Datenschutz in onkologischen Praxen und Zentren: Grundsätzliches sowie Änderungen durch die neue europäische Datenschutzverordnung

23.06.2018

Agenda

1. Ein neues Datenschutzrecht? Musste das wirklich sein?!
2. Anwendungsbereich der DSGVO?
3. Ändert sich denn überhaupt etwas?
4. Maßnahmen?

Die Workshopunterlagen und diverse weitere Informationen finden Sie auf unserer Website:

https://www.ecovis.com/datenschutzberater

Entwicklung der EU-DSGVO

Es war einmal…

Was es 1995 gab:

- **Umsetzung der Datenschutzrichtlinie 95/46/EG in nationales Recht**
- **In Deutschland: Bundesdatenschutzgesetz**
- **Eigenständige und unabhängige Datenschutzaufsichtsbehörden**
- **Unterschiedliche Bußgeldbestimmungen und -höhen**

Entwicklung der EU-DSGVO

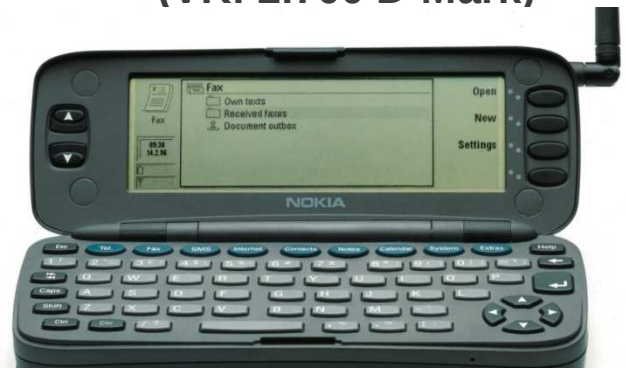
Es war einmal…

Was es 1995 noch nicht gab:

Entwicklung der EU-DSGVO

Es war einmal…

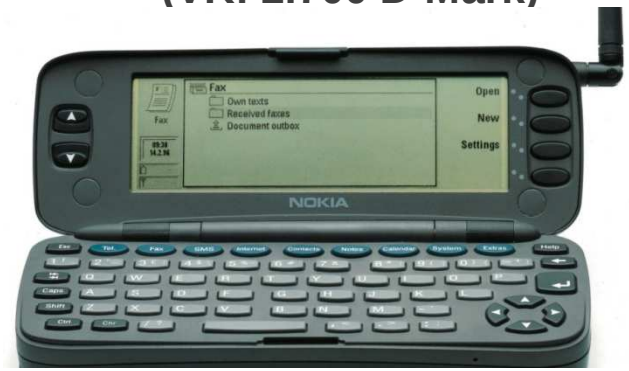
Nokia 9000 Communicator (VK: 2.700 D-Mark)



Entwicklung der EU-DSGVO

Es war einmal…

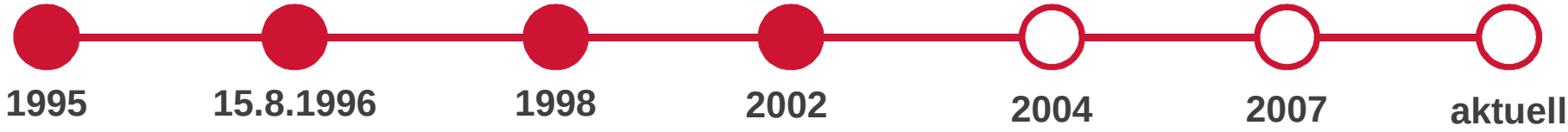
Nokia 9000 Communicator (VK: 2.700 D-Mark)



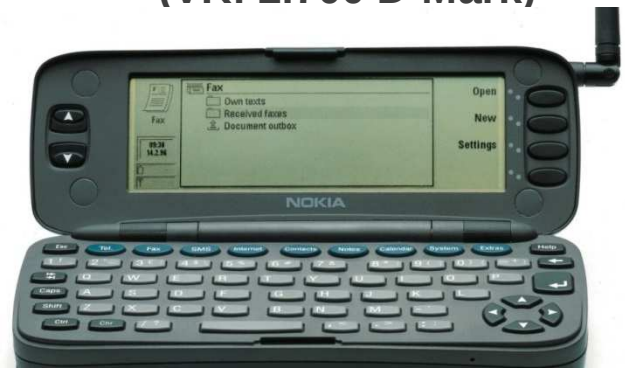
Google

Entwicklung der EU-DSGVO

Es war einmal…



Nokia 9000 Communicator (VK: 2.700 D-Mark)

