Zusammenarbeit mit Dritten: Auftragsverarbeitung, gemeinsame Verantwortlichkeit, …

Fachtagung Datenschutz im Gesundheitswesen 2023

Referent: David Koeppe

Ihr Referent:

David Koeppe

GDD-AK
„Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Vivantes - Netzwerk für Gesundheit GmbH
Aroser Allee 72-76
13407 Berlin
Tel. 030/130-111011
david.koeppe@vivantes.de

Agenda

- Rechtlicher Rahmen
  - Begriffsbestimmungen
  - Erforderlichkeit der Verantwortungsverortung
- Auftragsverarbeitung
  - Beispiele für Anwendungsfälle einer AV
  - AV-Vertrag
  - Pflichten der Beteiligten
  - Vertragsbestandteile
  - Praxisfälle: Achtung Klauseln!
- Gemeinsame Verantwortung
  - Vertrag zur Gemeinsamen Verantwortung
  - Besondere Aspekte in der Verantwortungsabgrenzung
  - Beispiele für Anwendungsfälle
- Einfluss nationalen Rechts auf die Zusammenarbeit mit Dritten
  - Bedingungen für die Anwendung des Art. 28 DS-GVO
  - § 203 StGB
  - Ärztliche Berufsordnung

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 weisungsabhängig verarbeitet (Art. 4 Ziff. 8)
- Dritter: jede/r außerhalb der Sphäre des Verantwortlichen/Auftragsverarbeiters und der betroffenen Person - als Adressat von Offenlegungen/Übermittlungen

Verortung der Verantwortung

Ausgestaltung einer Verarbeitungstätigkeit unter Beteiligung mehrerer eigenständiger juristischer/natürlicher Personen:

Getrennte Verantwortung - volle Verantwortung jeder Partei mit Verantwortungsübergang bei Datenübermittlung (analog zum zivilrechtlichen Gefahrenübergang);

➡ grds. zwei getrennte Verarbeitungstätigkeiten

Gemeinsame Verantwortung - *weitgehend* volle Verantwortung jeder Partei, jedoch mit selektiver Abgrenzung/Delegation

Auftragsverarbeitung - Hauptverantwortung beim Auftraggeber, Weisungsgebundenheit und partielle Verantwortlichkeiten nebst Rechenschaftspflichten beim Auftragnehmer

„Funktionsübertragung“

Bezeichnung für Beauftragungen, die keine Auftragsverarbeitungen sind:

- Wenn Zwecke und Mittel der Verarbeitung nicht vollständig in der Entscheidungsgewalt des beauftragenden Verantwortlichen liegen
- Folge: Übermittlung an einen weiteren Verantwortlichen
- Übermittlung/Offenlegung mit Erfordernis der rechtlichen Legitimation
- Nicht privilegiert
- Unter der DS-GVO wohl gelegentlich eine Gemeinsame Verantwortung

- Literaturkonstrukt dem BDSG-alt folgend -

Auftragsverarbeitung

Grundsätzliches

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

2 Kategorien von gesetzlichen Regelungen:

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

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 (z.B. im Rahmen des Art. 46 (2) c) DS-GVO)

Anwendungsfälle (1)

Typische Dienstleistungen als Auftragsverarbeitung:

- Datenträgerentsorgung ☑
- Web-Hosting ☑
  (zumindest soweit es über die temporäre Erfassung der IP-Adressen hinausgeht)
- Rechenzentrums-Betrieb (aber: RZ-Housing?) ☑
- Software as a Service (SaaS) ☑

Anwendungsfälle (2)

- (Fern-)Wartung IT/Medizintechnik ☑
- Archivbewirtschaftung ☑
- (Gegen-)Prüfung von MDK-Gutachten
  solange nicht durch Freiberufler (Wirtschaftsprüfer, Steuerberater) erbracht
- Erbringung von IT-Leistungen (IT-Infrastruktur, Service) für weitere Konzerngesellschaften
  grundsätzlich ja, aber bei enger Verflechtung ggf. gemeinsame Verantwortung

