AUFTRAGSDATENVERARBEITUNG FÜR DEN AUFTRAGGEBER: RECHTE UND PFLICHTEN

Dr. Bernd Schütze

Frühjahrstagung KHiT, Leipzig, 07. April 2016

HEALTHCARE SOLUTIONS

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.

AGENDA

- Klärung von Begrifflichkeiten
- Auftragsdatenverarbeitung – was muss ich berücksichtigen, woran sollte ich denken?
- Der ADV-Vertrag
- Und morgen? EU Datenschutz-Grundverordnung und ADV
- Sanktionsmöglichkeiten

KLÄRUNG VON BEGRIFFLICHKEITEN

AUFTRAGSDATENVERARBEITUNG

- **Grundlage: §11 BDSG**
- **Wieso eigentlich BDSG? Für mich gilt doch Krankenhausgesetz „xy“**

  Ja, im Prinzip schon, aber ...

  1) Subsidiaritätsprinzip resultiert aus §1 Abs. 3 BDSG

     „Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.“

     - Frage: Regelt Ihr Krankenhausgesetz die ADV „spezieller“ als das BDSG?

  2) Grundsätzlich sind die Vorgaben der EU Richtlinie 95/46 bindend (siehe diverse EuGH-Urteile)

     - D.h. Vorgaben Art. 16 und17 RL 95/46 müssen erfüllt werden
     - Viele Landesgesetze setzten die RL nicht um, so dass hier Vorgaben des BDSG oder der RL anzuwenden sind (in Deutschland wird überwiegend vom BDSG ausgegangen)

BEGRIFFLICHKEITEN UND DARAUS RESULTIERENDE FOLGEN

- **Übermitteln (§3 Abs. 4 Ziff. 3 BDSG)**

  Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass

  a) die Daten an den **Dritten** weitergegeben werden oder

  b) der **Dritte** zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

- **Dritter (§3 Abs. 8 S. 2/3 BDSG)**

  Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle.

  Dritte sind nicht der Betroffene sowie Personen und Stellen, die im **Inland**, in einem anderen **Mitgliedstaat** der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den **Europäischen Wirtschaftsraum** personenbezogene **Daten im Auftrag** erheben, verarbeiten oder nutzen.

- **D.h.: Bei einer Verarbeitung/Nutzung von Daten im Auftrag der verantwortlichen Stelle erfolgt keine Übermittlung**
- **Somit wird keine Einwilligung des Patienten dazu benötigt**

AUFTRAGSDATENVERARBEITUNG: §11 BDSG

- **Auftraggeber ist für Einhaltung aller Datenschutzvorschriften verantwortlich (§11 Abs. 1 BDSG)**
- **Dies beinhaltet jegliche Handlung des Auftragnehmers (der darf ja nur auf explizite Anweisung des Auftraggebers tätig werden)**
  - Zivilrechtlich natürlich Rückgriff auf Auftragnehmer möglich
- **Beispiele zur Auftragsdatenverarbeitung**
  - Ablage von personenbezogenen Daten auf extern gehosteten Servern
  - Schreibdienste durch externes Schreibbüro
  - Entsorgung von Akten oder Datenträgern durch externe Unternehmen
  - Prüfung/Wartung von automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen: immer Auftragsdatenverarbeitung (§11 Abs. 5 BDSG)

ADV UND SCHWEIGEPFLICHT

- **Apropos BDSG und andere Rechtsnormen: berufliche Schweigepflicht (§203 StGB)**

  §1 Abs. 3 BDSG:

  - „Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen... bleibt unberührt.

- **ADV und Beschlagnahmeschutz**

  Beschlagnahmeschutz für Patientendaten gilt entsprechend §97 stopp, wenn sich die Gegenstände bzw. Dokumente im Gewahrsam

  - des Arztes oder
  - einer Krankenanstalt, d. h. in deren Räumlichkeiten befindet oder
  - eines Dienstleisters, der für die behandelnde Person bzw. Institution personenbezogene Daten erhebt, verarbeitet oder nutzt

  Insbesondere damit natürlich auch beim ADV-Dienstleister.