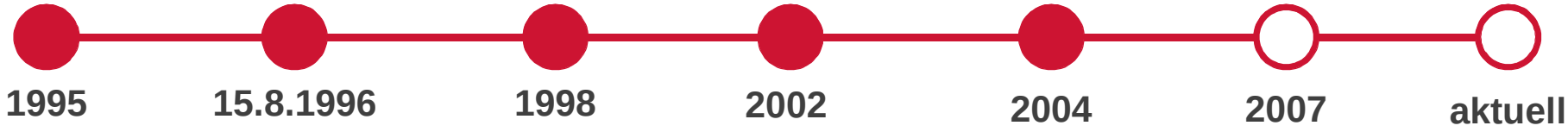


Google

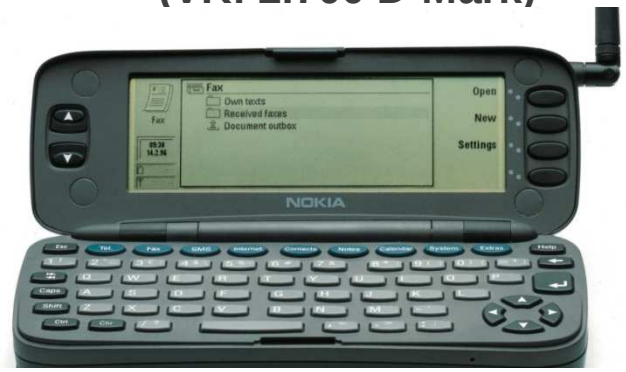
Blackberry

Entwicklung der EU-DSGVO

Es war einmal…



Nokia 9000 Communicator (VK: 2.700 D-Mark)



Google

Blackberry

Facebook

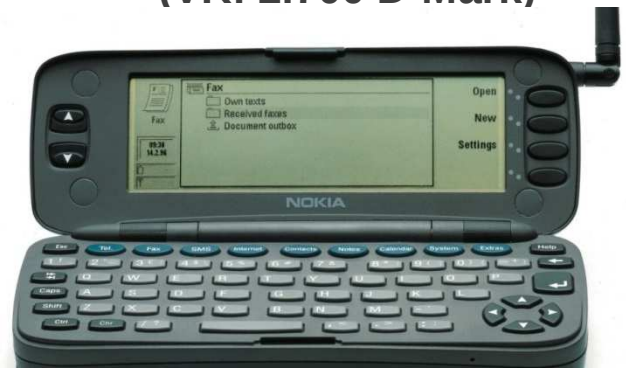
Entwicklung der EU-DSGVO

Es war einmal…

1995

15.8.1996

Nokia 9000 Communicator (VK: 2.700 D-Mark)



1998

Google

2002

Blackberry

2004

Facebook

2007

iPhone

aktuell

Google!

[theFacebook]

Entwicklung der EU-DSGVO

Es war einmal…

Seit 25.05.2018:

Datenschutz-Grundverordnung (EU-DSGVO)

- **Ziele**:
  - **Harmonisierung des Rechtsrahmens für den Datenschutz in Europa**
  - **Europaweite Koordination des Datenschutzes**
  - **Europaweite Koordinierung der Datenschutzaufsichtsbehörden**

- **Art. 8 EU-Grundrechtecharta**

> *Artikel 8*
>
> **Schutz personenbezogener Daten**
>
> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
>
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

- **Recht auf informationelle Selbstbestimmung (BVerfG)**

Anwendung der EU-DSGVO

Sachlicher Anwendungsbereich

- **Ganz / teilweise automatisierte Verarbeitung personenbezogener Daten**
  - Jede Verarbeitung mittels EDV, d. h. PC, Netzwerk mit Server, Notebook, Smartphone, Tablet, Videokamera, Kopierer…