(Keine) Anwendungsfälle (1)

- Beauftragung von medizinischer Labordiagnostik
  ärztliche Leistung - fachlich weisungsfrei - getrennte Verantwortung
- Beauftragung eines Post-Dienstleisters
  gesetzlich definierte Rolle, mit eigenen gesetzlichen Pflichten - getrennte Verantwortung
- Steuerberatung
  freiberuflich - fachlich weisungsfrei
  https://www.lda.bayern.de/media/veroeffentlichungen/FAQ_Steuerberater_keine_ADV.pdf
- Privatärztliche Abrechnung mit Forderungsabtretung
  zivilrechtlicher Forderungsübergang - neuer Verantwortlicher
- Zentrale Vorgangsdokumentation des (externen) Datenschutzbeauftragten
  gesetzlich definierte Funktion, fachlich weisungsfrei

(Keine) Anwendungsfälle (2)

- Wäschereileistungen, *Nebenleistung*: Anbringen von Namensaufnähern an Dienstkleidung

  bei nur geringem Anteil an der Gesamtdienstleistung: nein

- Führung eines einrichtungsübergreifenden medizinischen Qualitätssicherungsregisters (Rückmeldung von QS-Statistiken an die Teilnehmer, eigene Beschickung von Forschungsvorhaben mit Registerdaten)

  Verfolgung eigener Zwecke

(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

Privilegierung der AV

- Auftragsverarbeiter ist 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 Offenlegung in der Auftragsverarbeitung
  - nicht in der *DS-GVO*
- „Lediglich“ Formerfordernis des AV-Vertrages

Besondere Pflichten des Verantwortlichen I

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

Besondere Pflichten des Verantwortlichen II

- ✓ Kontrollen des Auftragsverarbeiters sind angesichts der Rechenschaftspflichten unverzichtbar - „hinreichende Garantien“ (Art. 28 Abs. 1)
  - Vor Auftragsvergabe und während der Auftragslaufzeit
  - 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

- ✓ Benennung eines Vertreters in der Union, bei Niederlassung außerhalb (Art. 27)
- ✓ Hinweispflicht des Verarbeiters bei vermuteter Rechtswidrigkeit der Weisungen (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

- ✓ 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 weitgehend dem Datenschutzrecht (nicht vollständig, nur wo ausdrücklich erwähnt)

- Pflichten aus den Artt. 25-43 (Kapitel IV „Verantwortlicher 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)

  Betrifft:

  - Unvollständigkeit des Aufgabenkatalogs im AVV
  - Verstoß gegen Weisungen
  - Eigene (Sekundär)Zwecke

Sanktionierung bei Verordnungsverstößen

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. 29, 32 und 37-39 (Weisungsgebundenheit, Sicherheit der Verarbeitung, Datenschutzbeauftragter)

Muster-AV-Vertrag

Mustervertrag für das Gesundheitswesen

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

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

https://www.gesundheitsdatenschutz.org/html/adv-vertrag.php

Praxisfälle

Vertragsklauseln

Praxisfälle: Klauseln (1)

„Der Auftragnehmer trifft die technischen und organisatorischen Maßnahmen in Anlage x. Der Kunde bestätigt hiermit, dass das durch die technischen und organisatorischen Maßnahmen vermittelte Sicherheitsniveau im Verhältnis zum Risiko der Verarbeitung durch den Auftragnehmer angemessen ist.“

Kritik: Abwälzung der Auftragnehmerverantwortung für Umsetzung des Art. 32 DS-GVO auf den Auftraggeber

Praxisfälle: Klauseln (2)

„Auf Anfrage des Kunden unterstützt der Auftragnehmer den Kunden im Rahmen des Zumutbaren bei:

- der Beantwortung von Beschwerden, Anfragen oder Anordnungen nach Ziffer x.y
- der Erfüllung sonstiger datenschutzrechtlichen Verpflichtungen nach dem anwendbaren Datenschutzrecht.

