Pegamed 2019

Folie 1

Früher war Datenschutz Ländersache. Seit Mai 2018 gibt es einen europäischen einheitlichen Datenschutz. Dies erleichtert wesentlich den innereuropäischen Handel und gibt dem EU Bürger überall transparente und durchschaubare Rechte. Selbst außereuropäische Lieferanten müssen sich bei Lieferungen in die EU den europäischen Datenschutzgesetzen unterwerfen.

Das Recht auf seine eigenen Daten, ist in der EU-Charta als Menschenrecht verankert und wird in der DSGVO zum Gesetz, das die Rechte der Dateninhaber und die Pflichten der Daten-Verarbeiter beschreibt, mit Sanktionen bei Nicht-Einhaltung der Pflichten mit Geld- bis Gefängnisstrafen.

Die DSGVO ist ein „Verbraucherschutzgesetz“.

Schwerpunkt dieses Vortrages ist die

- Aktuelle Bedrohungen und die Präventionen dazu
- Datenschutz-Grundlagen
- Rechte des Betroffenen mit Umsetzungsregeln für die Arztpraxis
- Vertragliche Bindung aller internen und externen Partner

Mit dieser Schulung folgen wir der DSGVO, dass diese Aufgabe ausdrücklich gemäß Art.39 (1) b) dem Datenschutzbeauftragten aufgibt.

Folie 2

Zurzeit sind die Rechte dem Patienten noch nicht in aller Gänze bekannt.

Trotzdem müssen wir uns jetzt schon auf die Inanspruchnahme vorbereiten. Eine Missachtung kann zu empfindlichen Geldbußen führen.

Folie 3

Identitätsdiebstahl ist der häufigste Einstieg bei Datendiebstahl oder Verschlüsselung der Daten und Erpressung (Ransomware).
Das Einfallstor ist zu 90% ein E-Mail-Anhang oder gefälschte Absender.

Die **Know-How Hemmschwelle sinkt** durch preiswerte Angebote im Darknet, von **Standard-Ransomware, Ransomware-as-a-Service** oder **Ransomware-Partner-Programme.** Sie erleichtern den Einstieg für Cyber-Kriminelle. Unterstützend hierzu sind monetäre Technologien wie Bitcoin, die es den Strafverfolgungsbehörden praktisch unmöglich machen, Lösegeldzahlungen zu verfolgen.

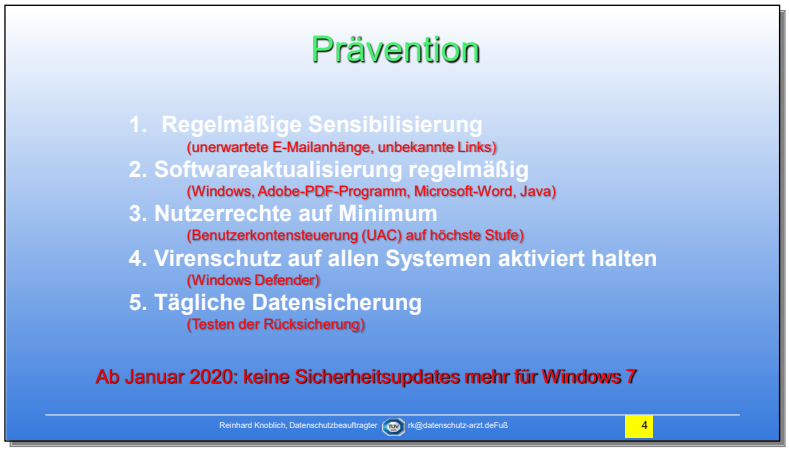
Doxing (neu)
Cyber-Kriminelle sind erfindungsreich. Einige von ihnen beschränken sich nicht nur darauf, die gesperrten Daten zu löschen, oder zu verschlüsseln, sondern drohen mit der Veröffentlichung (dem so genannten „Doxing"). Für Unternehmen, die mit privaten und sensiblen Kundendaten arbeiten, wie Finanzdienstleister, Krankenhäuser, Arztpraxen oder Anwaltsfirmen, kann dies katastrophale Konsequenzen haben. Sie verlieren nicht nur den guten Ruf ihres Unternehmens, sondern müssen ihre Kunden entsprechend den geltenden Datenschutzbestimmungen, über den Vorfall informieren und weitere umfangreiche Maßnahmen ergreifen, die schnell zu hohen Ausgaben führen können.