- **Nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen**
  - Digitale Sammlungen personenbezogener Daten
  - Auch analoge, manuelle Sammlungen (Akten), wenn gleichartiger innerer oder äußerer Aufbau und Karteikarten

Anwendung der EU-DSGVO

Sachlicher Anwendungsbereich

- Personenbezogene Daten
  - Alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche Person** beziehen
  - Bei juristischen Personen – B2B-Geschäft: Ansprechpartner als nat. Personen bedenken

- Beispiele

- **Name**
- **Anschrift**
- **Geburtsdatum**
- Email (dienstlich & privat)
- Handynummer (dienstlich & privat)
- Hobby
- Beruf
- Lohn/Gehalt
- Bildungsstand, Kenntnisse, Fähigkeiten
- **Gesundheitszustand /Krankheit**
- Bewerberdaten, Zeugnisse
- Kundendaten, Patientendaten,
- Daten von Geschäftspartnern
- Mitarbeiterdaten
- Besitzverhältnisse
- steuerliche Verhältnisse

Anwendung der EU-DSGVO

Persönlicher Anwendungsbereich - Normadressat

- **DSGVO richtet sich an:**
  - die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle
  - die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

- **Das heißt**:
  - (Einzel-) Unternehmen, gleich welcher Rechtsform
  - Vereine
  - Arztpraxen
  - Pflegedienste
  - Krankenhäuser

Die DSGVO richtet sich an JEDEN, der außerhalb des rein privaten Bereichs mit personenbezogenen Daten umgeht.

Ändert sich überhaupt etwas?

Datenschutz – bislang kein Thema?! Doch!

§ 9 Schweigepflicht

(1) Der Arzt hat über das, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekannt geworden ist, – auch über den Tod des Patienten hinaus – zu schweigen. Dazu gehören auch schriftliche Mitteilungen des Patienten, Aufzeichnungen über Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.

(3) Der Arzt hat seine Mitarbeiter und die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.

§ 10 Dokumentationspflicht

(1) Der Arzt hat über die in Ausübung seines Berufes gemachten Feststellungen und getroffenen Maßnahmen die erforderlichen Aufzeichnungen zu machen. Diese sind nicht nur Gedächtnisstützen für den Arzt, sie dienen auch dem Interesse des Patienten an einer ordnungsgemäßen Dokumentation.

(3) Ärztliche Aufzeichnungen sind für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht.

(5) Aufzeichnungen auf elektronischen Datenträgern oder anderen Speichermedien bedürfen besonderer Sicherungs- und Schutzmaßnahmen, um deren Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern.

§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, … anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

Änderungen zum BDSGI

Rechtsgrundsätze der EU-DSGVO

- **Verbot mit Erlaubnisvorbehalt (Art. 6)**
    - Der Umgang mit personenbezogenen Daten ist verboten, es sei denn, ich habe eine Erlaubnis (gesetzliche Norm oder Einwilligung des Betroffenen)
- **Transparenzgebot (Art. 5 Abs. 1)**
    - Der Betroffene ist umfassend zu informieren.
- **Zweckbindung (Art. 5 Abs. 1)**
    - Ich darf die Daten nur zu dem Zweck verwenden, zu dem ich sie erhoben habe.

Änderungen zum BDSG

Rechtsgrundsätze der EU-DSGVO

- **Datensparsamkeit, Datenminimierung (Art. 25 Abs. 2)**
  - Ich darf nur diejenigen Daten erheben und behalten, die für den Zweck erforderlich sind.
- **Technische und organisatorische Maßnahmen zum Schutz der Daten (Art. 25 Abs. 1)**
  - Ich muss Maßnahmen zur Umsetzung der Datenschutzgrundsätze treffen. (Anonymisierung, Berechtigungs-, Zugriffs- und Zutrittskonzepte, Lese- und Zugriffsprotokollierung, Wiederanlaufplan etc.)
- **Es kommen neu hinzu:**
  - Nachweisbarkeit, „**Rechenschaftspflicht**“
  - Risikobewertungen, Bildung von Risikoklassen nach Art der Daten, Eintrittswahrscheinlichkeit eines Schadens und dessen Höhe („Risiko-Folgen-Abschätzung“)

Änderungen zum BDSG

Ein Kernpunkt der Reform ist die Einführung „starker Sanktionen“ bei Datenschutzverstößen, die „wehtun sollen“.