Die Unterstützung wird auf Kosten des Kunden gewährt und ist nach entstandenem Aufwand zu vergüten, soweit diese nicht auf eine schuldhafte Verletzung der Vereinbarung oder anwendbaren Datenschutzrechts durch den Auftragnehmer veranlasst ist.“

Hinweis: Vergütungsregelung ist im Hauptvertrag zu regeln - Prüfung, ob Leistungspositionen dort enthalten sind.

Praxisfälle: Klauseln (3)

„Nur wenn die Zertifikate und Prüfberichte für den Kunden nicht ausreichen, um die Anforderungen und Audits und Kontrollen nach anwendbarem Datenschutzrecht einzuhalten, hat der Kunde das Recht auf eigene Kosten (i) zusätzliche Informationen und Unterlagen anzufordern, sowie (ii) nach vorheriger Mitteilung mit einer angemessenen Frist eine weitergehende Prüfung der für die verarbeiteten personenbezogenen Daten relevanten Kontrollumgebung und der Sicherheitspraktiken vorzunehmen, wobei die Auftragnehmer-Betriebsabläufe hierdurch nicht gestört werden dürfen und die Prüfung im Einklang den Auftragnehmer-Sicherheitsrichtlinien und dem anwendbaren Datenschutzrecht zu erfolgen hat."

Hinweis: Recht auf Prüfung muss ggf. erst argumentativ durchgesetzt werden; Kostendimensionen unklar, soweit nicht im Hauptvertrag festgelegt; zudem: wirtschaftliche/psychologische Hürde bei der Durchführung erforderlicher Kontrollen

Praxisfälle: Klauseln (4)

„Der Auftragnehmer muss für alle Unterauftragsverhältnisse, die die Übertragung personenbezogener Daten an einen Dritten außerhalb der Europäischen Union umfasst, der im Sinne der Datenschutzgrundverordnung 2016/679s keinen angemessenen Schutz bietet, die vorherige schriftliche Genehmigung der Klinik/Praxis einholen. Der Auftragnehmer wird angemessene Maßnahmen zur Herstellung eines angemessenen Datenschutzniveaus für die Übertragung ergreifen. Dazu zählen unter anderem Datenübertragungsvereinbarungen auf Grundlage der Standardvertragsklauseln der EU, die von der Europäischen Kommission verabschiedet wurden, um personenbezogene Daten vertraulich und sicher zu verarbeiten."

Hinweis: zu unbestimmt, „Maßnahmen" müssen vor Genehmigung konkret benannt werden - Pflicht des Verantwortlichen gemäß Art. 13 Abs. 1 lit. f DS-GVO, die Umstände und Garantien bei einer Drittlandverarbeitung zu benennen

Praxisfälle: Klauseln (5)

Formulierung im Hauptvertrag zum Vertrag zur Auftragsverarbeitung:

„Wenn betroffene Personen sich zur Geltendmachung ihrer Rechte an den Auftragnehmer wenden, wird der Auftragnehmer sie unter Verweis auf die pseudonyme Datenhaltung zwecks Realisierung der Rechtegewährung an den Auftraggeber verweisen. Dieser wird in Abstimmung mit dem Auftragnehmer und in dessen Auftrag die Rechte gewähren.“

Hinweis: Blödsinn. Pflichten zur Gewährung der Betroffenenrechte treffen Auftragnehmer nur mittelbar. Er definiert sich quasi selbst als Verantwortlichen - typische Regelung zu einer gemeinsamen Verantwortung

Praxisfälle: Klauseln (6)

Unterstützungspflichten des Auftragsverarbeiters gegenüber dem Verantwortlichen (Art. 28 Abs 3 lit. e) und f)):

- Bei der Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte und/oder
- Bei der Einhaltung der in den Artt. 32 bis 36 genannten Pflichten