AUFTRAGSDATENVERARBEITUNG – WAS MUSS ICH BERÜCKSICHTIGEN, WORAN SOLLTE ICH DENKEN?

AUSWAHL DES AUFTRAGNEHMERS

- **Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen (§11 Abs. 2 BDSG)**
  - D.h.: ggfs. muss ich in einer Ausschreibung den „teuereren“ Auftragnehmer auswählen, wenn dieser hinsichtlich der TOMs besser geeignet ist
  - D.h.: ich darf keinen Auftragnehmer beauftragen, dessen TOMs nicht dem notwendigen Schutzniveau entsprechen
  - Beispiel KIS-Wartung: sie haben nur genau einen Anbieter, der die Wartung übernehmen kann. Erfüllt dieser die Anforderungen nicht ...

AUSWAHL DES AUFTRAGNEHMERS

- **Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.**
  - D.h.: genaugenommen **vor** Auftragsvergabe **und vor** Verarbeitungsbeginn (sogenannte „Erstkontrolle“)
  - Danach: regelmäßig
- **Was heißt regelmäßig?**
  - Gesetzgeber schrieb keine Fristen ins Gesetz, da diese „der in der Praxis vorkommenden Bandbreite an Auftragsdatenverarbeitungen nicht gerecht“ (würde)
  - Pflicht zur Kontrolle: Hinweise auf Probleme beim Auftragnehmer liegen vor
  - Grundregel: je sensibler die Datenverarbeitung desto häufiger müssen Kontrollen erfolgen
    ➔ Gesundheitsdaten vermutlich mindestens einmal pro Jahr
  - ➢ Rechnung: Uniklinik mit etwa 150 ADV-Verträgen, bei jedem eine Überprüfung pro Jahr, …
- **Bitte an Dokumentation denken**
  - Fehlende Dokumentation kann bei Kontrolle durch die Aufsichtsbehörde Geld kosten

AUSWAHL DES AUFTRAGNEHMERS

- **Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.**
- **Was heißt überzeugen?**

  Vom Gesetzgeber ebenfalls bewusst offen gelassen, daher verschiedene Möglichkeiten:

  1) Datenschutzaudit im Rahmen einer Vor-Ort-Kontrolle
     (von Aufsichtsbehörden empfohlen, oftmals für Routinekontrollen aber nicht durchführbar)
  2) Testat eines Sachverständigen
  3) Unabhängige Zertifikate
     a) ISO 9001: als alleiniger Nachweis nicht geeignet
     b) ISO 27001: genaue Überprüfung nötig
        Beispiel: Zertifizierung Rechenzentrum nützt nichts, wenn die Dienstleistung vom Helpdesk eingekauft wird
     c) Datenschutzsiegel von GDD/BvD
        (Datenschutz Zertifizierungsgesellschaft mbH, speziell für ADV)
     d) ...
  4) Schriftliche Auskunft des Auftragnehmers anhand von Fragebögen

DER ADV-VERTRAG

ADV-VERTRAG

- **„Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind …“ (§11 Abs. 2 S. 2 BDSG)**
  1. der Gegenstand und die Dauer des Auftrags,
  2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
  3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
  4. die Berichtigung, Löschung und Sperrung von Daten,
  5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
  6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
  7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
  8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
  9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
  10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

ADV-VERTRAG

- **„Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind ...“ (§11 Abs. 2 S. 2 BDSG)**
  1. der Gege
  2. der Umfa zung von Daten, die Art de
  3. die nach
  4. die Berich
  5. die nach n vorzuneh
  6. die etwai
  7. die Kontr gspflichten des Auftragnehmers,
  8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
  9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
  10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Vertragsinhalte schauen wir uns mal an...