- **Bei Verstößen der Verantwortlichen und der Auftragsdatenverarbeiter gegen die Pflichten aus Art. 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43, z.B.:**
  - IT-Sicherheitsmanagement
  - Zusammenarbeit mit der Aufsichtsbehörde
  - Alle Vorschriften zur Auftragsdatenverarbeitung
  - Datenschutz-Folgeabschätzung (neu!)
  - **Datenpannen**

- **Höhe**
  - bis zu € 10.000.000 oder
  - bis zu 2% des gesamten, weltweit erzielten Jahresumsatzes
  - je nachdem, welcher der Beträge höher ist

Änderungen zum BDSG

- **Bei Verstößen gegen**
  - Grundsätze für die Verarbeitung, einschließlich Einwilligung
  - Rechte der betroffenen Personen
  - Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation
  - Alle Pflichten gemäß den Rechtsvorschriften der Mitgliedsstaaten, die aufgrund Öffnungsklausel erlassen wurden (bspw. Bestellung eines Datenschutzbeauftragten)
  - **Nichtbefolgen einer Anweisung der Aufsichtsbehörde**
  - **Nichtgewährung des Zugangs für die Aufsichtsbehörde**

- **Höhe**
  - bis zu € 20.000.000 oder
  - bis zu 4% des gesamten, weltweit erzielten Jahresumsatzes
  - je nachdem, welcher der Beträge höher ist

Maßnahmen

Wer benötigt einen Datenschutzbeauftragten?

- Bestellung **zwingend notwendig**, wenn (alternativ)
- **mindestens 10 Personen** im Unternehmen ständig mit automatisierter Datenverarbeitung beschäftigt sind
- Verarbeitungen erfolgen, die eine **Datenschutzfolgenabschätzung erforderlich** machen oder
- **Kerntätigkeit** in **umfangreicher** Verarbeitung **besonderer Kategorien von Daten** besteht
  - **Genetische Daten / Biometrische Daten / Gesundheitsdaten**
  - Beispielsweise Krankenhäuser, (Gen-)Labors, Familienberatungsstellen, Dienstleister im biometrischen ID-Management

– **Namentlich Meldung des DSB an Aufsichtsbehörde (derzeit nicht möglich)**
- **Fachliche Qualifikation notwendig, besonderer Kündigungsschutz**
- **Nicht: Praxisinhaber, Geschäftsführer etc.**

Brauchen Niedergelassene immer eine DSB?