Trend
Wenn eine Cyber-Bedrohung innerhalb eines Jahres um das 35-fache wächst, sollte jedes Unternehmen gewarnt sein. Banken decken sich mit Bitcoins ein, damit ihre Kunden (und sie selbst) Cyber-Kriminelle gegebenenfalls schnell für das Entsperren gehackter Daten bezahlen können, da die Ausfallzeiten von Umsatz und Produktivitätsverlusten in einer Größenordnung von Tausenden und häufig Hunderttausenden Euro führen könnten.
Schutz der Daten in der EU-Charta
Wegen der immensen Abhängigkeit der Daten von Sicherheitsmaßnahmen und damit der Abwehr eines sozialen Schadens, oder gar einer sozialen Vernichtung, ist das **Recht auf Schutz** und **Recht auf eigene Bestimmbarkei**t seiner Daten in Europa als **Menschenrecht** in der EU-Charta aufgenommen worden:

Artikel 8 der EU-Charta:
Schutz personenbezogener Daten
Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
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.
Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Diese unabhängige Stelle ist die EU-Datenschutz-Grundverordnung (EU-DSGVO) mit seiner Aufsichtsbehörde.

Folie 4



Angriffsziel Mitarbeiter
Erfolgreiche Angriffe auf Unternehmen folgen meistens dem gleichen Muster. Erstes Angriffsziel ist der Mitarbeiter, der mit Social-Engineering-Methoden dazu gebracht wird, Anhänge oder Links in vermeintlich seriösen E-Mails zu öffnen. Der Schadcode nutzt dann eine bekannte Sicherheitslücke im Betriebssystem Windows oder in einer Anwendung, wie zum Beispiel Acrobat Reader, Word, Excel, usw. aus, um sich im Netzwerk auszubreiten und weiteren Schadcode nachzuladen und nach einer bestimmten Zeit der Analyse zuzuschlagen.

Gefährliche E-Mails sind kaum als solche erkennbar
Die E-Mails mit Trojaner Anhang stammen scheinbar von Kollegen, Geschäftspartnern oder Bekannten und sind kaum von echten E-Mails zu unterscheiden. Die Häcker haben ganze Adressbücher und Korrespondenzen erbeutet und erstellen auf der Basis dieser Informationen E-Mails, die dem normalen Kommunikationsverhalten des Unternehmens ähnlich sind. Bei den zuletzt beobachteten Kampagnen ging es vor allem um angebliche Rechnungen, anstehende Paketlieferungen oder Bewerbungsschreiben. Eine weitere Kampagnenversion setzte auf direkten URL-Download anstelle von Anhängen, um die Maleware ans Ziel zu bringen.

Die sechs Präventionsregeln:

1. Bewusstseins-Änderung: „Uns wird schon nicht passieren“. Gemäß Studien fallen 97% der Anwender auf schadhafte E-Mais rein. Früher oder später wird es passieren, die Frage ist wann. Daher Vorbereitung auf den Ernstfall!

2. Ständige **Sensibilisierung** und gegenseitiges aufmerksam machen bei der Benutzung von E-Mails, unerwartete Anhänge auch nicht zu öffnen, und entgegen der persönlichen Neugierde nicht auf unbekannte Links zu klicken.

3. Regelmäßige **Softwareaktualisierungen** vom Betriebssystem Windows, den Anwendungsprogrammen für PDF- und Word Dokumente und Systemsprachen die das Internet verwendet zum Beispiel Java.

4. **Nutzerrechte** auf Minimum einstellen: Nutzer sollten nicht mit Admin-Rechten arbeiten. Hierzu zählt auch, dass die Benutzerkontensteuerung (UAC) von Windows auf die höchste Stufe eingestellt wird.

5. Den **Virenschutz** auf allen Systemen aktiviert und aktualisiert halten.

6. Regelmäßige und tägliche **Daten-Sicherungen** aller Programmdaten: Es sollten dabei mindestens täglich unterschiedliche Datenträger verwendet werden. Da Datenträger altern und fehlerhaft werden, muss quartalsmäßig deren Qualität durch Rückspiele der Daten in ein Testsystem überprüft werden.

Achtung:

Ab Januar 2020 wird von Microsoft die Auslieferung von Sicherheits-Updates für Windows 7 eingestellt. Das bedeutet, dass danach auftretende Fehler in der Software nicht mehr behoben werden. Das ist für Hacker das Startsignal intensiv nach neuen Sicherheitslücken in Windows 7 zu suchen, um ihre Schad-Software dafür auszurollen. Ähnlich wie es bei dem Trojaner Loki und Windows XP passierte, als Krankenhäuser, Bahnhöfe und gesamte Produktionsstätten lahmgelegt wurden.

Folie 5

EU-Charta
Das Recht auf seine eigenen Daten, ist in der EU-Charta als Menschenrecht im §8 verankert und wird in der DSGVO zum Gesetz, das die Rechte der Dateninhaber und die Pflichten der Daten-Verarbeiter beschreibt, einschließlich mit Sanktionen bei Nicht-Einhaltung der Pflichten mit Geld- bis Gefängnisstrafen.

