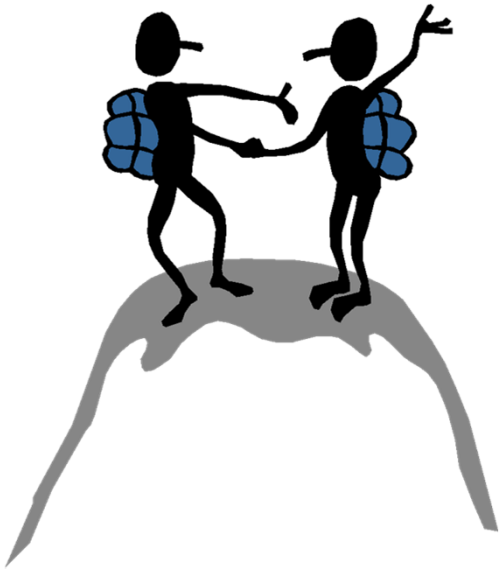

Muster-Auftragsdatenverarbeitungsvertrag
Eine AG von bvitg, BvD, GDD und GMDS

Dr. Bernd Schütze

BvD Verbandstag, 12. Mai 2015

Dr. Bernd Schütze

- Studium
  - > Studium Informatik (FH-Dortmund)
  - > Studium Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
  - > Studium Jura (Fern-Uni Hagen)
- Zusatz-Ausbildung
  - > Zusatzausbildung Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
  - > Zusatzausbildung Datenschutz-Auditor (TüV Süd)
  - > Zusatzausbildung Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)
- Berufserfahrung
  - > 10 Jahre klinische Erfahrung
  - > 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.

Warum einen weiteren „Muster-ADV-Vertrag“?

Es gibt Vorlagen von

- GDD (Stand 2009-10-14)
- **Aber keiner dieser Muster-Verträge geht auf die Besonderheiten ein, die wir in der Arztpraxis oder im Krankenhaus brauchen (von Forschung ganz zu schweigen)**
- LDI Bremen (Stand 2012-01-25)
- Bitkom (Stand 2014-01-09)
- …

Welche Besonderheiten brauchen wir denn?

1. Sozialdaten

Sozialdaten?

Legaldefinition „Sozialdaten“§67 Abs. 1 SGB X

- „…Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch

- **Arztpraxen, Apotheken und Krankenhäuser unterliegen damit nicht *grundsätzlich* dem Sozialdatenschutz**

  - Gemeindebehörden,
  - anerkannte Adoptionsvermittlungsstellen nach §2 Abs. 2 des Adoptionsvermittlungsgesetzes sowie
  - die Stellen, welche Aufgaben nach §67c Abs. 3 SGB X wahrnehmen

Sozialdaten?

ABER es gibt andere Auffassungen:

1. Erhebung beim Leistungserbringer
   - Entsprechend §67a Abs. 2 können Sozialdaten direkt beim Leistungserbringer erhoben werden.
   - Damit können Krankenhäuser/Arztpraxen Sozialdaten z.B. für eine Krankenkasse erheben.
   - Aus §67c SGB X in Verbindung mit §284 SGB V leiten einige Kassen ab, dass beim Leistungserbringer gespeicherte Patientendaten zugleich gespeicherte (i.S. von archivierten) Sozialdaten darstellen.
2. OVG Münster: Weitergabe personenbezogener Daten (Beschluss vom 20.07.1989; AZ - 18 B 613/89)
   - Personenbezogene Daten (§ 35I SGB I), die zur Erlangung von Sozialleistungen offenbart worden sind, dürfen … unter den Voraussetzungen der §§ 67 ff. SGB X verarbeitet werden
   - Erhalten Arztpraxen/Krankenhäuser „personenbezogene Daten zur Erlangung von Sozialleistungen“ bei Kostenübernahmeerklärungen durch Krankenkassen?

Folgt man diesen (und ähnlichen) Argumentation, so gelten die ADV-Vorschriften des SGB X, bzgl. ADV also §80 SGB X.