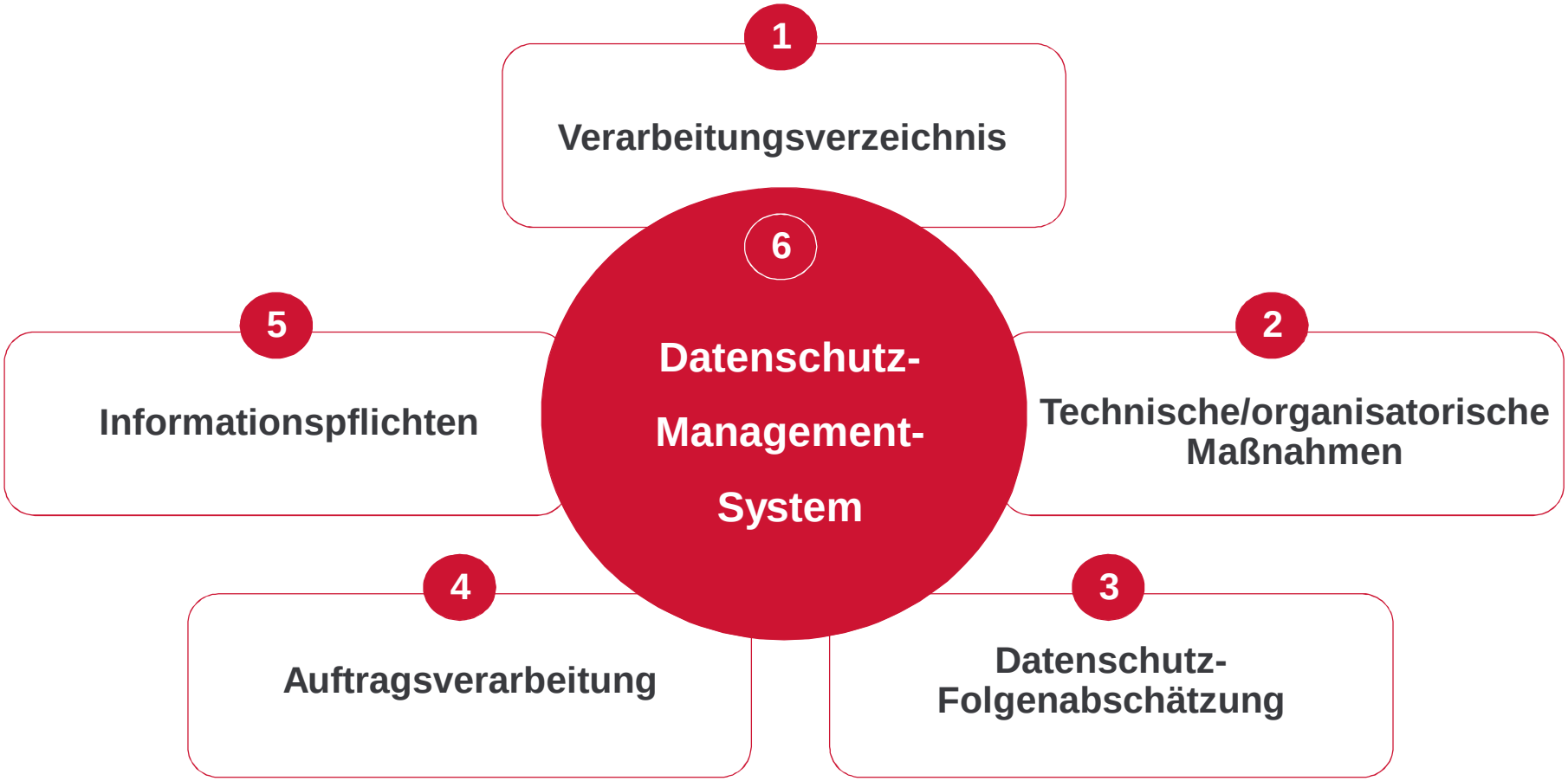
– Problem: Definition des **Umfangs** der Verarbeitung **besonderer Kategorien von Daten**

„Die Verarbeitung personenbezogener Daten sollte **nicht** als umfangreich gelten, wenn die Verarbeitung personenbezogener Daten von Patienten betrifft und durch einen **einzelnen Arzt oder** sonstigen Angehörigen eines Gesundheitsberufes erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein."

Derzeit keine klaren Aussagen vorhanden

- **Lieber auf Nummer sicher gehen soweit weniger als 10 Mitarbeiter vorhanden**

Datenschutz-Management-System (DSMS) mit seinen Bausteinen



- **Nachweispflicht!**

DSMS mit seinen Bausteinen

1. Verarbeitungsverzeichnis

Überprüfung aller Verarbeitungsvorgänge: elektronisch + Karteidaten!
Welche Daten werden überhaupt verarbeitet?

- Das Verarbeitungsverzeichnis dient dem Nachweis der Einhaltung der DSGVO
- Sämtliche Verarbeitungen personenbezogener Daten werden hier dokumentiert,

  z.B. Einsatz des Praxisverwaltungssystems

  Verarbeitungen sind automatische oder nichtautomatische Verfahren bzw. Vorgänge im Zusammenhang mit personenbezogenen Daten (Erheben, Erfassen, Ordnen, Speichern, Anpassen, Verändern, Verwenden, Offenlegen, Übermitteln, Abfragen, Lösen, Verknüpfen etc.).

- Das Verzeichnis ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen (Art. 30 Abs. 4 DSGVO)

Das Verarbeitungsverzeichnis ist künftig das zentrale Element einer ordnungs-gemäßen Datenschutzdokumentation!