(zu) häufig: selbst verfasste Aufzählung von Unterstützungsszenarien - unter Weglassen einzelner, gesetzlich vorgegebener Szenarien

***Tipp**: mehr Einfallslosigkeit bei der Vertragsformulierung*

Fazit AV

Entscheidend:

Prüfung (fremder) AV-Verträge

1. Auf vollständige Umsetzung der gesetzlichen Anforderungen
2. Auf Angemessenheit der Vertragsklauseln

Ansonsten:

Ein Vertrag zur Auftragsverarbeitung steht nicht nur für eine Pflicht, Papier zu beschreiben, sondern ist ein Anlass, eine Datenverarbeitung im Verhältnis zwischen Auftraggeber und Auftragnehmer sach- und vorschriftsgemäß auszugestalten.

Es sollte eine enge Verzahnung mit vorhandenen Elementen des Datenschutz-Managements-Systems erfolgen.

Beispiel für eine Prüf-Checkliste

Checkliste: Vollständigkeit AV-Vertrag gem. Art. 28 DS-GVO

Verarbeitung:

Auftragsgegenstand/Applikation:

Auftragsverarbeiter:

Vertragselemente	Vorhanden (j/n)	Bemerkung
Bestimmung des Auftragsgegenstands; Art, Zweck, Dauer der Verarbeitung		
Definition Betroffenengruppen		
Definition Datenkategorien		
Dokumentierte Weisung des AG		
Verpflichtung der Personen beim AN zur Vertraulichkeit / Verschwiegenheit		
Zusicherung von Maßnahmen nach Art. 32 DS-GVO		
Genehmigungsvorbehalt des AG bei der Unterauftragsvergabe		
Auferlegung der Pflichten des AN auch für Unterauftragnehmer, Bieten von Garantien, Haftung des AN für Unterauftragnehmer		
Drittland: Vorhandensein geeigneter Garantien		
Unterstützung des AG bei der Gewährung von Betroffenenrechten (Kapitel III der DS-GVO)		
Unterstützung des AG bei der Einhaltung der Pflichten nach den Art. 32 - 36 DS-GVO		
Löschung und / oder Rückgabe der Daten nach Abschluss der Erbringung der Verarbeitungsleistungen		
Zurverfügungstellung erforderlicher Informationen zum Nachweis der Einhaltung des Art. 28 DS-GVO / Zulassung von Inspektionen		
Informationspflicht des AN im Fall erkannter Rechtsverstößlichkeit von Weisungen		
Ggf. als Anlage: Benennung von Unterauftragnehmern		
Ggf. als Anlage: Skizze der Maßnahmen gem. Art. 32 DS-GVO/Sicherheitskonzept		

Zusätzliche Anmerkungen:

Geprüft durch:
Datum:

Gemeinsame Verantwortung

Gemeinsam für die Verarbeitung Verantwortliche

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

Vertrag zur GV („JCA“)

Kann sehr schlank gehalten werden - je nachdem, wie komplex die Verarbeitung bzw. die Pflichtendelegation ist.

Kern des Vertrags ist die Übersicht über die Pflichtenaufteilung.

3.2 Abgrenzung Verantwortlichkeiten / Beteiligung an der Verarbeitung

Pflicht	Verantwortlicher 1	Verantwortlicher 2
Festlegung der Zwecke und Mittel zur Verarbeitung	X	X
Festlegung der zu verarbeitenden Daten(-kategorien)	X	X
Festlegung, wer welche Pflichten aus der DS-GVO erfüllt	X	X
Wer fungiert als Anlaufstelle für die betroffenen Personen?		
Wer stellt betroffenen Personen das Wesentliche der Vereinbarung zur Verfügung?		
Wer ist für die Informationspflicht nach Art. 13 DS-GVO verantwortlich?		
Wer ist für die Informationspflicht nach Art. 14 DS-GVO verantwortlich?		
Wer beantwortet Auskunftsanfragen nach Art. 15 DS-GVO?		