ADV-VERTRAG:
GEGENSTAND, UMFANG UND DAUER DES AUFTRAGS

- Meistens wird der genaue Gegenstand des Auftrags in einem Hauptvertrag dargestellt sein, sodass an dieser Stelle auf den entsprechenden Vertrag verwiesen werden kann
- Gleiches gilt für die Dauer der Beauftragung
- Cave: Prüfungsberechtigten Dritten (z.B. Aufsichtsbehörden, Auditoren, ...) muss Einblick in datenschutzrechtlich relevante Vereinbarungen gewährt werden
  → Unkenntlichmachung von schützenswerten Stellen innerhalb des Vertrag bei Prüfung erforderlich
- Cave: Rahmenvertrag beinhaltet meist nicht die datenschutzrechtlichen Aspekte des Auftrags (Art der Unterstützung, betroffener Personenkreis, ...)
  hier muss der ADV-Vertrag dann diese Angaben beinhalten
- Welche Weisungsbefugnisse hat der Auftraggeber gegenüber dem Auftragnehmer? Was darf der Auftragnehmer selbstständig entscheiden?

ADV-VERTRAG:
TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

- **Im Vertrag: Verpflichtung der vereinbarten Maßnahmen**
  - Stand der Technik berücksichtigen
- **Eigentliche Maßnahmen im Anhang aufführen**
- **Wichtig: im Vertrag Anpassung der TOMs berücksichtigen**
  → im zeitlichen Verlauf muss auf sich wandelnde Gegebenheiten reagiert werden können ohne Notwendigkeit für neue Vertragsgestaltung
- **Bei Maßnahmen wie Protokollierung ggfs. auf Hinzuziehung der Mitarbeitervertretung achten (potentielle Kontrolle von Mitarbeitern)**
  - Auf Auftragnehmer hat Mitarbeitervertretung des Uaftraggebers keinen Zugriff, daher Protokollauswertung durch Auftragnehmer entsprechend „sensibel“ behandeln

ADV-VERTRAG: BERICHTIGUNG, LÖSCHUNG UND SPERRUNG VON DATEN

- Betroffene haben grundsätzlich das Recht auf Berichtigung, Sperrung und Löschung
- Auftraggeber bleibt dem jeweiligen Betroffenen gegenüber verantwortlich
- Auftraggeber muss daher Auftragnehmer mit der Durchführung entsprechender Maßnahmen beauftragen können
- Regelung notwendig: Betroffener wendet sich Auftragnehmer – was soll dieser tun?

Sonderfall:

- Auftragnehmer steht Pfändung/Insolvenz ins Haus:
  ➔ Vorgehen bzgl. Umgang mit evtl. vorhandenen Daten des Auftraggebergeregelt?
  Gesundheitsdaten können viel Geld wert sein...

ADV-VERTRAG: PFLICHTEN DES AUFTRAGNEHMERS

- **Auftragnehmer muss vertraglich dahingehend verpflichtet werden, dass der Auftraggeber die für ihn geltenden gesetzlichen Bestimmungen einhalten kann (z.B. Aufsichtsbehörde des Auftraggebers zuständig, Informationspflichten gegenüber Betroffenen)**
- **Datenschutzbeauftragter des Auftragnehmers wird dem Auftraggeber benannt**
- **Verpflichtung des Personals des Auftragnehmers auf das Datengeheimnis**
  - Cave: Verpflichtung des AN-Personals i.d.R. nur auf BDSG möglich
  - Hinweis: Verpflichtung auf §203 StGB nicht möglich!
    (Entweder gilt der §203 StGB oder er gilt nicht; Verpflichtung nicht möglich)
  - ABER: Verpflichtung Auftragnehmer sowie dessen Personal nach §17 UWG möglich
    ➔ Versuch der Weitergabe von Geschäfts- oder Betriebsgeheimnis = strafbare Handlung
- **Verpflichtung des Aufragnehmers zur Mitteilung von Vertragsverletzungen und Datenpannen**
- **Darf der Auftragnehmer Daten des Auftraggebers für sich selbst nutzen? (Sekundärnutzung, z.B. zur Qualitätskontrolle, Testdaten)**
- **Rückgabe/Löschung der Daten des Auftragnehmers nach Auftrags-/Vertragsende**