Vorrangsrecht
Durch sein Vorrangsrecht steht die DSGVO **über allen** nationalen Gesetzen!

Die EU-DSGVO und das nationale Recht
Die wichtigste Grundlage hierfür ist das EU-Recht, dass nach Rechtsprechung des EuGHs, Vorrang vor den jeweiligen nationalen Gesetzen hat. Somit müssen die Länder ihr nationales Recht so anpassen, **dass dem Unionsrecht nicht widersprochen wird**.
Die DSGVO gestützt auf Art. 16 Abs. 2 – verfolgt das Ziel einer Vollharmonisierung. Zugleich belässt sie den Mitgliedstaaten substanzielle Regelungsspielräume. Diese Handlungsspielräume ergeben sich aus den sogenannten Öffnungsklauseln.

Öffnungsklauseln
Die Öffnungsklauseln sollen den Mitgliedstaaten die Möglichkeit geben, nationale Regelungen einzubinden. Art. 6 Abs. 2, 3 und 4 (…) DSGVO
Damit fällt das Bundesdeutsche Datenschutzgesetz (BDSG) weg und wird durch das **Datenschutz-Anpassungs- und Umsetzungsgesetz (**DSAnpUG-EU) ersetzt, auch vereinfacht als „**BDSG neu**“ bezeichnet.

Folie 6

Das Datenschutzgesetz schützt den Betroffenen – Wer ist der Betroffene?
Die Datenschutzgesetze sind ausschließlich zum Schutze für die Daten von **natürlichen** und **lebenden Personen**, nicht für juristische Personen, z.B. GmbH, AG oder Institutionen, usw. Diese Person wird im Gesetz als **Betroffener** bezeichnet.
Verstirbt diese natürliche Person, so endet der Datenschutz. Ein rechtmäßiger Erbe kann die Daten nur dann übernehmen, wenn dies testamentarisch vom Verstorbenen verfügt worden ist.
Die ärztliche **Schweigepflicht** §203 Strafgesetzbuch bleibt jedoch bestehen. Dadurch kann der Fall eintreten, dass die Daten nicht offenbart werden dürfen. Außer es liegt ein testamentarischer Wille zur Aufhebung der Schweigepflicht vor.

Die Schweigepflicht kann allerdings durch Gerichtsbeschluss aufgehoben werden, oder durch den Arzt selbst, wenn bestimmte Umstände eintreten und er „im Wohle des Verstorbenen zu handeln reklamiert.
Neben dem Datenschutzgesetz bestehen also noch weitere Gesetze die eine Verschwiegenheits-Verpflichtungen beinhalten:
- Strafgesetzbuch → Berufsgeheimnis
- Telemediengesetz → Brief- E-Mail-Geheimnis
- Sozialgesetzbuch Sozialgeheimnis

Der Datenschutz regelt in der Hauptsache 3 Dinge:
- Die Verarbeitungs-Befugnis der Daten durch einen Treuhänder
- Die Pflichten und Verweildauer der Daten beim Treuhänder
- Die Rechte des Betroffenen während dieser Verweildauer

- **Die Verarbeitungs-Befugnis**

Daten zu verarbeiten ist nur dann erlaubt, wenn eine **Einwilligung** des Betroffenen vorliegt, oder ein **Gesetz** es erlaubt (Erlaubnisvorbehalt), sonst ist es verboten.
Beispiel für gesetzliche Erlaubnis-Gründe:
- Sozialgesetzbuch -> Abrechnung zur KV
- Röntgenverordnung -> Röntgenbefunde
- Krebsregister -> Krebserkrankungen
- Betäubungsmittel-Verschreibungsverordnung -> Substitutionsbehandlungen
- Reichsversicherungsordnung -> Unfallmeldung an BG
- Ansteckende Krankheiten nach Infektionsschutzgesetz -> Gesundheitsamt
- AU mit Diagnose -> Krankenkasse
- Geburt -> Standesamt
- Ärztliche Stellungnahme -> MDK
- Notstand -> Meldung an die Behörden bei Gefahren HIV-Infektion, Straftaten, Kinds-Misshandlung, Alkoholsucht

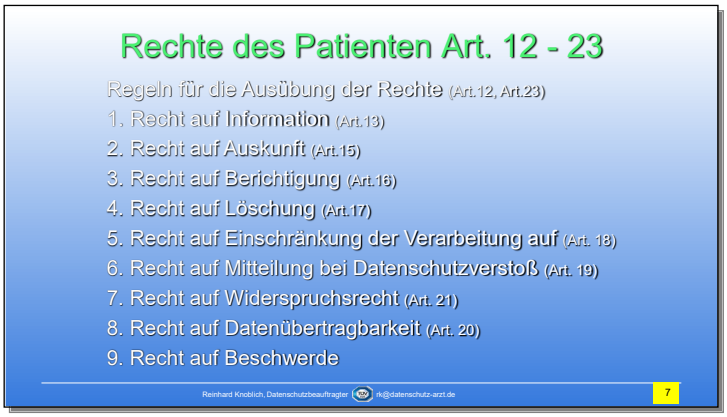
2. Pflichten und Verweildauer der Daten beim Verarbeiter/Treuhänder
Pflichten die dokumentiert werden müssen:
- Zweck und die Rechtsgrundlage der Datenverarbeitung

