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

Auftrags(daten)verarbeitung

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

Auftragsdatenverarbeitung

- Möglichkeit, Dienstleister mit Datenverarbeitung zu beauftragen, ohne eine Übermittlungsbefugnis zu benötigen
- Interessant angesichts beschränkter Erlaubnistatbestände bei Gesundheitsdaten
- Aufwändige Vertragsgestaltung
- Hürde der Offenbarungsbefugnis bei Berufsgeheimnissen

Agenda

- Rechtlicher Rahmen durch die DS-GVO
  - Merkmale, was ist anders?
- Auftragsdatenverarbeitung
  - Abgrenzung Funktionsübertragung
  - ADV-Vertrag
  - Vertragsbestandteile
- Einfluss nationalen Rechts auf die Auftragsverarbeitung
  - § 203 StGB (?)
  - Krankenhausgesetze
  - SGB X
- Vorstellung Muster-AV-Vertrag

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

Rechtlicher Rahmen

Begriffsbestimmungen

- **Verantwortlicher**: Natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung entscheidet (Art. 4 Ziff. 7)
- **Auftragsverarbeiter**: Natürliche oder juristische Person, die pb Daten im Auftrag des Verantwortlichen verarbeitet (Art. 4 Ziff. 8)
- **Auftragsverarbeitung**: Tätigkeit des Auftragsverarbeiters für den Verantwortlichen

Grundsätzliches

AV als Rechtskonstrukt geregelt im **Art. 28 DS-GVO**

2 Kategorien von Regelungen:

1. Regelungen, die im Vertrag zu fixieren sind (Art. 28 Abs. 3)
2. Regelungen, die kraft GVO unmittelbar gelten (und nicht im Vertrag auftauchen *müssen*)

Privilegierung der AV?

Dafür spricht:

- Auftragsverarbeiter gemäß Art. 4 Nr. 10 DS-GVO kein „Dritter“ - also der Sphäre des Verantwortlichen (nicht der der betroffenen Person) zuzurechnen
- Keine gesonderte Zulässigkeitsvoraussetzung für die Auftragsverarbeitung
- Regelung der Verantwortlichkeiten lässt die Existenz eines eigenen Schutzbedarfs nicht plausibel erscheinen

… oder doch nicht?

Ggf. könnte die Zulässigkeit regelmäßig im Rahmen der Interessenabwägung als gegeben anzusehen sein. (*Regelmäßigkeit = „Privilegierung“*)

- Problematisch, da für besondere Daten eine Interessenabwägung nicht vorgesehen ist und eine AV demnach dort nicht anwendbar wäre

„Funktionsübertragung“

Bezeichnung für Beauftragungen, die keine Auftrags(daten)verarbeitungen sind:

- Wenn Zwecke und Mittel der Verarbeitung nicht vollständig in der Entscheidungsgewalt des beauftragenden Verantwortlichen liegen
- Nicht privilegiert
- Übermittlung/Offenlegung mit Erfordernis der rechtlichen Legitimation

Exkurs: Gemeinsam für die Verarbeitung Verantwortliche

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

- Gemeinsame Festlegung von Zwecken und Mitteln der Verarbeitung gem. Art. 26
- Vereinbarung zur Festlegung der Pflichtenaufteilung
- Pflichtenaufteilung den Betroffenen zur Verfügung zu stellen
- Geltendmachung von Rechten gegenüber jedem Verantwortlichen

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

Auftragsverarbeitung

Vertrag

„… auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten…“ (Art. 28 Abs. 3 Satz 1)

- schriftlich, auch elektronisch möglich (Art. 28 Abs. 9)
- Die Kommission oder eine Aufsichtsbehörde (Kohärenzverfahren) kann Standardvertragsklauseln festlegen

Vertragsinhalte

Zu regelnde Inhalte gem. Art 28 Abs. 3, ggü. dem § 11 BDSG *beibehalten*:

- ✓ Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen (Art. 28 Abs. 3 Satz 1)
- ✓ Weisungsgebundenheit (Art. 28 Abs. 3 lit. a) - *vorbehaltlich…*
- ✓ Löschung oder Rückgabe der personenbezogenen Daten an den Verantwortlichen (Art. 28 Abs. 3 lit. g) - *vorbehaltlich…*

Vertragsinhalte II

Zu regelnde Inhalte, ggü. dem § 11 BDSG *verändert/spezifiziert*:

- ✓ *Vertraulichkeits*verpflichtung der Personen beim Auftragsverarbeiter (Art. 28 Abs. 3 lit. b)
- ✓ Auftragsverarbeiter muss erforderliche TOM gemäß Art. 32 ergreifen (Art. 28 Abs. 3 lit. c)
- ✓ Keine Unterauftragnehmer ohne vorherige Genehmigung sowie Übertragung der Datenschutzpflichten des Auftragsverarbeiters (Art. 28 Abs. 3 lit. d)

