplante Datenübermittlung in Drittstaaten	Kategorien von Empfängern [...], einschließlich Empfänger in Drittländern oder internationalen Organisationen
Allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind	eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gem. Art. 32

Auftragsverarbeiter: Neu – eigenständige Dokumentation

§ 4e BDSG	Art. 30 DS-GVO
	den Namen und die Kontaktdaten des Auftragsverarbeiters, sowie gegebenenfalls des Vertreters des Auftragsverarbeiters
	den Namen und die Kontaktdaten eines jeden Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen
	den Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten des Auftragsverarbeiters und des Verantwortlichen
	Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
	gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
	eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32

Rahmenbedingungen

Begriffsbestimmungen

- Tätigkeit
  - Begriff „Tätigkeit“ in DS-GVO nicht definiert
- Verantwortlicher
  - Definition in Art. 4 Abs. 7 DS-GVO
- Zweck
  - Begrifflichkeit in DS-GVO nicht definiert
  - Umgang mit Zweck aber in Kommentaren dargelegt (z.B. Simitis)
- Verletzung des Schutzes personenbezogener Daten
  - Definition in Art. 4 Abs. 12 DS-GVO
- Stand der Technik
  - In DS-GVO nicht definiert
  - Siehe z. B. § 3 Abs. 6 Bundes-Immissionsschutzgesetz, IT-Sicherheitsgesetz

Rahmenbedingungen

Form des Verzeichnisses

- Es existiert genau ein Verzeichnis, in dem alle Verarbeitungstätigkeiten für jeden
- Verantwortlichen (Art. 30 Abs. 1 DS-GVO) bzw. Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO)

  („Jeder Verantwortliche und gegebenenfalls sein Vertreter führen *ein* Verzeichnis [...]“)
- Das genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. (Art. 30 Abs. 3 DS-GVO)
- Auf Anfrage muss der Verantwortliche bzw. der Auftragsverarbeiter der Aufsichtsbehörde das Verzeichnis zur Verfügung stellen (Art. 30 Abs. 4 DS-GVO)
- Eine Verfügbarmachung für Jedermann ist nicht vorgesehen
- (Aber natürlich auch nicht verboten)

Rahmenbedingungen

Sanktionen: Art. 83 Abs. 4 lit. a DS-GVO

Bei Verstößen gegen die Pflicht:

- Geldbußen von bis zu 10.000.000 EUR oder
- im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs
- je nachdem, welcher der Beträge höher ist

Merke: Einen Verstoß kann auch ein

- unvollständiges Verzeichnis
- fehlerhaft geführtes Verzeichnis
- nicht aktuelles Verzeichnis

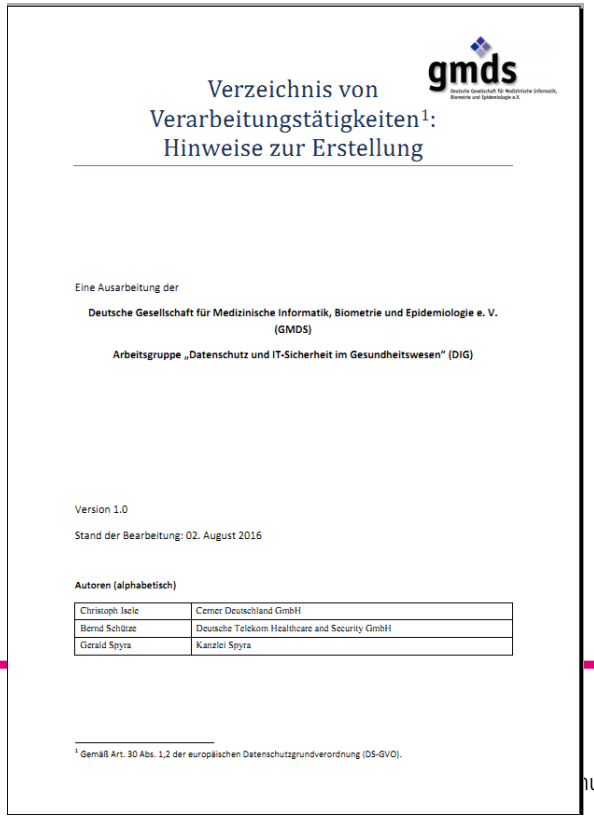
darstellen.

Hinweis: Ausarbeitung der GMDS

gmds
Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

EU DS-GVO: Verzeichnis von Verarbeitungstätigkeiten: Hinweise zur Erstellung

- Ausarbeitung online verfügbar (https://gesundheitsdatenschutz.org/doku.php/arbeitshilfe_ds-gvo_2016)
- Abschnitt Hinweise zur Umsetzung
  - Übergangsregelung
  - Unterschiede BDSG/DS-GVO
  - Erläuterung Begrifflichkeiten
  - ...
- Abschnitt (Mindest-) Anforderungen zur Dokumentation
  - Für den Verantwortlichen
  - Für den Auftragsverarbeiter



gmds

Verzeichnis von Verarbeitungstätigkeiten[1]: Hinweise zur Erstellung

Eine Ausarbeitung der

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG)

Version 1.0

Stand der Bearbeitung: 02. August 2016

Autoren (alphabetisch)

Christoph Isele	Cerner Deutschland GmbH
Bernd Schütze	Deutsche Telekom Healthcare and Security GmbH
Gerald Spyra	Kanzlei Spyra

[1] Gemäß Art. 30 Abs. 1,2 der europäischen Datenschutzgrundverordnung (DS-GVO).

Was könnte eine relevante Verarbeitungstätigkeit darstellen?

Mögliche Beispiele im Krankenhaus

Personaldaten

- Stammdatenverwaltung
- Zeiterfassung
- Urlaubsplanung
- Lohn-/Gehaltsabrechnung
- Weiterbildung (Anträge, Bewilligungen, ...)
- Dokumentation Mitarbeitergespräche
- Bewerbungsverfahren
- ...

Cave: auch manuelle Personalakten

Patientendaten

- Administrative Daten
- Tumordokumentation
- Fachdokumentation, z.B. OP-Dokumentation
- „Entertainment“
  (z. B.. Abrechnung Fernsehen, Telefonie, WLAN)
- Studien
- ...

Cave: auch manuelle Patientenakten

Beispiel: Benutzerverwaltung

Fazit

Was ist zu tun?

- Verfahrensverzeichnis als Ausgang für Überarbeitung nutzen
- Angaben Verfahrensverzeichnis entsprechend Anforderungen DS-GVO ergänzen
- Tätigkeiten, die bisher im Verfahrensverzeichnis nicht dokumentiert werden mussten, erfassen und dokumentieren
- Auftragsverarbeiter ggfs. wegen erforderlicher Zuarbeit ansprechen
- Auftragsverarbeiter ansprechen und auf eigene Dokumentationspflicht hinweisen
- Sanktionen können empfindlich sein