- Verarbeitungsmethoden in einem Verzeichnis auflisten
- Technische und organisatorische Maßnahmen zur Sicherstellung der Datensicherheit aufstellen und benennen
- Erfüllung der Betroffenen-Rechte sicherstellen

Daten müssen in der Regel nach **10 Jahren (Mindest-Zeitraum) gelöscht** werden, wenn nicht ein anderes Gesetz (BGB, Röntgengesetz, usw.) dagegenspricht. Aber spätestens nach 30 Jahre, wenn der Vorwand der Schadensersatz-Abwehr nach BGB wegfallen ist. Die Daten müssen aber während dieser Zeit von den anderen Daten isoliert und für den täglichen Gebrauch gesperrt werden.

3. Rechte des Patienten/Betroffener
- Recht auf Auskunft, welche Daten verarbeitet und an wen sie weitergegeben werden.
- Recht auf Löschung/Berichtigung seiner Daten
- Recht auf Bestimmung der Weitergabe seiner Daten, an eine andere Stelle, in einem standardisierten und maschinell lesbaren Format, so dass die andere Stelle die Daten übernehmen kann

Folie 7



Rechte des Patienten Art. 12 – 23

Die Rechte des Patienten sind zugleich Pflichten der Arztpraxis. Missachtung dieser Rechte sind ein Datenschutzverstoß.
Diese Rechte sind:
Regeln für die Ausübung der Rechte (Art.12)

1. Recht auf Information vor Datenerhebung (Art.13)
2. Recht auf Auskunft (Art.15)
3. Recht auf Berichtigung (Art.16)
4. Recht auf Löschung (Art.17)
5. Recht auf Einschränkung der Verarbeitung auf (Art. 18)
6. Recht auf Mitteilung bei Datenschutzverstoß (Art. 19)
7. Recht auf Datenübertragbarkeit (Art. 20)
8. Recht auf Widerspruch (Art. 21)
9. Recht auf Beschwerde bei der Datenschutzbehörde

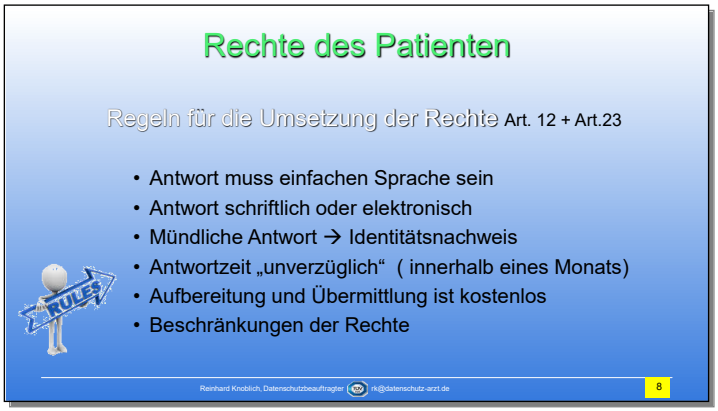
Folgende Rechte werden in Arztpraxen nur sehr selten vorkommen:

10. Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden (Art. 14)
Wurden die Patientendaten in der Arztpraxis erhoben, ohne dass der Patient darüber Bescheid wusste, so teilt die Arztpraxis dem Patienten folgendes mit:
Den Namen und die Kontaktdaten des Verantwortlichen (Arzt-Inhaber)
Zusätzlich die Kontaktdaten des Datenschutzbeauftragten
Die Zwecke für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung
Gegebenenfalls die Empfänger an die die Daten weitergereicht werden

11. Recht auf Unbetroffenheit von automatisierten Entscheidungen im Einzelfall einschließlich Profiling (Art. 22)
Manche Arzt-Systeme untersuchen im Hintergrund die Patientendaten auf Eignung zur Teilnahme an einer Studie und übertragen diese weiter. Dieser Prozess könnte eine automatisierte Entscheidung, oder ein sogenanntes Profiling sein, wie es Banken zur Feststellung der Kreditwürdigkeit tun. Dieser Vorgang wird zurzeit untersucht und der Datenschutzaufsichtsbehörde zur Beurteilung vorgelegt, inwieweit eine Einverständniserklärung notwendig, bzw. Anfechtungsrecht des Patienten besteht.

