Workshop 4: Europäische Datenschutzgrundverordnung - Konsequenzen für die Informationsverarbeitung im deutschen Gesundheitswesen

Christoph Isele

Cerner Deutschland

Berlin, 18. April 2016; conhIT-Satellitenveranstaltung "Datenschutz und IT-Sicherheit im Gesundheitswesen (DIG)"

Datenverarbeitung Teil 2

- … aus Sicht einer Einrichtung im Gesundheitswesen

- Für die Verarbeitung Verantwortliche
- Auftragsverarbeiter
- Übermittlung personenbezogener Daten an Drittländer

DS GVO generell

- Datenverarbeitungsbegriff moderner als bei BDSG
  - Mehr organisatorische Varianten
  - Starke Trennung von Regelungen für Behörden und für eigene Zwecke aufgehoben
- Stärkung der Rechte der Betroffenen / Bürger
  - Mehr Transparenz und mehr Nachweise
- Konsolidierungsphase für die Interpretation/Auslegung der Gesetze

Rechtmäßigkeit der Verarbeitung (Art. 6)

- Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen ;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt ;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen ;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde ;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt .

Einwilligung (Art 7)

- Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
- … schriftliche Erklärung … muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. …
- … Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

- ? Löschen der Daten

- Bei Kindern auch Einwilligung der Eltern

Für die Verarbeitung Verantwortlicher

- Der Verantwortliche ist für die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten verantwortlich und muss dessen Einhaltung nachweisen können (Art 5(2) "Rechenschaftspflicht").
  - "Unternehmensgruppe" eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht
  - Hauptniederlassung, Niederlassungen
  - Gemeinsam für die Verarbeitung Verantwortliche — Art 24
  - Auftragsverarbeiter — Art 28
    a) *Weitere Auftragsverarbeiter*
  - Auftragsverarbeiter im Drittland — Art 40 ff

Unternehmensgruppe - Konzern

- Art 4 (19)
  "Unternehmensgruppe" eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;
- Erwägungsgrund (37):
  Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. …
- Erwägungsgrund (47) → Art 6 (1) f
- Erwägungsgrund (48)
  … Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.

Pflichten des Verantwortlichen

- Art 24
  Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen **um**, um sicherzustellen und den Nachweis dafür erbringen zu können, **dass die Verarbeitung gemäß dieser Verordnung erfolgt.**
  - Anlage zu §9 Absatz 1 gibt es nicht mehr
  - Verpflichtung auf Datengeheimnis (BDSG §5) steht so nicht in der GVO
  - Siehe Art 40 Verhaltensregeln

- Art 25
  Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
  - Stand der Technik
  - Datenminimierung

Pflichten des Verantwortlichen

- Verzeichnis von Verarbeitungstätigkeiten
  - *a) Kontaktdaten des Verantwortlichen*
  - *b) Zwecke der Verarbeitung*
  - *c) Kategorien betroffener Personen und Kategorien betroffener Daten*
  - *d) Kategorien von Empfängern (auch Drittland)*
  - *e) Übermittlung personenbezogener Daten in ein Drittland*
  - *f) Fristen für die Löschung*
  - *g) Technische und organisatorische Maßnahmen*

- Ersetzt die Meldepflicht im BDSG; dort zunächst nur an den DSB
- Kein öffentliches Verfahrensverzeichnis mehr, aber auf Verlangen der Aufsichtsbehörde zu zeigen
- Auch bei Auftragsverarbeitern obligatorisch
- Befreiung für Unternehmen bis 250 Mitarbeiter
  Befreiung gilt nicht bei Gesundheitsdaten

Meldung, Benachrichtigung bei Verletzung des Schutzes

- Meldung an die Aufsichtsbehörde **innerhalb von 72 Stunden** wenn nicht möglich Begründung für die Verzögerung
- Auch der Auftragsverarbeiter meldet unverzüglich Vorfälle an den Verantwortlichen

- Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.
- Benachrichtigung der betroffenen Person … ist nicht erforderlich, wenn :
  - der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat
  - das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen besteht aller Wahrscheinlichkeit nach nicht mehr
  - dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung …

Datenschutz-Folgenabschätzung (Art 35)

- Die Folgenabschätzung enthält zumindest Folgendes:
  - a) *eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;*
  - b) *eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;*
  - c) *eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und*
  - d) *die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, …*
- Konsultation der Aufsichtsbehörde bei einem hohen Risiko
- Bei Zwecken öffentlicher Gesundheit kann der Verantwortliche durch nationales Recht verpflichtet werden die Aufsichtsbehörde zu konsultieren
- **Aufsichtsbehörde muss innerhalb von 8 bis 14 Wochen antworten**
- Listen durch die Aufsichtsbehörden für Vorgänge, bei denen immer / nie eine Folgenabschätzung durchzuführen ist.