Vertragsinhalte III

Zu regelnde Inhalte, ggü. dem § 11 BDSG *verändert/spezifiziert* (Forts.):

- ✓ Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei
  - der Gewährung von Betroffenenrechten mit geeigneten TOM (Art. 28 Abs. 3 lit. e)
  - der Erfüllung der Pflichten zur Gewährleistung der Sicherheit personenbezogener Daten und zur Datenschutz-Folgenabschätzung und zur vorherigen Konsultation (Art. 28 Abs. 3 lit. f)
  - der Erfüllung der Rechenschaftspflichten beim Nachweis der Einhaltung aller Verpflichtungen aus dem Art. 28 einschließlich Ermöglichung und Unterstützung von Prüfungen (Art. 28 Abs. 3 lit. h)

(Fern)Wartung

- Keine gesonderte Erwähnung im Kontext der AV
- Bei Relevanz für personenbezogene Daten als AV anzusehen:
  - Keine eigenen Zwecke des Dienstleisters
  - Keine Festlegung der Mittel (?) - Fiktion

Besondere Pflichten des Verantwortlichen I

- ✓ Benennung eines Vertreters in der Union, bei Niederlassung außerhalb (Art. 27)
- ✓ Ordnungsgemäßer Vertragsschluss gemäß Art. 28 Abs. 3
- ✓ neuerdings Beachtung der Drittlandproblematik innerhalb der AV

Besondere Pflichten des Verantwortlichen II

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

- ✓ Kontrollen des Auftragsverarbeiters sind angesichts der Rechenschaftspflichten unverzichtbar - „hinreichende Garantien“ (Art. 28 Abs. 1)
  - ➢ Duldungs- und Mitwirkungspflicht des Auftragsverarbeiters ist gegeben (Art. 28 Abs. 3 lit. h)
  - ➢ Insbesondere genehmigte Verhaltensregeln nach Art. 40 bzw. Zertifizierungen nach Art. 42 können herangezogen werden, um hinreichende Garantien des Art. 28 Abs. 1 u. 4 nachzuweisen (Art. 28 Abs. 5)

Besondere Pflichten des Auftragsverarbeiters I

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

- ✓ Benennung eines Vertreters in der Union, bei Niederlassung außerhalb (Art. 27)
- ✓ Hinweispflicht des Verarbeiters bei vermuteter Rechtswidrigkeit der Verarbeitung (Art. 28 Abs. 3 Satz 3)
- ✓ Gewährleistung, dass Beschäftigte nur nach Weisung des Verantwortlichen verarbeiten (Art. 29, Art. 32 Abs. 4)
- ✓ Führung eines Verzeichnisses der Verarbeitungstätigkeiten (mit Tätigkeiten für den Verantwortlichen) (Art. 30 Abs. 2 - 4)

Besondere Pflichten des Auftragsverarbeiters II

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

- ✓ Zusammenarbeit mit der Aufsichtsbehörde (Art. 31)
- ✓ Unverzügliche Meldung der Verletzung des Schutzes pb Daten an den Verantwortlichen (Art. 33 Abs. 2)
- ✓ Beachtung der Regelungen zum Datenschutzbeauftragten (Artt. 37 - 39)
- ✓ Beachtung Drittland-Auflagen (Artt. 44 - 50)
- ✓ Würdigung der Haftungsregelungen für Schadenersatz (Art. 82, insb. Abs. 4)

Stellung des Auftragsverarbeiters I

Auftragsverarbeiter unterliegt nun weitergehend dem Datenschutzrecht (nach wie vor nicht vollständig, nur wo ausdrücklich erwähnt)

- Pflichten aus den Artt. 25-43 (Kapitel IV „Verantwortliche und Auftragsverarbeiter“)
- Sanktionskatalog
- Gemeinsame Haftung gegenüber den betroffenen Personen

Ansonsten weisungsgebunden (Art. 28 Abs. 3 lit. a sowie Art. 29)

Stellung des Auftragsverarbeiters II

- Auftragsverarbeiter wird zum Verantwortlichen, sobald er Zwecke und Mittel rechtsverstößlich selbst bestimmt (Art. 28 Abs. 10)
- Neubewertung der betriebswirtschaftlichen Risiken für Auftragsverarbeiter

Drittlandverarbeitung

Neu: AV auch mit Drittlandsitz des Auftragsverarbeiters möglich zu berücksichtigen:

- Benennung Vertreter in der EU (Art. 27)
- Drittlandregeln (s. folgenden Vortrag)
  - Angemessenheitsbeschluss
  - Geeignete Garantien

Sanktionierung bei Verordnungsverstößen

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

Für Verantwortlichen und Auftragsverarbeiter gleichermaßen wirksam, für letzteren jedoch nur in Bezug auf die „Pflichtenzuteilung“ der DS-GVO (Art. 83 Abs. 4 lit. a)