12. Gründe zur Beschränkung der Rechte (Art. 23)
Die Rechte, und damit auch die Pflichten, können eingeschränkt werden, wenn die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, usw. beeinträchtigt werden.

Folie 8



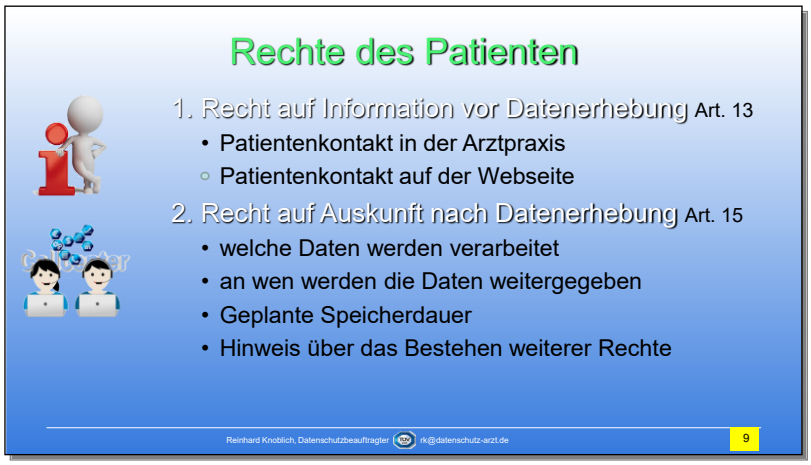
Regeln für die Ausübung der Rechte (Art. 12)

Der Patient muss über seine Rechte informiert werden.

- Die Ermöglichung der Rechte muss in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erläutert und realisiert werden. Dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.
- Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch.
- Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form (zum Beispiel: Ausweis) nachgewiesen wurde.
- Die Arztpraxis muss dem Rechtsbegehren innerhalb eines Monats nach Eingang des Antrags nachkommen. Diese Frist kann um weitere zwei Monate verlängert werden, wenn die Anzahl der Anträge ein Übermaß erreicht. Die Arztpraxis unterrichtet den Patienten innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde, oder einen gerichtlichen Rechtsbehelf einzulegen. Stellt der Patient den Antrag elektronisch, so ist er nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern er nichts anderes angibt.
- Kosten zur Bearbeitung dürfen nicht erhoben, die Informationen müssen unentgeltlich zur Verfügung gestellt werden. Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person kann der Verantwortliche entweder
- ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder
- sich weigern, aufgrund des Antrags tätig zu werden. Die Arztpraxis hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen.
- Beschränkungs-Gründe für Rechte (Art. 23)

Die Rechte, und damit auch die Pflichten, können eingeschränkt werden, wenn die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, usw. beeinträchtigt werden.

Folie 9



1. Recht auf Information vor Datenerhebung (Art.13)
Der Patient hat das Recht vor der Datenerfassung, umfangreich über die Verarbeitung seiner Daten informiert zu werden.

- Patienteninformationsblatt bei Erstkontakt zum Patienten: Die Information muss nicht unterschrieben werden, sie ist nur eine Information. Zur Dokumentation, dass informiert wurde, genügt ein Datumsvermerk in der elektronischen Patientenakte. Es besteht keine Pflicht diese in anderen EU-Sprachen anzubieten. Bei Kindern unter 16 Jahren müssen die Erziehungsberechtigten informiert werden.
- Können Daten, oder Nachrichten in einem Praxis-Webformular übermittelt werden, handelt es sich dabei bereits um eine Datenerfassung. Folglich muss der Patient über das WIE seiner Datenverarbeitung informiert werden. Zur Dokumentation genügt dort ein Bestätigungs-Haken und ein Link zu den Datenschutzerklärungen auf der Website. Danach dürfen die Daten erst zur Praxis übermittelt werden.

2. Auskunftsrecht nach Datenerhebung (Art.15)
Dem Informationsrecht korrespondiert ein Auskunftsrecht des Betroffenen. Dieser kann in angemessenen Abständen Auskunft über die Datenverarbeitung, vor allem über den Zweck, welche Daten verarbeitet werden und über weitere den Empfänger seiner Daten verlangen. Der Begriff „angemessene Abstände“ ist im Gesetz undefiniert und kann als „nicht mehr als einmal pro Jahr“ ausgelegt werden, oder ab einer wesentlichen Änderung der Daten.