ADV-VERTRAG: KONTROLLPFLICHTEN

- **Auftragnehmer muss kontrollieren (gesetzlich vorgeschrieben**
  Aber: Auftragnehmer muss sich nicht kontrollieren lassen
- **Vertragliche Vereinbarung notwendig, dass Auftragnehmer Kontrolle zulässt und unterstützt**
  - Zutritt zu den Räumlichkeiten des Auftragnehmers (wann)
  - Wann müssen Kontrollen angekündigt werden, wann nicht
  - Wer darf kontrollieren (Auftraggeber, Beauftragte des Auftraggebers, Aufsichtsbehörden,...)
  - Was darf kontrolliert werden?
    (Abgrenzung zu evtl. schützenswerten Frmengeheimnissen des Aufragnhmees nötig?)
  - ...
- **Jede Kontrolle muss dokumentiert werden**
  - Nach §43 Abs. 1 Nr. 2b BDSG kann eine Aufsichtsbehörde ein Bußgeld verhängen, wenn der Nachweis einer erfolgten Erstkontrolle vom Auftraggeber nicht erbracht werden kann
  - Bitte auch Dokumentieren: wie habe ich mich überzeugt, dass der Auftragnehmer geeignet ist und die TOMs den Vorgaben entsprechen?

ADV-VERTRAG: UNTERAUFTRAGNEHMER

- **24 x 7 – Support: häufig Unterauftragnehmer, z.B. follow-the-sun**
- **Gesetzgeber schreibt Regelung vor, wie mit Unterauftragnehmer umgegangen werden muss, daher viele Freiheitsgrade für Auftraggeber und Auftragnehmer**
  - Wichtig: Für alle Unterauftragnehmer muss die Erhaltung des mit dem Aufragnehmer vereinbarten Schutzniveau gelten
- **Wichtig: ADV nur in der EU bzw. dem EWR möglich ➔ bei Verarbeitung in anderen Ländern Rechtsgrundlage (i.d.R. Einwilligung des Betroffenen) zwingend erforderlich**
  - Unterauftragnehmer in Drittländern (= alles außerhalb EWR)
  - Rechtsgrundlage:
    - EU-Standardvertragsklausen (Standard)
    - Binding Corporate Rules (nur innerhalb eines Unternehmensverbundes)
    - individuelle Genehmigung durch die Aufsichtsbehörde (wird selten zum Tragen kommen)
    - (Einwilligung Betroffner nur Ausnahmefall möglich)
- **EU-Standardvertragsklausen: Betroffener muss vorher informiert werden**
  ➔ Alle Patienten informieren, dass evtl. Daten in einem Drittland verarbeitet werden

ADV-VERTRAG: HILFSMITTEL

- Muster ADV-Vertrag für das Gesundheitswesen
- Ausarbeitung von BvD, bvitg, GDD und GMDS
- Verfügbar z.B. auf der Homepage der GMDS-AG DIG
  http://gesundheitsdatenschutz.org/doku.php/adv-mustervertrag-2015

UND MORGEN?
EU DATENSCHUTZ-GRUNDVERORDNUNG

ADV UNTER DER EU DS-GVO

Die gute Nachricht:

- Vieles kommt einem bekannt vor ...
- Im Detail ist da vielleicht doch das eine oder andere Erwähnenswerte ...

ADV UNTER DER EU DS-GVO

Die gute Nachricht:

- **Viele**
- **Im De**

Die nachfolgenden Ausarbeitung beruht auf der offiziellen Übersetzung* des Trilog-Ergebnisses

