BayLDA

Bayerisches Landesamt für Datenschutzaufsicht

Neues aus der TELEMEDIZIN

Andreas Sachs

Wiesbaden, 07. Mai 2019

Wer steht vor ihnen

Andreas Sachs

ist Informatiker, Leiter des Referats „Cybersicherheit & Technischer Datenschutz“ und Vertreter des Präsidenten beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) in Ansbach.

Einige Schwerpunktthemen

Datenpannen & Hacking

Trackingverfahren

Privacy by Design

Automotive

IT-Sicherheit

Datenschutzfolgenabschätzung

Verschlüsselungsverfahren

Zertifizierung

Rechenschaftspflicht

Telemedizin – Was ist das?

- **Medizinische Versorgung** und Betreuung von **Patienten** unter Einsatz modernster **Kommunikationsmittel** und **IT-Technik**
- Umfasst Diagnostik, Therapie und Rehabilitation
- Es werden **besondere personenbezogene Daten** nach Art. 9 DS-GVO verarbeitet

Telemedizin – Warum?

- **Optimierung** der Abläufe der ärztlichen Versorgung
- Reduzierung von **Wartezeiten**
- Ist für Patienten **bequemer**
- Reduzierte **Anfahrtswege**
- Kann die ärztliche Versorgung **verbessern**
- Kann **Kosten** reduzieren

Telemedizin – Anwendungsfelder?

Kein ganz trennscharfe Abgrenzung, z.B.:

- *Elektronische **Gesundheitskarte***
- ***Telematikinfrastruktur***
- *Elektronischer **Arztbrief***
- Elektronische **Kommunikation** (inkl. Apps)
- **Videosprechstunde**
- **Sensorüberwachung** (z.B. Herzschrittmacher)
- ***Vernetzung** von Krankenhäusern (z.B. Teleneurologie)*

Beispiel 1: Videosprechstunde

Quelle: www.aerzteblatt.de

Sog. **eHealth-Gesetz** gestattet seit 2017 den Einsatz von **Videosprechstunden**

Deutscher Ärztetag hat am 10.05.2018 eine **Lockerung** des sog. „**Fernbehandlungsverbots**“ beschlossen
Nachbehandlung sowie
(unter bestimmten Voraussetzungen) auch ausschließliche Fernbehandlung möglich

Dem flächendeckenden Einsatz steht nichts mehr im Weg.
Heute: **Anforderungen der DS-GVO**

Anpassungen des Berufsrechts, StGB sowie Neuerungen der DS-GVO zu **Dienstleistern**

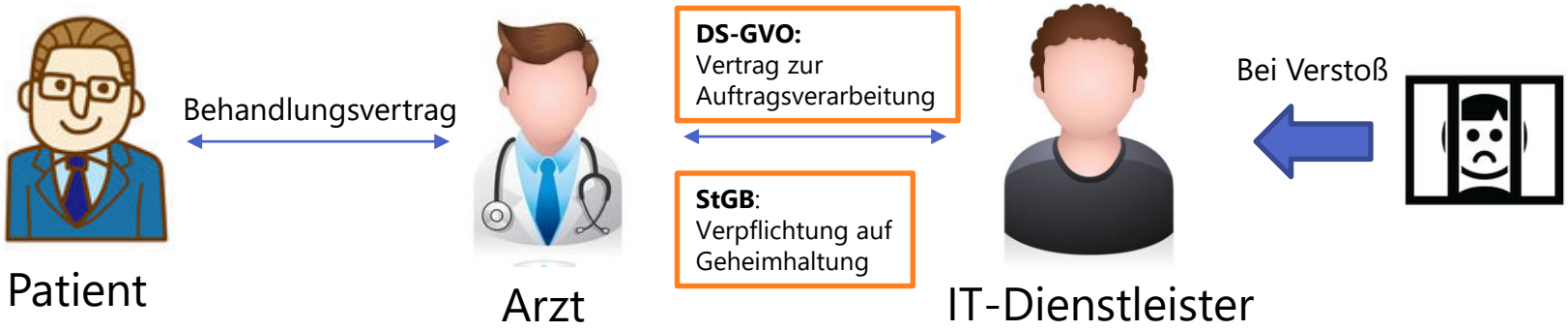
Kurzer Einschub: Einsatz von Dienstleistern