DSMS mit seinen Bausteinen

2. Technische und organisatorische Maßnahmen

- Dienen der Vorbeugung, Minimierung und Behebung von Mängeln und Risiken bei der Verarbeitung personenbezogener Daten
- Technische und organisatorische Maßnahmen nach Art. 30 Abs. 1 DSGVO:
  - Pseudonymisierung und Verschlüsselung personenbezogener Daten
  - Gewährleistung von Integrität, Vertraulichkeit, Verfügbarkeit, Belastbarkeit der Systeme und Dienste
  - Wiederherstellung der Verfügbarkeit personenbezogener Daten nach technischen oder physischen Zwischenfällen
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluation der Wirksamkeit der Maßnahmen
- Technische und organisatorische Maßnahmen müssen anhand des Art. 5 Abs. 2 DSGVO dokumentiert werden (Rechenschaftspflicht)

DSMS mit seinen Bausteinen

Beispiele für techn./org. Maßnahmen

Pseudonymisierung

- Festlegung der durch Pseudonymisierung zu ersetzenden identifizierbaren Daten
- Definition der Pseudonymisierungsregel, zufällige Erzeugung der Zuordnungstabellen

Verschlüsselung

- Schlüssel können für die Dauer des Kommunikationsvorgangs oder mittel- bis langfristig eingesetzt werden
- Festlegung zur Auswahl geeigneter kryptografischer Verfahren

Maßnahmen zur Gewährleistung von Integrität und Vertraulichkeit der Systeme und Dienste

- Formulierung von Sicherheitsleitlinien
- Zugriffskontrolle und sicherer Umgang mit Speichermedien

Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste

- Sicherheitskopien von Daten, Prozesszuständen, Transaktionshistorien…
- Schutz vor äußeren Einflüssen

Wiederherstellung bei Zwischenfällen

- Notfallkonzept, -handbuch erstellen

Überprüfung, Bewertung, Evaluierung der Wirksamkeit der Maßnahmen

- Audits, Zertifizierungen, externe Prüfungen

Weitere Maßnahmen:

- Einschränkung der Nutzungsrechte
- Protokollierung von Zugriffen
- Transparenz- und Rechenschaftspflicht durch weitreichende Dokumentation

DSMS mit seinen Bausteinen

3. Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch (Art. 35 Abs. 1 DSGVO)

- Notwendigkeit einer Datenschutz-Folgenabschätzung bei besonders hohen Risiken nach Art. 35 Abs. 3 DSGVO:
  - Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient
  - Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 oder Art. 10 DSGVO
  - Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

DSMS mit seinen Bausteinen

4. Auftragsverarbeitung

Auftragsverarbeiter sind natürliche oder juristische Personen, eine Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- Jeder Auftragsverarbeiter führt ein Verzeichnis der Verarbeitungstätigkeiten, die er im Auftrag eines Verantwortlichen übernommen hat.
- Grundlage der Zusammenarbeit von Verantwortlichen und Auftragsverarbeiter ist ein Vertrag mit zwingenden Inhalten:
  - Personenbezogene Daten dürfen vom Auftragsverarbeiter nur auf dokumentierte Weisung des Verantwortlichen verarbeitet werden
  - Verpflichtung der mit der Bearbeitung befassten Personen auf die Vertraulichkeit oder gesetzliche Verschwiegenheitsverpflichtung muss gewährleistet werden
  - Einsatz von Subunternehmern bedarf der Zustimmung des Auftraggebers
  - Sicherheit der Datenverarbeitung (technische und organisatorische Maßnahmen) müssen eingehalten werden
  - Löschung / Rückgabe aller Daten bei Beendigung des Auftrages (wenn keine gesetzliche Aufbewahrungspflicht besteht)