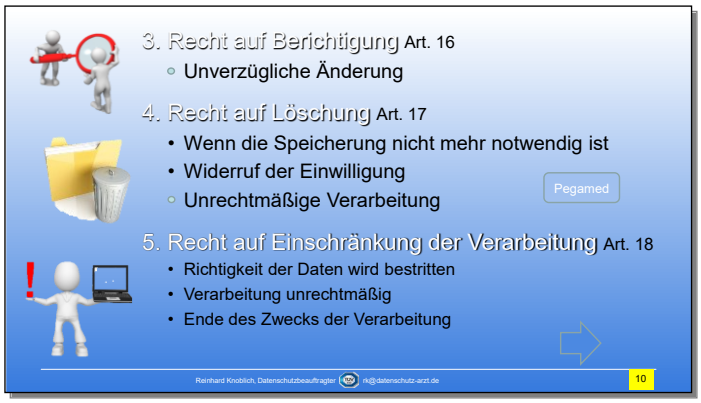
- Patientendaten:

Der Auskunftsumfang kann bedeuten, dass die gesamte Patientenakte auf Papier oder elektronisch ausgedruckt werden muss. Patientendaten sind Daten zur Dokumentationen über

- Anamnese
- Diagnose
- Therapie
- Fremdbefunde
- Soziale Einschätzungen und Beschreibungen über den Patienten
- Nicht Patientendaten sind:
- Leistungsziffern
- Bemerkungen zur Qualität von Medikamenten und Behandlungsmethoden
- Unter Umständen kann es Daten geben, die bei Bekanntwerden beim Patienten Beschwerden auslösen. Dann werden diese Daten nicht weitergegeben. Zum Beispiel: psychologische Befunde, oder Ergebnisse aus Therapiegesprächen von

Minderjährigen gegen ihre Eltern. Dies muss aber dann vom Arzt medizinisch begründet und dokumentiert werden.
- Auskunft an wen die Daten übermittelt wurden.
- Auskunft über die geplante Speicherdauer, bzw. wann die Daten gelöscht werden.
- Information über das Bestehen des Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung, Widerspruchsrecht gegen die Verarbeitung, Beschwerderecht bei der Aufsichtsbehörde.

Folie 10



3. Recht auf Berichtigung (Art.16)

Resultiert eine Datenverarbeitung in unrichtigen personenbezogen Daten des Patienten, so hat dieser ein Recht auf unverzügliche Berichtigung.

4. Recht auf Löschung (Art.17)

- Wenn die Speicherung der Daten nicht mehr notwendig ist, bzw. der Zweck der Datenverarbeitung nicht mehr gegeben ist.
- Wenn der Betroffene seine Einwilligung zur Datenverarbeitung widerrufen hat.
- Wenn die Daten unrechtmäßig verarbeitet wurden.
- Wenn eine Rechenschaftspflicht zum Löschen nach EU- oder nationalen Recht besteht.

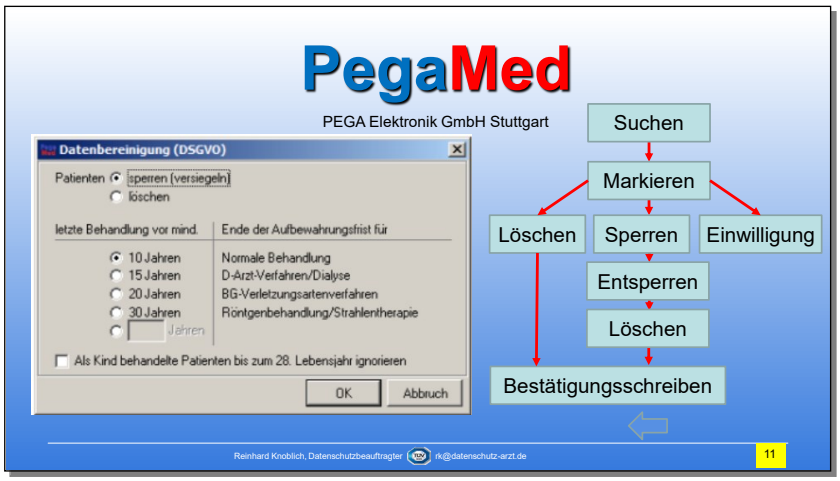
5. Recht auf Einschränkung der Verarbeitung (Art. 18)

Unter Geltendmachung seines Rechts auf Einschränkung der Verarbeitung kann der Patient verlangen, dass sämtliche erhobene personenbezogene Daten fortan nur mit individueller Einwilligung (und zur Geltendmachung und Durchsetzung von Rechtsansprüchen) verarbeitet werden dürfen. Die Berechtigung der Arztpraxis zur Speicherung wird dadurch allerdings nicht berührt. Ist eine Einschränkung erfolgt, dürfen die gespeicherten Daten nicht mehr wie bisher verwendet werden können, sie sind „gesperrt“.