Beispiel für einen Vertrag gemäß Art. 26:
https://www.gesundheitsdatenschutz.org/html/gemeinsam_verantwortlich.php

Besondere Aspekte

Häufigster Anlass für eine gemeinsame Verantwortung:

- Unmöglichkeit für eine Partei, die Betroffenenrechte zu gewähren
- Delegation der Gewährung der Betroffenenrechte an die datenführende Stelle

Besonders heikel:

Versuch der händischen Regelung der Haftungsverteilung

Anwendungsfälle (1)

- Klinische Studie: Krankenhaus im Auftrag des Sponsors

  Klassisches Szenario für gemeinsame Verantwortung
  - abhängig vom Leistungsumfang des Studienzentrums

- Erbringung von IT-Leistungen (IT-Infrastruktur, Service) für weitere Konzerngesellschaften

  bei enger Verflechtung ggf. gemeinsame Verantwortung, meist eher Auftragsverarbeitung

- Erbringung sämtlicher Leistungen im Personalwesen (Abrechnung, Aktenführung, Prozessvertretung, Personalentwicklung) für weitere Konzerngesellschaften

  gemeinsame Verantwortung, ggf. auch Auftragsverarbeitung

Anwendungsfälle (2)

- Betreiben von „Fanpages“ im Rahmen eines Telemediendienstes (z.B. Facebook)

  Redaktionell Verantwortlicher lockt die „Fans“ (potenzielle Patienten und Beschäftigte) an und ermöglicht dem Plattformbetreiber damit erst die Verfolgung auch eigener Verarbeitungsziele mit den Besucherdaten - gewissermaßen eine *Sekundärnutzung*

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 (Art. 9 (4))
  - Krankenhausrecht
  - Sozialrecht
  - Berufsgeheimnisse

Beispiel I: LKG Berlin

Das Landeskrankenhausgesetz Berlin sieht seit dem 1. Januar 2023 einen (teilweise) neuen Umgang mit Auftragsverarbeitungen vor.

- Unterscheidung zwischen **reiner (Fern-)Wartung** mit Zugriffsmöglichkeit *aber* ohne aktiven Umgang mit den Daten (§ 24 Abs. 6 LKG Berlin) und
- **„echter“ Auftragsverarbeitung** (§ 24 Abs. 7 LKG Berlin)
  - Keine Drittlandverarbeitung ohne Angemessenheitsbeschluss
  - Ausdrückliche Pflicht zur Sicherstellung eines strafrechtlich (§ 203 StGB) angemessenen Rahmens bei Auslandsverarbeitung
  - Anzeigepflicht gegenüber der Fachaufsicht

Beispiel II: § 80 SGB X

Auftragsverarbeitung von Sozialdaten:

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)

Einflussmöglichkeiten

Art. 26 DS-GVO

- sieht keine Ausgestaltungsmöglichkeiten („Öffnungsklauseln“) für die Gesetzgeber vor,
- ist damit abschließend geregelt.
- Allerdings ist der Regelungsgehalt der Vorschrift nicht sehr dicht…

Berufsgeheimnisse I

Nach wie vor gilt:

- Weder Auftragsverarbeitung noch Gemeinsame Verantwortung bieten eine Offenbarungsbefugnis im Rahmen spezialgesetzlicher Geheimnisse gegenüber dem Dienstleister
- Seitens der DS-GVO keine Anhaltspunkte für eine andere Betrachtung

Berufsgeheimnisse II

Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (2017):

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

Berufsgeheimnisse III

- Offenbarung bei Auftragsverarbeitung innerhalb des § 203 StGB *im erforderlichen Umfang* erlaubt; Auftragsverarbeiter = „mitwirkende Person(en)“
- Erfordernis einer strafrechtlichen Schweigepflichtentbindungserklärung?
  - Nein
  - Artt. 13/14 sind zu beachten

Berufsgeheimnisse IV

- Erfordernis zur Verpflichtung des Dienstleisters, seine beschäftigten Personen auf den § 203 StGB zu verpflichten
- Zusätzliche Vertragsklausel, idealerweise im Art. 28-Vertrag

- Ist ein gemeinsam (Mit-)Verantwortlicher als mitwirkende Person anzusehen?