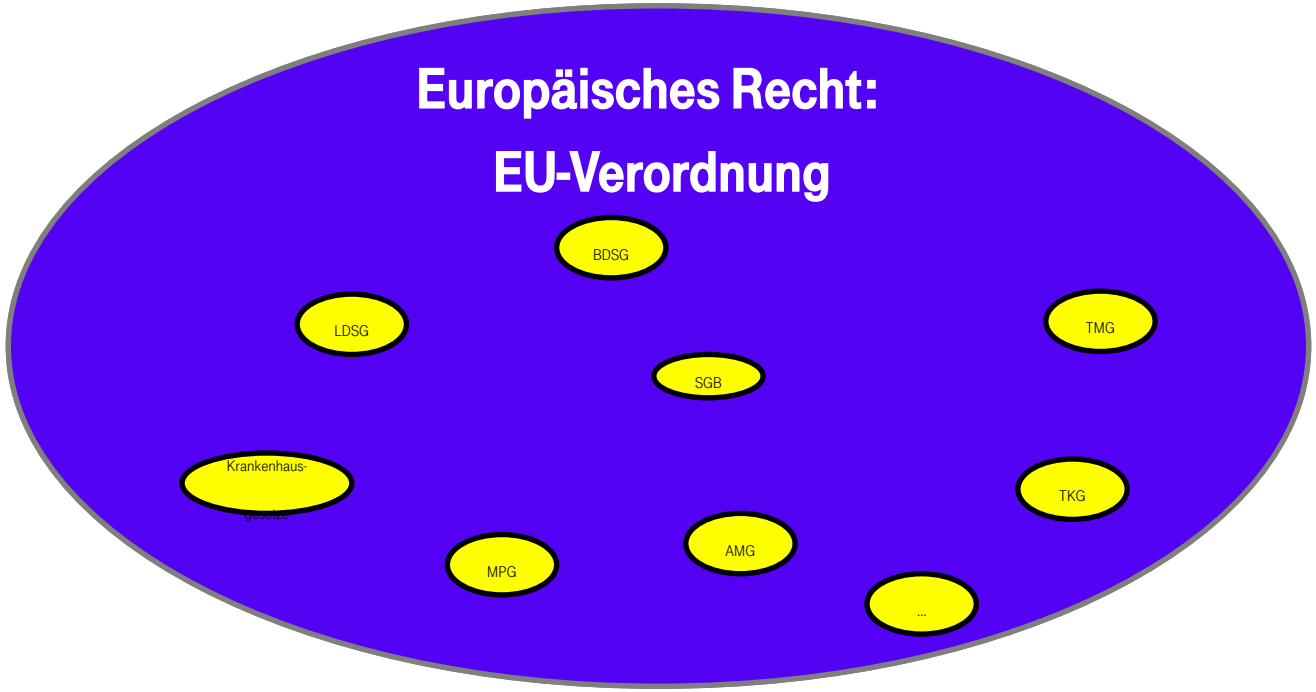
D.h. die Nummerierung der Artikel usw. in der finalen Version kann abweichen

Inhaltlich bleibt hingegen alles bestehen.

(* http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1455435317242&uri=CONSIL:ST_5455_2016_INIT)

EU VS. DEUTSCHES RECHT

Grundsatz: Anwendungsvorrang des EU-Rechts



1. Inhaltsgleiches deutsches Recht wird „überlagert“
2. Nur an den Stellen, wo deutsches Recht als „ergänzend“ zum EU-Recht angesehen werden kann, gelten weiterhin diese Regelungen

ART. 26 „AUFTRAGSVERARBEITER “

- **Erlaubt nur Auftragsverarbeitern, die hinreichende Garantien dafür bieten, dass die betreffenden technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet**
- **Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Zustimmung des für die Verarbeitung Verantwortlichen in Anspruch**
- **Durchführung einer Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten,**
  - der bzw. das den Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen bindet
  - in dem Gegenstand und Dauer der Verarbeitung,
  - Art und Zweck der Verarbeitung,
  - Art der personenbezogenen Daten,
  - Kategorien von betroffenen Personen
  - Pflichten und Rechte des für die Verarbeitung Verantwortlichen festgelegt sind

ART. 26 „AUFTRAGSVERARBEITER “

- **Erlaub** **den**
  techni **ung im**
  Einkla **troffenen**
  Perso
- **Auftra** **der allgemeine**
  schrift
- **Durch** **eines Vertrags**
  oder e
  - (
  - i
  - A
  - A
  - Kategorien von betroffenen Personen
  - Pflichten und Rechte des für die Verarbeitung Verantwortlichen festgelegt sind

1) Sorgfältige Auswahl des Auftragnehmers bleibt bestehen
2) Auftragnehmer darf nur ausgewählt werden, wenn Datenschutz/-sicherheit bei ihm gewährleistet
3) ADV-Vertrag muss abgeschlossen werden