Für Auftragsverarbeiter insbesondere einschlägig:

- Artt. 25 - 39 (Allgemeine Pflichten, Sicherheit personenbezogener Daten, Datenschutz-Folgenabschätzung und vorherige Konsultation, Datenschutzbeauftragter)

Umstellungserfordernisse I

Bei Altverträgen:

- BDSG-Vertragsmuster gehen bereits teilweise über die Anforderungen des § 11 hinaus
- Soll-Ist-Analyse (Checkliste) und konsentierte Nachbesserung, *aber:* individuelle Nachbesserung meist nicht sinnvoll, da Rechtsrahmen (für den Auftragsverarbeiter) nicht vergleichbar
- Zeitbedarf für Umstellungsprozess berücksichtigen

Umstellungserfordernisse II

Bei (künftigen) Neuverträgen:

- Anerkannte Vertragsmuster verwenden (z.B. von GDD, BITKOM etc.)
- Auf (anfänglich) waghalsige DS-GVO-Interpretationen des Vertragspartners achten

Zwischenzeitlich Verträge, die beiden Regelungen genügen???

- ➢ Mit Übergangsklauseln denkbar
- ➢ Anwendbarkeit der Auftragsverarbeitung grundsätzlich wie bisher

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

Einfluss nationalen Rechts

Einflussmöglichkeiten

Art. 28 DS-GVO

- sieht keine Ausgestaltungsmöglichkeiten („Öffnungsklauseln“) für die Gesetzgeber vor,
- ist damit abschließend geregelt.
- Höchstens spezialgesetzliche Bedingungen für die Anwendbarkeit sind denkbar
  - Berufsgeheimnisse
  - Sozialrecht

Berufsgeheimnisse? I

Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen:

- Ausweitung des Berufsgeheimnisses auf „bei der Berufsausübung mitwirkende Dritte“
- Zugleich Offenbarungsbefugnis gegenüber diesen Dritten, soweit erforderlich

Berufsgeheimnisse? II

Bisher gilt:

- Auftragsdatenverarbeitung keine Offenbarungsbefugnis gegenüber dem Dienstleister

- Offenbarung ist zu vermeiden

- Seitens der DS-GVO keine Anhaltspunkte für eine andere Betrachtung

Berufsgeheimnisse? III

Künftig gilt:

- Offenbarung bei Auftragsverarbeitung innerhalb des § 203 StGB erlaubt; Auftragsverarbeiter = mitwirkende Person(en)
- Erfordernis einer Schweigepflichtentbindungserklärung?
  - ➢ Eher nein
  - ➢ Art. 13/14 ist besonders ernst zu nehmen

Restrisiko nach § 203-Reform

Umstritten, inwieweit folgende Regelungen einer Offenbarung innerhalb einer AV entgegenstehen:

- Heilberufliche Berufsordnungen
- Landeskrankenhausgesetze

(in unterschiedlichem Maße)

Exkurs: § 80 SGB X

Auftragsverarbeitung von Sozialdaten:

- von der DS-GVO abweichende Regelungen des § 80 SGB X sind entfallen
- zusätzliche Auflagen:
  - Mitteilungspflicht gegenüber Rechts- oder Fachaufsicht
  - Keine Vergabe in unsichere Drittländer
  - zus. Bedingungen für nicht-öffentliche Auftraggeber (gilt gem. Abs. 5 nicht für Wartungsverträge)

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

Vorstellung Muster-AV-Vertrag

Mustervertrag für das Gesundheitswesen

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

Gemeinsame Ausarbeitung der zuständigen Facharbeitskreise von

- Berufsverband der Datenschutzbeauftragten Deutschlands e. V. - **BvD**
- Bundesverband Gesundheits-IT e. V. - **bvitg**
- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. - **gmds**
- Gesellschaft für Datenschutz und Datensicherheit e. V. - **GDD**

sowie der

- Deutschen Krankenhausgesellschaft e. V. - **DKG**

Mustervertrag für das Gesundheitswesen II

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

Mustervertrag besteht aus:

- ✓ Auftragsverarbeitungs-Vertrag mit
  - ✓ alternativen und optionalen Klauseln, um für möglichst viele Situationen anwendbar zu sein
  - ✓ Kommentierung zur Herleitung und Begründung der Regelungen
  - ✓ Zahlreichen Literaturhinweisen
  - ✓ Anlagenmuster (Unterauftragnehmerliste, TOMs)
  - ✓ Beispiel für eine Verpflichtungserklärung von Beschäftigten
- ✓ Begleitende Ausarbeitung mit Hinweisen zum Umgang mit bestehenden Altverträgen

http://ds-gvo.gesundheitsdatenschutz.org/html/index.php

Diskussion

Quelle: pixabay.com