Sozialdaten?

Aber §80 SGB X entspricht doch §11 BDSG? Fast:

– Auswahl des Auftragnehmers

- §11 Abs. 2 BDSG:
  „Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen **sorgfältig auszuwählen**. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind…“
- §80 Abs. 2 SGB X:
  „Eine Auftragserteilung für die Erhebung, Verarbeitung oder Nutzung von Sozialdaten **ist nur zulässig, wenn der Datenschutz beim Auftragnehmer** nach der Art der zu erhebenden, zu verarbeitenden oder zu nutzenden Daten **den Anforderungen genügt, die für den Auftraggeber gelten**. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind…“

Sozialdaten?

§80 Aber SGB X entspricht doch §11 BDSG? Fast:

– Weitergehende Vorschriften für Auftraggeber und Auftragnehmers, z.B. Weisung/Kontrolle
  - BDSG und SGB beide gemeinsam Abs. 2 Ziff. 7

Anforderungen des §80 SGB X deutlich „härter“ als die Anforderungen des §11 BDSG
Und: Anzeigepflicht bei der Aufsichtsbehörde entsprechend §80 Abs. 3 SGB X

a) Auskünfte bei ihm einzuholen,
b) während der Betriebs- oder Geschäftszeiten seine Grundstücke oder Geschäftsräume zu betreten und dort Besichtigungen und Prüfungen vorzunehmen und
c) geschäftliche Unterlagen sowie die gespeicherten Sozialdaten und Datenverarbeitungsprogramme einzusehen

Welche Besonderheiten brauchen wir denn?

1. Sozialdaten
2. Umgang mit §203 StGB

Umgang mit §203 StGB

Wir brauchen:

- Klarstellung, dass Datenschutz und Schweigepflicht auf unterschiedlichen Gesetzgebungen beruhen
- Klarstellung, dass ADV nicht die §203-Frage lösen kann
- Klarstellung, dass §203 StGB gemäß §205 Abs. 1 StGB ein Antragsdelikt ist, wobei den Antrag gemäß nur der Verletzte (bzw. der gesetzliche Vertreter oder im Todesfall der Erbe) stellen kann
- D.h.: eine Datenschutz-Aufsichtsbehörde darf Straftaten gemäß §203 StGB nicht verfolgen und auch nicht sanktionieren

§ 205 Strafantrag

(1) In den Fällen des § 201 Abs. 1 und 2 und der §§ 201a, 202, 203 und 204 wird die Tat nur auf Antrag verfolgt. Dies gilt auch in den Fällen der §§ 202a und 202b, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.
(2) Stirbt der Verletzte, so geht das Antragsrecht nach § 77 Abs. 2 auf die Angehörigen über; dies gilt nicht in den Fällen der §§ 202a und 202b. Gehört das Geheimnis nicht zum persönlichen Lebensbereich des Verletzten, so geht das Antragsrecht bei Straftaten nach den §§ 203 und 204 auf die Erben über. Offenbart oder verwertet der Täter in den Fällen der §§ 203 und 204 das Geheimnis nach dem Tod des Betroffenen, so gelten die Sätze 1 und 2 sinngemäß.

§ 77 Antragsberechtigte

(1) Ist die Tat nur auf Antrag verfolgbar, so kann, soweit das Gesetz nichts anderes bestimmt, der Verletzte den Antrag stellen.
(2) Stirbt der Verletzte, so geht sein Antragsrecht in den Fällen, die das Gesetz bestimmt, auf den Ehegatten, den Lebenspartner und die Kinder über. Hat der Verletzte weder einen Ehegatten, oder einen Lebenspartner noch Kinder hinterlassen oder sind sie vor Ablauf der Antragsfrist gestorben, so geht das Antragsrecht auf die Eltern und, wenn auch sie vor Ablauf der Antragsfrist gestorben sind, auf die Geschwister und die Enkel über. Ist ein Angehöriger an der Tat beteiligt oder ist seine Verwandtschaft erloschen, so scheidet er bei dem Übergang des Antragsrechts aus. Das Antragsrecht geht nicht über, wenn die Verfolgung dem erklärten Willen des Verletzten widerspricht.
(3) Ist der Antragsberechtigte geschäftsunfähig oder beschränkt geschäftsfähig, so können der gesetzliche Vertreter in den persönlichen Angelegenheiten und derjenige, dem die Sorge für die Person des Antragsberechtigten zusteht, den Antrag stellen.
(4) Sind mehrere antragsberechtigt, so kann jeder den Antrag selbständig stellen.