Änderungen des Strafgesetzbuches (§ 203 StGB):

- **Bisher**: Weitergabe von Privatgeheimnissen an „**berufsmäßig tätige Gehilfen**“
- **Bisher**: **IT-Dienstleister** und Auftragsverarbeiter fielen **nicht** darunter
- **Bisher**: **Theoretisch** blieb dann nur die **Einwilligung** übrig

- **Neu**: „Fremde Geheimnisse“ können auch gegen „**sonstige mitwirkenden Personen**“ offenbart werden, sofern **erforderlich**
- **Neu**: Es können auch **Subdienstleister** eingesetzt werden
- **IT-Dienstleister/Auftragsverarbeiter** können sich bei Verstößen auch **strafbar** machen
- **Neu**: **Pflicht zur Geheimhaltung** muss vom Arzt auf die Dienstleister(kette) **übertragen** werden

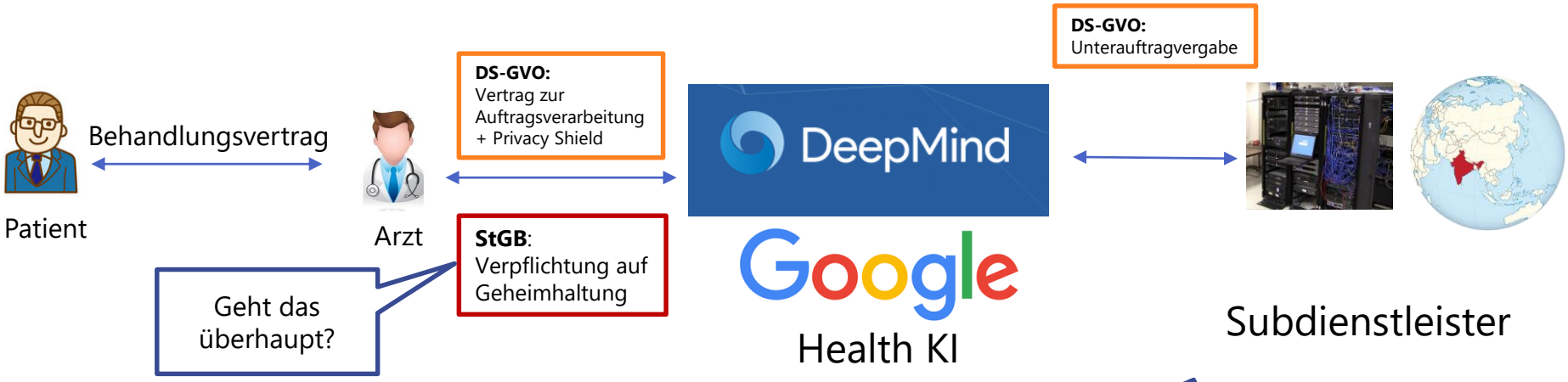
Kurzer Einschub: Einsatz von Dienstleistern – Gedankenspiel?

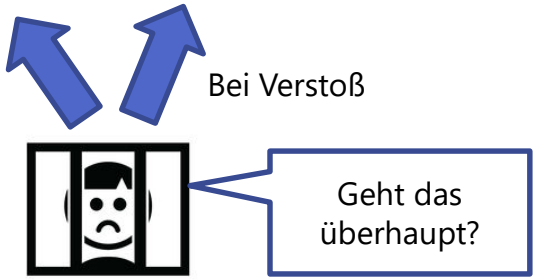


Bewertung:

- Spiegelt die Realität vom Einsatz von IT-Technik bei medizinischer Versorgung wieder
- Mehr Rechtssicherheit für Ärzte
- IT-Dienstleister im Gesundheitsbereich werden sich weiter professionalisieren

Kurzer Einschub: Einsatz von Dienstleistern – Gedankenspiel?