ART. 26 „AUFTRAGSVERARBEITER “

- **Insbesondere ist im Vertrag vorgesehen, dass der Auftragsverarbeiter**
  - Daten nur auf dokumentierte Weisung des für die Verarbeitung Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet
  - gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen
  - unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den für die Verarbeitung Verantwortlichen bei der Einhaltung der in den Artikeln 30 bis 34 genannten Pflichten unterstützt
  - nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des für die Verarbeitung Verantwortlichen entweder zurückgibt oder löscht
  - dem für die Verarbeitung Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom für die Verarbeitung Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt
- **Einem Unter-Auftragnehmer sind vom Auftragsverarbeiter dieselben Pflichten aufzuerlegen, die für ihn selbst gelten**

ART. 26 „AUFTRAGSVERARBEITER “

- **Insbes**
  - I Bezug auf die
    on –
  - onen zur
    spflicht
  - rmationen den
    nten Pflichten
  - n nach Wahl
  - der Einhaltung

    der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom für die Verarbeitung Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt
- **Einem Unter-Auftragnehmer sind vom Auftragsverarbeiter dieselben Pflichten aufzuerlegen, die für ihn selbst gelten**

Vertragsinhalte entsprechen (weitestgehend) den Anforderungen von §11 BDSG

INFORMATION DES BETROFFENEN

- **Art. 14 (= Informationspflicht bei Erhebung der Daten bei der betroffenen Person)**

  Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der für die Verarbeitung Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit (Abs. 1 Lit d):

  - gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

- **Art. 14a (= Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden)**

  Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der für die Verarbeitung Verantwortliche der betroffenen Person Folgendes mit (Abs. 1 Lit. D):

  - gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

- **Art. 15 (= Auskunftsrecht der betroffenen Person)**

  Die betroffene Person hat das Recht... (Abs. Lit c):

  - die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben worden sind oder noch weitergegeben werden, speziell bei Empfängern in Drittländern oder bei internationalen Organisationen

- **Art. 4 Abs. 7**
  - "Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, an die personenbezogene Daten weitergegeben werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

INFORMATION DES BETROFFENEN

- Müssen Patienten künftig alle ADV-Dienstleister genannt werden? Wohl ja.
- Evtl. Web-Portal der Klinik hierzu nutzen und Patienten Link zur Verfügung stellen.
- Cave:
  - Der Patient muss sich bzgl. „Empfänger informieren können
    ➔ Änderungen des Links, Änderungen Liste usw.
    ➔ Info für Pat. muss aufrechterhalten werden!
  - Wie ersieht der Patient aus der Liste der ADV-Dienstleister, was auf ihn zutrifft? (Pat. mit Knochenbruch wird vermutlich in anderen Systemen dokumentiert als bspw. ein onkologischer Patient)

ART. 30 „SICHERHEIT DER VERARBEITUNG“

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

Diese Maßnahmen schließen gegebenenfalls Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die 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

ART. 30 „SICHERHEIT DER VERARBEITUNG“

Der für di… …ung

- des St…
- der Im…
- der Ar…
- der un… …en Rechte und Freihe…

geeignete… …tzniveau zu gewährlei…

Diese Ma…

- die Ps…
- die Fä… … Dienste im Zusan…
- 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

1. Prüfen: ob ADV mit pseudonymisierten Daten erbracht werden kann
2. Dokumentation der Prüfung, festhalten der Begründung, warum bzw. warum nicht
3. Abwägungsmöglichkeit betriebswirtschaftlicher Kosten beinhaltend gegeben
   ➔ Keine absolute Sicherheit gefordert!