DSMS mit seinen Bausteinen

5. Informationspflichten des Verantwortlichen ggü. Betroffenen (Art. 12ff. DSGVO)

- **Differenzierung nach Ort der Erhebung**
  - Erhebung bei dem Betroffenen
  - Erhebung bei Dritten
- **Inhalt** (unter Anderem)
  - Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten, Zwecke der Datenverarbeitung, Kategorien der erhobenen Daten, Empfänger oder Kategorien von Empfängern dieser Daten, Dauer der Speicherung, ggfls. Berechtigte Interessen des Verantwortlichen für die Datenverarbeitung
  - Bestehen der Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Möglichkeit des Widerrufs der Einwilligung, Bestehen des Beschwerderechts bei der Aufsichtsbehörde)
  - Quelle, aus der die personenbezogenen Daten stammen
  - beabsichtigte Zweckänderung

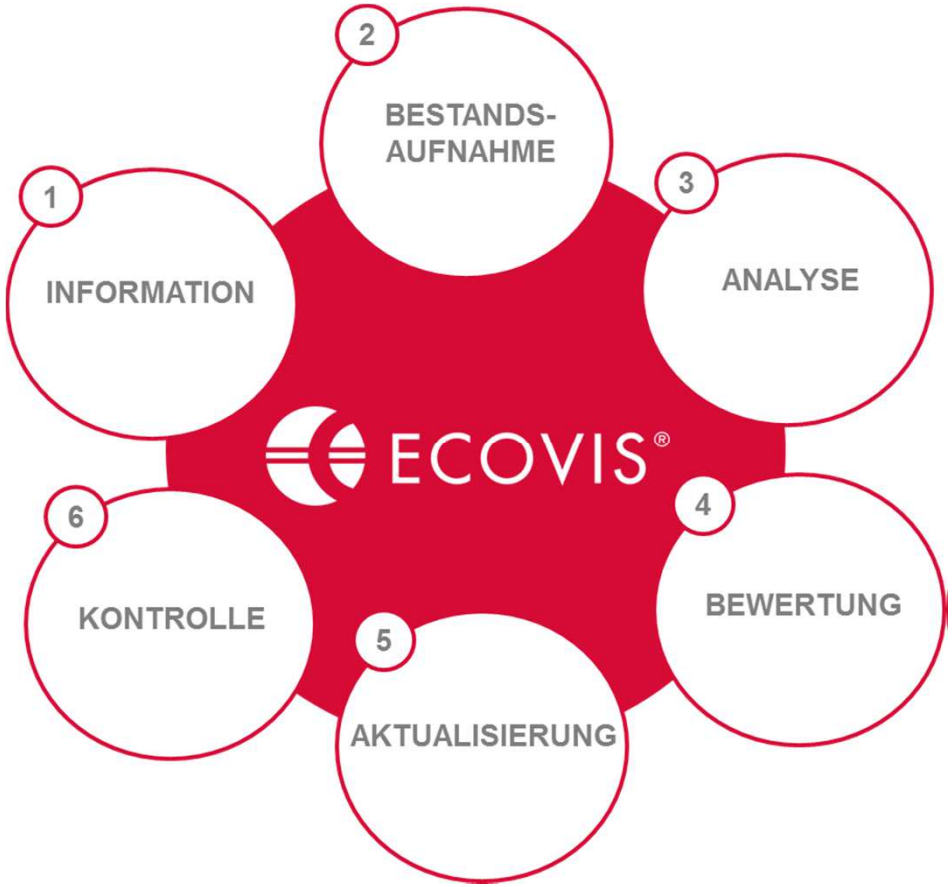
Abmahnung bei unzureichender Datenschutzerklärung?!

Insbesondere nach § 3a UWG – Informationspflichten sind Marktverhaltensregelungen

- **Internetauftritt anpassen!**

DSMS mit seinen Bausteinen

6. Datenschutz-Management-System / Datenschutzrichtlinie



Sensibilisierung der Ärzte und Mitarbeiter

➢ **interne Handreichung sinnvoll**

- Verhalten bei Erfassen von Patientendaten
- Verhalten im Wartebereich
- Auskünfte per Telefon
- Dürfen Partner immer mit zum Arztgespräch?
- Wer ist in der Praxis für den Datenschutz verantwortlich?
- Wer darf Rezepte oder Befunde abholen?
- Keine Patientendaten, -namen oder Fotos von der Kartei/Arztbriefe/Röntgenbilder etc. über WhatsApp versenden!