Bewertung:

- **Datenschutzrechtlich** können AV-Verträge mit unsicheren Drittstaaten geschlossen werden (= Keine Übermittlung an Dritte)
- **Relevanter Auswahlfaktor: Art. 25 DS-GVO** (Datenschutz durch Technikgestaltung)
- Übernehmen die **Firmen** die Verpflichtung auf **Geheimhaltung** nach StGB?
- Wie kann z.B. der Subdienstleister in Südindien **strafrechtlich ermittelt/belangt** werden?
- Dürfen nach StGB dann nur deutsche Dienstleister (auch Sub-Dienstleister) eingesetzt werden?
- **Berufsordnungen** der Ärzte sind teilweise schon an Regelung des StGB angepasst.

Zur Beruhigung: KI-Analyse wohl keine Auftragsverarbeitung

DS-GVO:
Unterauftragvergabe

Verantwortlicher

Übermittlung i.d.R. durch **Einwilligung**

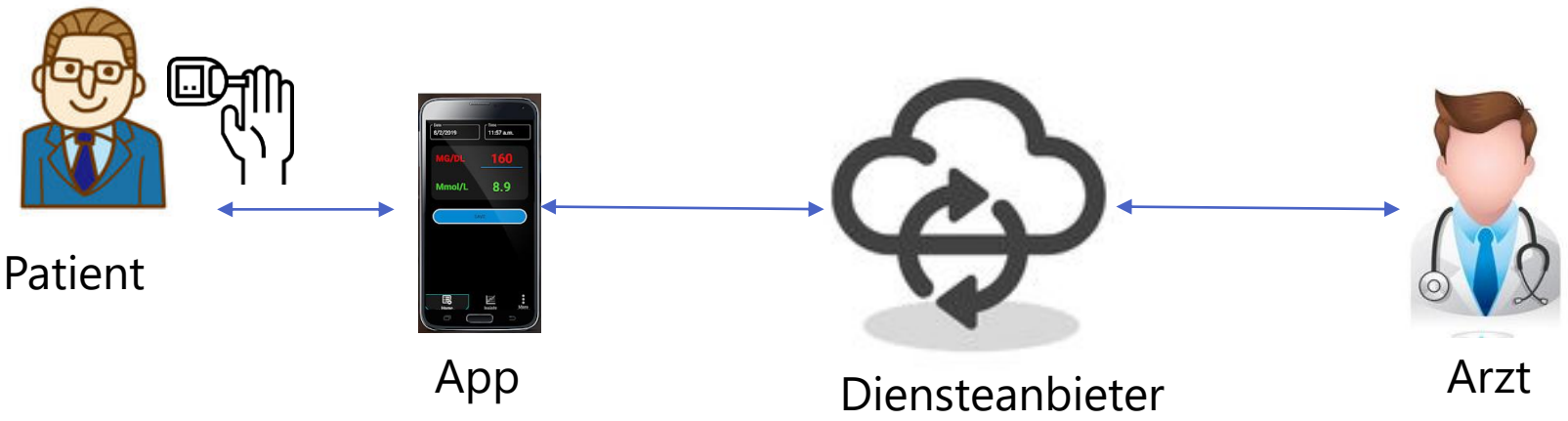
DeepMind

Google

Verantwortlicher

Großes Thema: Informations-pflichten

Beispiel 2: Sensorverarbeitung



- Anwendungsfelder z.B. Blutzuckerüberwachung, Schlafapnoe, Chronische Herzinsuffizienz,…
- Patient steuert (Senor-)Informationen bei
- Dienstanbieter vermittelt Kommunikation und stellt ggf. eigene Leistungen zur Verfügung
- Datenschutzrechtlich i.d.R. über Einwilligung des Patienten
- Besonderes Augenmerk auf Sicherheit der Verarbeitung