Verhaltensregeln (Art 40)

- Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern die Ausarbeitung von Verhaltensregeln, …
- Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten oder ändern oder erweitern, mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird
    - *a) faire und transparente Verarbeitung;*
    - *b) die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen;*
    - *c) Erhebung personenbezogener Daten;*
    - *d) Pseudonymisierung personenbezogener Daten;*
    - *e) Unterrichtung der Öffentlichkeit und der betroffenen Personen;*
    - *f) Ausübung der Rechte betroffener Personen;*
    - *g) …*
    - *h) die Maßnahmen und Verfahren gemäß den Artikeln 24 und 25 und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32;*
    - *i) …*

Mehrere Einrichtungen sind beteiligt

Gemeinsam für die Verarbeitung Verantwortliche (Art 26)

- Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, …
- …
- Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.

Auftragsverarbeiter (Art 28)

- 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.
- Vertragliche Vereinbarung
- Schriftliche Genehmigung von Unterauftragnehmern
- personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten
- Befugte Personen zur Vertraulichkeit verpflichten
- Alle erforderliche Maßnahmen zur IT Sicherheit ergreifen (Art 32)

Auftragsverarbeiter (Art 28)

- Mitwirkung bei Pflichten des Auftraggebers gegenüber Aufsichtsbehörde und Betroffenen
- Löschen der Daten nach Abschluss

- Art 28 (5) – Zukunft ?
  - Einhalten der Verhaltensregeln oder Zertifikat, die für die übergeordnete Verarbeitung gelten

- Art 28 (10) – quasi als Verneinung von Art 28 (3) a
  - Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Übermittlung personenbezogener Daten an Drittländer

- Alle Bestimmungen der Artikel 44 bis 50 sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.
- Auf der Grundlage eines Angemessenheitsbeschlusses (Art 45)
- Vorbehaltlich geeigneter Garantien (Art 46)
  - Standarddatenschutzklauseln
  - Entsprechende genehmigte Verhaltensregeln
  - Entsprechende genehmigte Zertifizierungen
- Verbindliche interne Datenschutzvorschriften - durch die zuständige Aufsichtsbehörde genehmigt (Art 47)

- Ausnahmen für bestimmte Fälle in denen eine Übermittlung zulässig ist
  - vergleichbar den Rechtmäßigkeiten der Verarbeitung in Artikel 6 Einwilligung, Erfüllung des Vertrags, im Interesse der betroffenen Person, öffentliches Interesse, Verteidigung von Rechtsansprüchen ...

Vergleich zum BDSG

- Die explizite Charakterisierung von Wartung als Auftragsdatenverarbeitung entfällt

- Die Einrichtung automatischer Abrufverfahren ist nicht mehr gesondert geregelt

„Datenverarbeitung im Auftrag“

- Die Regelungen der DS-GVO für Auftragsverarbeiter überschneiden sich inhaltlich weitgehend mit den bekannten Bestimmungen des BDSG § 11. Die Unternehmen werden also nicht mit völlig neuen Regelungen konfrontiert.
- Für Auftragsverarbeiter bringt die DS-GVO dennoch einige Neuerungen. Das betrifft insbesondere die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten, eine umfangreichere Dokumentation sowie die veränderten Haftungsregelungen.
- Für die Verarbeitung Verantwortliche und Auftragsverarbeiter sollten also, ihr Datenschutzmanagement internen überprüfen und sich rechtzeitig auf die neuen Regeln einstellen.

Fragen ?
Kommentare
Anmerkungen

Kontakt

Christoph Isele
Cerner Deutschland

Tel: +49 (173) 2385940
Mail: Christoph.Isele@cerner.com