Patient und DSGVO

- **Einwilligung für besondere Datenverarbeitungsvorgänge**
  - **Routinemäßige Behandlung beruht meist auf gesetzlicher Grundlage, z.B. SGB V**

➡ **Keine Einwilligung zur Datenverarbeitung nötig, z.B. bei Abrechnung KV; Gutachten durch MDK**

  - **Abrechnung über private Verrechnungsstelle, Weitergabe Blutprobe an externes Labor**

➡ **Einwilligung nötig**

  - ➢ **Vorliegen von Einwilligungserklärungen muss nachgewiesen werden können**

- **Information der Patienten über Datenverarbeitung in verständlicher und leicht zugänglicher Form**

  z. B. durch Aushang im Wartebereich, Vordrucke

Einsichts- und Auskunftsrecht

- **Auch bisher schon: § 630g BGB**

  Einsichtsrecht in (vollständige) Patientenakte

- **Datenschutzrechtliches Auskunftsrecht: Patient kann jetzt unverzügliche Auskunft zu den über seine Person gespeicherten Daten verlangen**

- **Recht des Patienten auf Datenübertragbarkeit: betrifft Daten die vom Patienten auf Basis einer Einwilligung selbst zur Verfügung gestellt wurden und elektronisch verarbeitet werden**

Aufbewahrungs- und Löschungsfristen

Ärztliche Aufzeichnungen sind für mind. 10 Jahre nach Abschluss der Behandlung aufzubewahren, § 10 Abs. 3 Berufsordnung. Längere Fristen gesetzlich möglich, z.B. Röntgenaufnahmen.

Patienten haben Recht auf Berichtigung unrichtiger, personenbezogener Daten in der Patientendokumentation. Aber nur bezüglich Tatsachen (z.B. Größe, Gewicht). Ärztliche Bewertungen können nicht berichtigt werden.

Patient hat Anspruch auf unverzügliche Löschung der Daten, wenn die Daten nicht mehr benötigt werden oder die Einwilligung in die Verarbeitung widerrufen wurde. Vor Ablauf der 10-Jahresfrist tritt an die Stelle der Löschung eine Sperrung.

Externe Dienstleister und DSGVO

z. B. EDV-Wartung, private Verrechnungsstellen

- Auftragsverarbeitungsvertrag gem. Art 28 III DSGVO unter Beachtung der ärztlichen Schweigepflicht

Wie verhalte ich mich gegenüber der Aufsichtsbehörde?

-> nur eingeschränkte Rechte gegenüber sogenannten Berufsgeheimnisträgern

- **keine umfassende Auskunft über Patientengeheimnisse**
- **nur beschränkte Betretungsrechte im Rahmen der Schweigepflicht**
- **kein Durchsuchungsrecht ohne richterlichen Beschluss!**
- **keine Pflicht zur Selbstbelastung: bei Zweifel, ob gegebenenfalls Schweigepflicht verletzt wurde erst Rechtsrat einholen!**
- **Datenpannen (z. B. Hackerangriff, aber auch falscher Faxempfänger) sind binnen 72 Stunden der Aufsichtsbehörde zu melden (Online-Formular)**

Fraglich: Muss auch ein Verstoß gegen die Schweigepflicht als Datenpanne gemeldet werden (z. B. Auskunft über Gesundheitszustand an Kinder des Patienten)?

Aber: generelle Auskunftsverweigerung unter Berufung auf Schweigepflicht nicht ratsam (Bußgeld möglich)

Sehr gerne vertreten wir Ihre Interessen

ECOVIS L+C Rechtsanwaltsgesellschaft mbH

mit den Niederlassungen in

Landshut

ECOVIS L+C Rechtsanwaltsgesellschaft mbH
Podewilsstraße 3 - 84028 Landshut
Tel.: +49 871 96216-25
Fax: +49 871 96216-27

Regensburg

ECOVIS L+C Rechtsanwaltsgesellschaft mbH
Osterhofener Straße 10/III - 93055 Regensburg
Tel.: +49 941 79969-86
Fax: +49 941 79969-88

Memmingen
München
Nürnberg
Leipzig
Weiden