Beispiel 3: Telechirurgie

Quelle: www.ukaachen.de

- Vernetzung der **Leistungserbringer untereinander**
- **Fachexperten** können (in Echtzeit) **zugeschalten** werden
- **Patienten** sind **keine aktiven** Akteure
- **Herausforderungen**:
  - Sicherheit
  - Schnelle Netze (bei Operationen)

Grundlegende Fragestellungen

- Rechtsgrundlagen
- Datenschutz durch Technik
- Sicherheit der Verarbeitung
- Informationspflichten
- Datenschutzfolgenabschätzung
- Zertifizierung

Rechtsgrundlagen

- Es werden besondere personenbezogene Daten nach Art. 9 DS-GVO verarbeitet
  - Keine Interessenabwägung möglich
  - Gesetzliche Erlaubnisse, Verträge oder Einwilligung
  - Erhöhte Anforderungen an technische und organisatorische Maßnahmen

- Änderungen des Strafgesetzbuches / Berufsordnung zum Einsatz von Dienstleistern
  - Dienstleister(-ketten) möglich
  - Verpflichtung zur Geheimhaltung an Dienstleister übertragen
  - Drittlandstransfer auf Basis DS-GVO mittels AV-Vertrag möglich
  - Strafverfolgungsmöglichkeiten bei Drittlandstransfer unklar
  - Relevanter Auswahlfaktor von Dienstleistern: Art. 25 DS-GVO (Datenschutz durch Technik)

Datenschutz durch Technik

Art. 25 Abs. 1 DS-GVO
Datenschutz durch Technikgestaltung

Art. 32 DS-GVO
Sicherheit der Verarbeitung

Risikoorientierter Ansatz

Bestandteil der Rechenschaftspflicht

Art. 25-DS-GVO:

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 der mit der Verarbeitung verbundenen **Risiken** für die Rechte und Freiheiten natürlicher Personen

trifft der Verantwortliche sowohl zum **Zeitpunkt der Festlegung der Mittel** für die Verarbeitung als auch zum **Zeitpunkt der eigentlichen Verarbeitung**

geeignete **technische und organisatorische Maßnahmen** – wie z. B. Pseudonymisierung –, die dafür ausgelegt sind, die **Datenschutzgrundsätze** wie etwa Datenminimierung wirksam umzusetzen

und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und **die Rechte der betroffenen Personen** zu schützen.

Datenschutz durch Technik

Grundsätze der Verarbeitung (Art. 5 Abs. 1 DS-GVO)

- Rechtmäßigkeit und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Sicherheit der Verarbeitung
  - Art. 32 DS-GVO

Technische Komponente Art. 25 DS-GVO

Datenschutz durch Technik

Betroffenenrechte nicht vergessen (Art. 12 ff. DS-GVO)

- Transparente Information
- Rechte auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Einschränkung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Recht, keinem Profiling unterworfen zu sein (mit Ausnahmen)

Technische Komponente Art. 25 DS-GVO

Datenschutz durch Technik bei Telemedizin

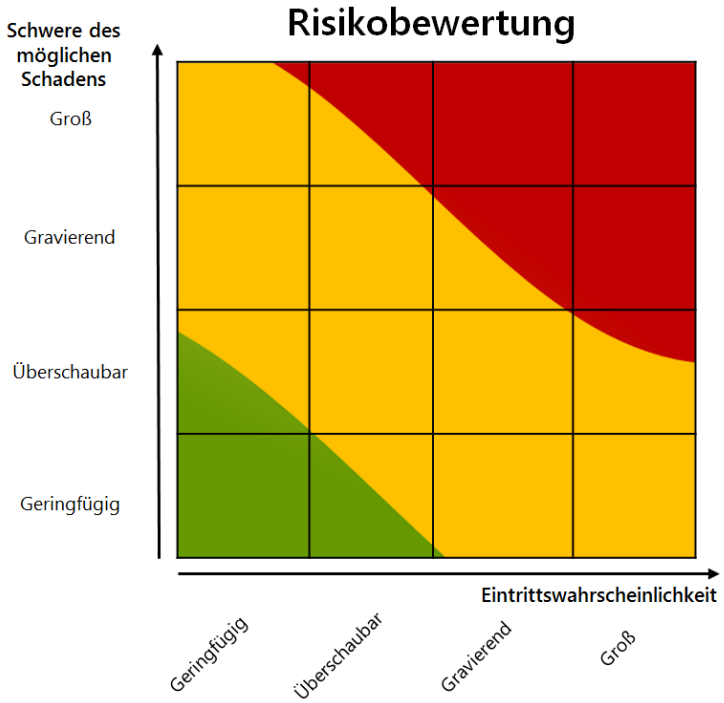
Anbieter/Betreiber von Telemedizin-Lösungen:

- Datenschutz muss schon Bestandteil einer System-/Produktentwicklung sein
- Fokus auf Einhaltung der Zweckbindung bei Forschung/Entwicklung – auch bei eigenen Dienstleistern
- Wünschenswert/Notwendig: Ende-zu-Ende-Verschlüsselung wo möglich
- Löschen/Sperren von Daten von Anfang an einplanen
- Betroffenenrechte Software-/Produktseitig unterstützen

Nutzer von Telemedizin-Lösungen:

- Sorgfältige Auswahl der Dienste/Produkte (Ausblick Zertifizierung)
- Interne Regelungen an Telemedizinlösungen anpassen
- Verarbeitungsverzeichnis aktualisieren

Verhältnis Art. 9 Daten und Risiko



Weitere Informationen im DSK-Kurzpapier „Risiko“ unter datenschutzkonferenz-online.de

Risikobestimmung anhand der Faktoren:

- Art, Umfang, Umstände, Zweck der Verarbeitung
- Schwere des möglichen Schadens
- Eintrittswahrscheinlichkeit des möglichen Schadens

⇒ Es liegt bei Art. 9 Daten **nicht immer** ein **hohes Risiko** vor.

Aber: Es liegt **i.d.R. bei Art. 9** ein **erhöhtes Risiko** und damit eine höhere Anforderung an TOM vor

⇒ Auswirkungen auf Durchführungspflicht einer DSFA
⇒ Damit auch auf die Bestellpflicht eines DSBs

Kurzer Einschub: Bußgelder bei technischen Verstößen

Ein Verstoß gegen Datenschutz durch Technikgestaltung kann mit bis zu 10 Mio. Euro / 2% Umsatz sanktioniert werden

Sicherheit der Verarbeitung

Sicherheit (Security) in der DS-GVO

Schutz vor Fehlhandlung

Schutz gegen Angriffe

Schutz vor Verlust

Sicherheit der Verarbeitung

30.10.2018 16:28 Uhr | Security

Vivy: Gravierende Sicherheitsmängel in Krankenkassen-App aufgedeckt

Die App, die bei Millionen von Versicherten und 16 Kassen im Einsatz ist, hatte schwerwiegende Sicherheitsmängel. Die Verantwortlichen sehen das anders.

Von Fabian A. Scherschel 221

28.03.2018 12:30 Uhr

Sicherheitslücken: Medizinische Geräte können gehackt werden

Medizinische Geräte wie Herzschrittmacher oder Insulinpumpen können gehackt werden – auch wenn die Gefahr gering ist. Anfälliger ist eher die IT in Krankenhäusern, die ein Einfallstor für Hacker zu medizinischen Überwachungsgeräten sein kann.