ART. 30 „MELDUNG VON VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN“

- Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der für die Verarbeitung Verantwortliche ohne unangemessene Verzögerung und möglichst **binnen höchstens 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde
- es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt
- Falls die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden erfolgt, ist ihr eine Begründung beizufügen
- Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem für die Verarbeitung Verantwortlichen ohne unangemessene Verzögerung

ART. 30 „MELDUNG VON VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN“

Innerhalb von 72 Stunden nach Ereignis: sportlich…

- **Die Meldung enthält mindestens folgende Informationen**
  - eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Datensätze;
  - den Namen und die Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen
  - eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
  - eine Beschreibung der von dem für die Verarbeitung Verantwortlichen **ergriffenen odervorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes** personenbezogener Daten und gegebenenfalls zur Eindämmung ihrer möglichen nachteiligen Auswirkungen
- **Der für die Verarbeitung Verantwortliche dokumentiert etwaige Verletzungen des Schutzes personenbezogener Daten unter Beschreibung aller im Zusammenhang mit der Verletzung stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Die Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.**

ART. 30 „MELDUNG VON VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN“

Innerhalb von 72 Stunden nach Ereignis:

1. **Die jüngste Vergangenheit zeigte: keiner ist sicher**
2. **Daher: Reaktionsteam erstellen; wissend, dass dieses hoffentlich nie aktiv wird**
3. **Der Datenschutzbeauftragte alleine wird im Eintrittsfall alleine überfordert sein!**

- **Die M**
  - möglich mit
  - rechpartners
  - ogener Daten;
  - **geschlagenen** gegebenenfalls
- **Der fü**

perso **ehenden**
Fakte **n muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.**

ART. 32 „BENACHRICHTIGUNG DER VON EINER VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN BETROFFENEN PERSON“

- Besteht die Wahrscheinlichkeit, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten bewirkt, so benachrichtigt der für die Verarbeitung Verantwortliche die betroffene Person ohne unangemessene Verzögerung von der Verletzung
- Die Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die *Art der Verletzung* des Schutzes personenbezogener Daten und enthält mindestens die in Artikel 31 Absatz 3 Buchstaben b, d und e genannten Informationen und Empfehlungen
- Sorgt der für die Verarbeitung Verantwortliche durch geeignete Maßnahmen dafür, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr besteht, kann evtl. die Benachrichtigungspflicht hinsichtlich der betroffenen Person entfallen

ART. 32 „BENACHRICHTIGUNG DER VON EINER VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN BETROFFENEN PERSON“

- Beste … ein hohes Risiko … beitung Veran …
- Die Be … *Art der Verlet* … Absatz 3 Buchs …
- Sorgt … hohe Risiko für die Re … besteht, kann evtl. d …

Benachrichtigt wird

1. Bei eingetretener Datenpanne
2. Bei Wahrscheinlichkeit des Eintretens einer Datenpanne

Beispiel:

- Gestohlener Laptop, gut verschlüsselte Festplatte -> wohl keine Benachrichtigung erforderlich
- Gestohlener Laptop, keine Verschlüsselung -> Benachrichtigung wohl erforderlich

ART. 35 „BENENNUNG EINES DATENSCHUTZBEAUFTRAGTEN“

- **Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn**
  - die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die in ihrer gerichtlichen Eigenschaft handeln, oder
  - die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen, oder
  - die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen **Verarbeitung besonderer Kategorien von Daten** gemäß Artikel 9 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 9a besteht.
- **Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann**
- **Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt**
- **Der Datenschutzbeauftragte kann Beschäftigter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen**

ART. 35 „BENENNUNG EINES DATENSCHUTZBEAUFTRAGTEN“

- Der fü … l einen Daten …
  - … ne von …
  - … der … gs und/oder … nen Personen …
  - … der … Daten über …
- Eine U … ern von jeder Niede …
- Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt
- Der Datenschutzbeauftragte kann Beschäftigter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen

- Krankenhäuser benötigen weiterhin einen Datenschutzbeauftragten
- Hersteller von Informationssystemen evtl. künftig nicht mehr (Allerdings kann der nationale Gesetzgeber die aktuelle Regelung beibehalten)