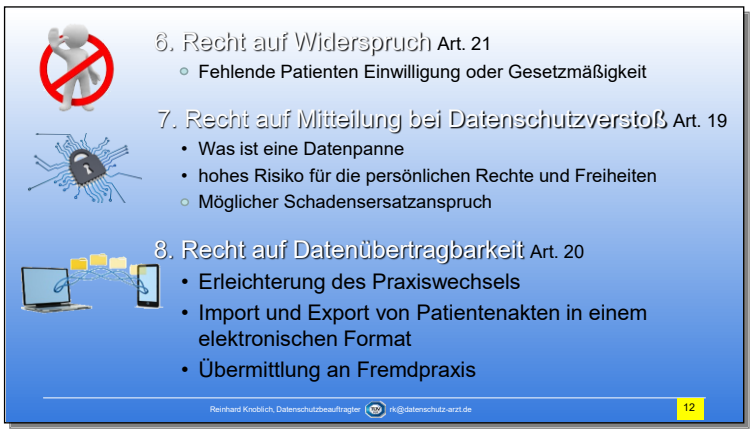
- Der Patient stellt die Richtigkeit der Daten infrage und bestreitet diese. Für die Dauer der Überprüfung der Richtigkeit sind die Daten zu sperren und dürfen nicht weiterverarbeitet werden. Je nach Prüfungsergebnis bleiben die Daten gesperrt, oder die Daten werden entsperrt und sind für die weitere Verarbeitung wieder verfügbar.
- Ist die Verarbeitung unrechtmäßig und der Patient lehnt die Löschung seiner Daten ab und verlangt stattdessen die Einschränkung der Nutzung der Daten, sind diese zu sperren
- Endet der Zweck der Verarbeitung, in der Regel nach zehn Jahren ohne Patienten Kontakt und der Patient verlangt Löschung der Daten, der Arzt jedoch zur Ausübung oder Verteidigung von Rechtsansprüchen, noch benötigt (30 Jahre Schadensersatzanspruch des Patienten nach BGB) werden diese nur gesperrt.

Achtung: Erwirkt der Betroffene die Einschränkung der Verarbeitung, begründet dies für den Verantwortlichen die **Informationspflicht, den Betroffenen vor der Aufhebung der Einschränkung zu unterrichten**. Zusätzlich ist die Arztpraxis verpflichtet, Dritte an welche die Daten übermittelt worden sind zu informieren, damit diese ihre Verarbeitungsprozesse selbst einschränken können.

Folie 11



Folie 12



6. Widerspruchsrecht (Art. 21)

- Erfolgt eine Datenverarbeitung durch die Arztpraxis ohne Einwilligung des Patienten oder aufgrund fehlender Gesetzmäßigkeit, so steht dem Patienten das Recht zu, dieser Verarbeitung zu widersprechen. Die Daten wären unverzüglich zu löschen.

7. Mitteilungspflicht bei Datenschutzverstoß (Art. 19)

- Datenschutzverstoß oder Datenpanne ist die Verletzung der Sicherheits-Barrieren, die zur Vernichtung, Verlust oder Offenlegung der Daten führen könnte. Ob der Verstoß unbeabsichtigt oder unrechtmäßig ausgelöst wurde, spielt keine Rolle, es genügt die Wahrnehmung, dass es eine Verletzung gegeben haben könnte.
- Bedeutet die Datenpanne ein „voraussichtlich hohes Risiko für die persönlichen Rechte und Freiheiten“ des Betroffenen, so ist der Betroffene unverzüglich von der Datenschutzverletzung „in klarer und einfacher Sprache“ zu unterrichten. Ist die Unterrichtung des Patienten nur mit einem „unverhältnismäßigen Aufwand“ möglich, muss der Umstand über eine öffentliche Bekanntmachung angezeigt werden.
- Wird dem Patienten durch eine unzulässige Datenverarbeitung Schaden zugefügt, so ist die Arztpraxis dem Patienten gegenüber zum Schadenersatz verpflichtet. Die Grundlage für den Schadenersatz kann auf verschiedenen Rechtsgrundlagen beruhen. Neu ist hierbei das Recht auf Schadenersatz nach Art. 82 Abs. 1.

„Jede Person, der wegen eines Verstoßes gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.“

8. Recht auf Datenübertragbarkeit (Art. 20)

- Neu im Vergleich zum alten Datenschutzrecht ist die Berechtigung des Patienten, von der jeweiligen Arztpraxis die ungehinderte und uneingeschränkte Übermittlung erhobener personenbezogener Daten an eine dritte Arztpraxis zu verlangen. Dies dient dem Ziel,