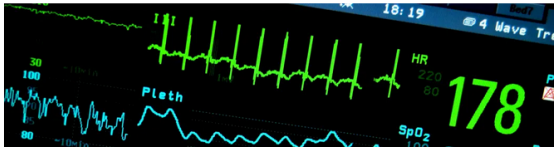
Von Andrea Barthélémy, dpa 36

24.04.2019 16:02 Uhr

Telematik im Gesundheitswesen: Freie Ärzteschaft warnt vor unsachgemäßer Konnektor-Installation

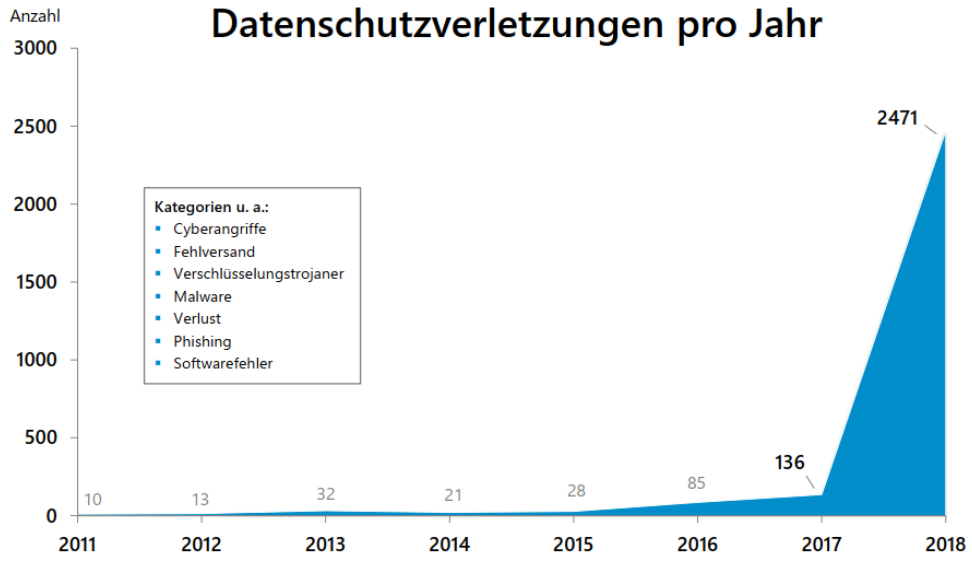
Techniker, die in Praxen Konnektoren für den Zugang zur telematischen Infrastruktur installieren, sollen häufig Firewalls und Virenschutzprogramme abschalten.

Von Detlef Borchers 79



- Es existieren reale Sicherheitsrisiken bei Anwendungen/Systemen im Gesundheitsbereich
- Art 32 DS-GVO fordert ein dem Risiko angemessenes Schutzniveau
- Bei „Verletzungen der Sicherheit“ kommt es gemäß Art. 33/34 zu einer Meldeverpflichtung
- Der Gesundheitsbereich gerät zunehmend in den Fokus von professionellen Cyberkriminellen

Sicherheit der Verarbeitung: Ransomware



Tätigkeitsbericht des BayLDA 2017/18

Das BayLDA erhält ca. 1-2 Ransomware-Meldungen/Woche

16.11.2018 14:47 Uhr

Fürstenfeldbruck: Malware legt Klinikums-IT komplett lahm

Im bayerischen Fürstenfeldbruck muss die örtliche Klinik seit Tagen fast komplett ohne Computer auskommen; verantwortlich ist Malware.

Von Martin Holland 762

Aktuelle Ransomware-Welle

Verschlüsselung teils erst in 3. Stufe:

1. Stufe: Angriff mit fortgeschrittener Malware (z.B. Emotet)
2. Stufe: Ermittlung des Bankguthabens
3. Stufe: Verschlüsselung und Lösegeldforderung in Höhe des Bankguthabens

Sicherheit der Verarbeitung bei Telemedizin

Anbieter/Betreiber von Telemedizin-Lösungen:

- Security muss schon Bestandteil einer System-/Produktentwicklung sein
- Einsatz eines Informationssicherheitsmanagementssystems (ISMS)
- Regelmäßige Schwachstellen-/Penetrationstests
- Sehr stringentes Patch-Management
- Incident-Respone-Planung und Übung
- Einsatz von Verschlüsselung/Pseudonymisierung zur Risikoreduzierung
- Regelmäßige Überprüfung/Verbesserung

Nutzer von Telemedizin-Lösungen:

- Geeignete Einbindung in eigenes Praxisnetz (ggf. (logische) Netztrennung)
- Sorgfältige Auswahl der Dienste/Produkte (Ausblick Zertifizierung)
- Bei mobilen Lösungen (Notebooks): Vollverschlüsselung und VPN-Anbindung
- Bei Nutzung von Videosprechstunde die Diskretion nicht vergessen

Datenschutzfolgenabschätzung

- Bei einem **wahrscheinlich hohen Risiko** muss eine DSFA nach Art. 35 DS-GVO durchgeführt werden
- Ist **Bestandteil der Rechenschaftspflicht** nach Art. 5 Abs. 2 DS-GVO
- **Schwellwertbestimmung** für hohes Risiko geht eng mit der **Restrisikobeurteilung** des Art. 25 DS-GVO einher
- Behauptung: Eine DSFA ist die **Ausnahme** statt der Regel
- Instrument zur **systematischen Risikobehandlung** bei Hochrisikoverarbeitungen
- Im Medizinbereich: Unbestimmter Rechtsbegriff „**umfangreich**“ („large scale“) relevant
- **Bestellpflicht eines DSB** bei Pflicht zur Durchführung einer DSFA

Datenschutzfolgenabschätzung

- Aufsichtsbehörden müssen Listen mit Verarbeitungen veröffentlichen, bei denen i.d.R. eine DSFA notwendig ist
- Diese Liste gibt es und wurde schon europäisch abgestimmt
- Es gibt momentan keine einheitliche europäische Liste

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
16	Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO - auch wenn sie nicht als „umfangreich" im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist - sofern eine nicht einmalige Datenerhebung mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen stattfindet und diese Daten von einer zentralen Stelle empfangen und aufbereitet werden.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Arzt nutzt ein Webportal oder setzt eine App an, um mit Patienten mittels Videotelefonie zu kommunizieren und Gesundheitsdaten durch Sensoren beim Patienten (z.B. Blutzucker, Sauerstoffmaske,...) detailliert und systematisch zu erheben und zu verarbeiten.

- Prämisse: innovative Anwendung / mobile Sensoren
- Zentrale Verarbeitung
- Bei Videosprechstunde i.d.R. keine DSFA-Pflicht

Zertifizierung

- **Problem heute**: Verantwortlicher darf Auftragsverarbeiter nur auswählen, wenn diese ihn unterstützen– insbesondere was die **TOM** angeht – die DS-GVO einzuhalten.
- **Lösung** DS-GVO: **Spezielle Zertifizierungen**, die Rechtswirkung haben
- Momentan Abstimmung der Kriterien bei den Aufsichtsbehörden
- Es können Privatunternehmen **akkreditiert** werden, die Zertifizierungen ausstellen
- Aktueller Stand: **Zertifizierung von Verarbeitungen** (beim Verantwortlichen(Auftragsverarbeiter) machbar, von reinen Produkten ohne Verabeitung personenbezogener Daten nicht
- **Prognose**: Ab 2025 werden nur noch Dienstleister mit DS-GVO Zertifizierungen eingesetzt

Zusammenfassung

- **Telemedizin** im Jahr 2019 ist aufgrund Änderungen der **rechtlichen** Rahmenbedingungen **möglich** geworden
- Die **DS-GVO** stellt einen (europaweit) geltenden **Schutzbereich** für **Gesundheitsdaten** auf
- Deutliche **Verschiebung** der Bewertung auf den **technischen Datenschutz**
- Technische Verstöße sind – neu - **bußgeldbewehrt**
- **Datenschutzfolgenabschätzung** nur bei Hochrisikoverarbeitungen, die es bei Telemedizin geben kann
- **Datenschutz durch Technik** ermöglicht es, Telemedizin rechtskonform und sicher einzusetzen und das Vertrauen der Patienten zu gewinnen
- **Zertifizierungen** werden die nächsten Jahre als hochwirksames Instrument zur Auswahl von Dienstleistern kommen

Vielen Dank für Ihre Aufmerksamkeit.

Zeit für Fragen?