ART. 28: „VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN“

- **Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen eine Aufzeichnung zu allen Kategorien von im Auftrag eines für die Verarbeitung Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung personenbezogener Daten, die Folgendes enthält:**
  - den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes für die Verarbeitung Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie eines etwaigen Vertreters des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten
  - die Kategorien der Verarbeitungen, die im Auftrag jedes für die Verarbeitung Verantwortlichen durchgeführt werden;
  - gegebenenfalls Übermittlungen von 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 44 Absatz 1 Buchstabe h genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
  - wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
- **Die Aufzeichnungen sind schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann**
- **Der für die Verarbeitung Verantwortliche, der Auftragsverarbeiter sowie der etwaige Vertreter des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde die Aufzeichnungen auf Anforderung zur Verfügung**
- **Ausnahmetatbestand von Abs. 4 (weniger als 250 Mitarbeiter beschäftigt) gilt nicht bei der Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1**

ART. 28: „VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN“

- **Jeder A gorien von im Auftrag person**
  - d Verarbeitung V ür die V n
  - d rt werden;
  - g chließlich der A Artikel 44 A
  - w
- **Die Auf nn**
- **Der für die Verarb eichnungen auf Anfor**
- **Ausnahmetatbestand von Abs. 4 (weniger als 250 Mitarbeiter beschäftigt) gilt nicht bei der Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1**

- **Verfahrensverzeichnis bisher ausschließlich Aufgabe des Auftraggebers**
- **Künftig muss Auftragnehmer für bei ihm stattfindende Datenverarbeitung die Verfahren dokumentieren**

WAS IST ZU TUN?

- **Hinweis: §11 Abs. 5 BDSG entfällt ➔ Wartung nicht mehr automatisch ADV**
- **Gesamtschuldnerischer Haftung de für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters (Art. 77)**
  - Aber: Entlastungsmöglichkeit des Auftragsverarbeiters vorhanden
- **Auftragsverarbeiter verpflichten auf**
  - Informationspflichten bei Verstoß gegen Art. 5 (Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten ➔ Verstoß Bußgeldbewehrt)
  - Informationspflicht bei Verstoß gegen TOMs (Art. 30 ➔ Bußgeldbewehrt)
  - Unterstützung bei „Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 25 ➔ Bußgeldbewehrt)
  - Unterstützung bei der Folgenabschätzung

WAS IST ZU TUN?

– **Ggfs. Rechtsgrundlage überprüfen z. B.. Einwilligung**

Neue Pflichten, insbesondere

- Recht zum Widerruf Einwilligung und Pflicht zum Hinweis hierauf
- Keine Schriftformerfordernis mehr, aber Beweislast trägt für die Verarbeitung Verantwortlicher
- Angabe Speicherdauer
- Zweck der Verarbeitung
- Procedere bzgl. Informationspflichten anpassen

Neu z. B.

- Zweck der Verarbeitung
- Vorgesehene Firsten für Löschung
- Allgemeine Beschreibungen der TOMs

Unterstützung ADV-Dienstleister einfordern

SANKTIONSMÖGLICHKEITEN

SANKTIONSMÖGLICHKEITEN

- **§43 Abs. 1 Ziff. 2b BDSG**
  - „einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung über die Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt“
  - Geldbuße bis zu fünfzigtausend Euro (ggfs. pro falsch vergebenem Auftrag)
  - ABER: Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

SANKTIONSMÖGLICHKEITEN

- **Art. 77 Abs. 1 EU DS-GVO**
  - Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder moralischer Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter.

SANKTIONSMÖGLICHKEITEN

- **Art. 79 Abs. 2a Eu DS-GVO**

  Allgemeine Bedingungen für die Verhängung von Geldbußen u.a.

  - Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung
  - Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
  - etwaige einschlägige frühere Verstöße
  - Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind
  - Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde

SANKTIONSMÖGLICHKEITEN

- **Art. 79 Abs. 3a Eu DS-GVO**
  - Geldbußen von bis zu 10 Mill. € oder im Fall eines Unternehmens von bis zu 2 % Jahresumsatz
    - ➔ Z. B. bei Verstoß bzgl. Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter
  - Geldbußen von bis zu 20 Mill. € oder im Fall eines Unternehmens von bis zu 4 % Jahresumsatz
    - ➔ Z. B.: Fehlende Einwilligung, Verarbeitung ohne Rechtsgrundlage, Übermittlung Drittland

FRAGEN?

Kontakt: Bernd.Schuetze@T-Systems.com