Berufsgeheimnisse V

Öffnung der Ärztlichen Berufsordnungen für mitwirkende Personen i.S.d. § 203 StGB (2018):

- Ergänzung im § 9 Abs. 4 MBO-Ä
- Damit ist eine Offenbarung im Rahmen der Inanspruchnahme von Dienstleistern zulässig.

Zugleich: Erfüllung der Anforderungen des Art. 9 Abs. 3 DS-GVO in Bezug auf Geheimnisverpflichtung

Berufsgeheimnisse VI

Aber:

- Einschränkung der Privilegierung der AV durch § 12 Abs. 2 der MBO-Ä in Bezug auf *Abrechnung*
- Für eine AV in Sachen Abrechnung ist nach wie vor eine Einwillligung/Schweigepflichtentbindung des Patienten erforderlich

➢ Systemfremd; nur Forderungsabtretungen gemeint? - kein Hinweis auf eingeschränkte Geltung, also auch bei der AV

Restrisiko bei der AV

Folgende Regelungen stehen einer Offenbarung innerhalb einer AV ggf. entgegen:

- *Explizit*: Berufsordnungen (Ärztliche)

  (in ggf. unterschiedlichem Maße)

- *Implizit*: AV ins Ausland… oder gar in Drittstaaten?

  (Reichweite national-strafrechtlichen Schutzes?)

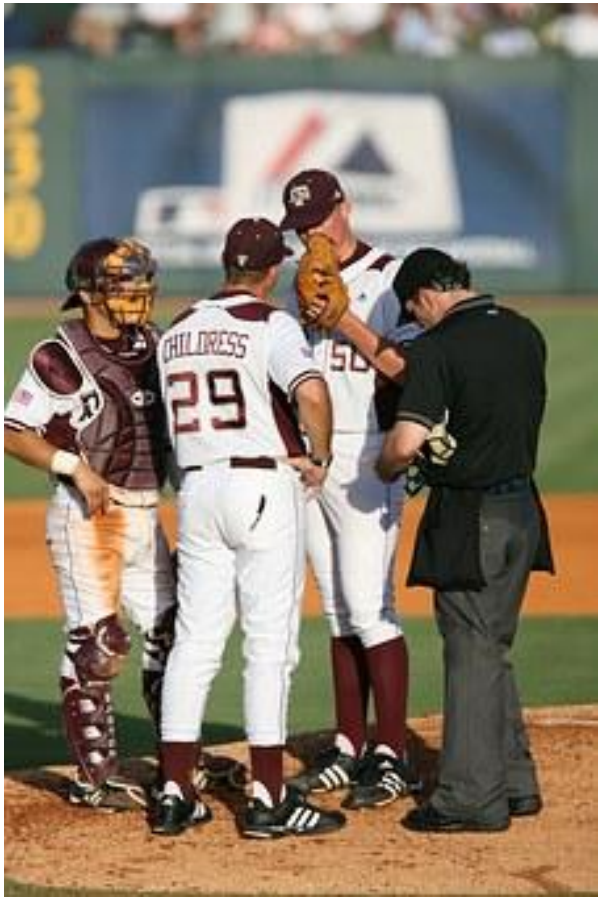
Zum Nachlesen:

Kurzpapier Nr. 13 der Datenschutzkonferenz:
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf
mit Hinweisen zur Anwendbarkeit in den Anhängen.

Orientierungshilfe des Bayerischen Landesbeauftragten für den Datenschutz:
https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf

Guidelines 07/2020 on the concepts of controller and processor in the GDPR:
https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

Noch Diskussionsbedarf?



Quelle: pixabay.com