§203 StGB:
Also nur ein theoretisches Hindernis?

- Stimmt, so gut wie keine Urteile aus dem strafrechtlichen Umfeld
- Aber zivilrechtlich, z.B.
  - Landgericht Flensburg, Urteil vom 05. Juli 2013, Az: 4 O 54/11:
    Externe Dritte, wie z. B. auch Softwarewartungsunternehmen, dürfen lediglich zum Zwecke der Softwarepflege und -wartung herangezogen werden, wenn sichergestellt ist, dass sie hierdurch keinen Zugriff auf die Patientendaten erlangen können.
    (http://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Flensburg&Datum=05.07.2013&Aktenzeichen=4%20O%2054/11)
  - ADV? Laut EU sind ADV-Dienstleister keine Dritte, LG Flensburg urteilte anders…

Welche Besonderheiten brauchen wir denn?

1. Sozialdaten
2. Umgang mit §203 StGB
3. TOMs unter den Gesichtspunkten der unterschiedlichen Gesetze in Deutschland

TOMs unter den Gesichtspunkten der unterschiedlichen Gesetze in Deutschland

- Unterschiedliche Definitionen, Beispiel „Löschen“
- Bundesrecht, 16 x Landesrecht, 2 x Kirchenrecht = Fünf verschiedene Definitionen
  1) Unkenntlichmachen gespeicherter personenbezogener Daten
  2) Löschen das Beseitigen gespeicherter Daten
  3) Das endgültige Unkenntlichmachen gespeicherter Daten
  4) Das Unkenntlichmachen von Daten oder das Vernichten des Datenträgers
  5) Das dauerhafte Unkenntlichmachen gespeicherter Daten
- RL 95/46/EG bietet zwar keine Definition des Löschbegriffs, aber
  - Im Urteil des EuGH vom 13. Mai 2014 wird der Begriff „Löschen“ im Sinne von „Löschen im physikalischen Sinn“ oder als irreversibel anonymisieren angesehen
  - EU-Definition := physikalisch Löschen oder irreversibel anonymisieren
- Sechs Definitionen zu Löschen: was muss im Vertrag vereinbart werden?
- (Kann mit anderen Begriffen nahezu beliebig fortgesetzt werden)

Welche Besonderheiten brauchen wir denn?

Es gilt noch viel ein bisschen mehr zu beachten…

1. Sozialdaten
2. Umgang mit §203 StGB
3. TOMs unter den Gesichtspunkten der unterschiedlichen Gesetze in Deutschland
4. Umgang mit Beschlagnahmeschutz
5. Darstellung der landesgesundheitsrechtlichen Grundlagen für einen ADV-Vertrag
6. Darstellung der bundes- und landesrechtlichen Anforderungen an einen ADV-Vertrag
7. Umgang mit Datenverarbeitung außerhalb EU/EWR
8. Umgang mit EU-Standardvertragsklausen
9. Regelung bzgl. Umgang mit Zurückbehaltungsrecht i.S.v. § 273 BGB
10. Schadensersatz- und Haftungsfragen ansprechen
11. Verpflichtung entsprechend TKG/UWG
12. Informationspflichten gemäß §13 TMG
13. Umgang mit Zweckänderung durch den Auftragnehmer, z.B. Weitergabe der Daten nach Pseudonymisierung/Anonymisierung
14. ….

Diskussion

Kontakt: Schuetze@medizin-informatik.org