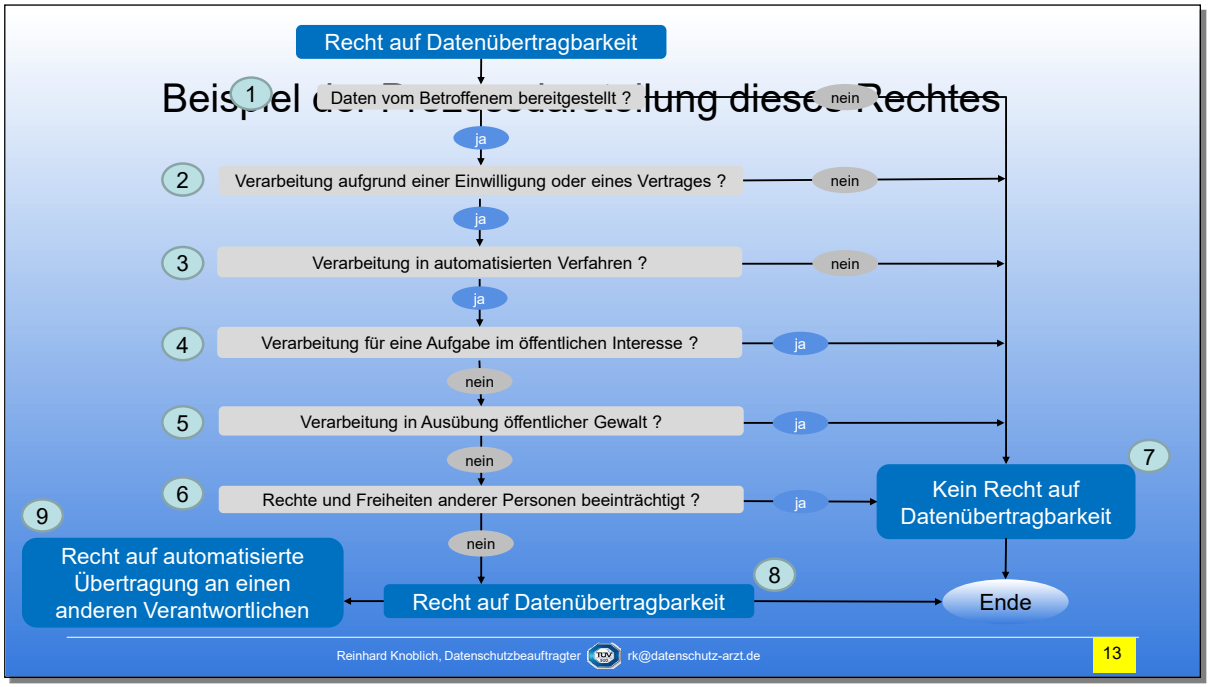
einer besseren persönlichen Hoheit auf die eigenen Daten, um sie vereinfacht auf einen Dritten zu übertragen, ohne dass eine erneute Eingabe notwendig ist.

- Dazu kann der Patient von der Arztpraxis die Herausgabe und Übermittlung der erhobenen Daten in einem „strukturierten, gängigen und maschinenlesbaren Format“ an eine andere Arztpraxis verlangen.
- Alternativ kann der Patient aber auch die direkte Übermittlung von der Arztpraxis zu Arztpraxis verlangen, ohne seine eigene Zwischenschaltung.

Strukturiertes, gängiges und maschinenlesbares Format ist eine Voraussetzung, um Daten in unterschiedliche Datenbanken direkt zu übertragen.
Gängige maschinenlesbare Formate:

- BDT (KV Abrechnungsdatei textbasiertes Dateiformat)
- XLSX (Excel-Tabelle Office basiertes Dateiformat)
- CSV (textbasiertes Dateiformat)
- XML (HTML-basiertes Dateiformat)

Folie 13



Recht auf Datenübertragbarkeit

(Art. 20 DSGVO)

Das Recht auf Datenübertragbarkeit ist neu und umfasst einerseits ein Recht des Betroffenen, vom Verantwortlichen die zu seiner Person gespeicherten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt zu bekommen, und andererseits die Verpflichtung des Verantwortlichen, auf Verlangen des Betroffenen diese Daten einem anderen Verantwortlichen zu übermitteln. Das Recht auf Datenübertragbarkeit besteht aber nicht uneingeschränkt, sondern ist einerseits davon abhängig, aufgrund welcher Rechtsgrundlage die Daten verarbeitet werden (Einwilligung oder Vertrag), wie der Verantwortliche die Daten erhalten hat (vom Betroffenen selbst) und für welche Zwecke die Daten verarbeitet werden.
Der Datenschutzprozess „Recht auf Datenübertragbarkeit“ zeigt einen Überblick über dieses neue Recht.

Erläuterungen:

Zu 1: Daten vom Betroffenen bereitgestellt?
Das Recht auf Datenübertragbarkeit greift bei Erfüllung der sonstigen Voraussetzungen nur für diejenigen Daten, die die betroffene Person selbst einem Verantwortlichen bereitgestellt hat.

Zu 2: Verarbeitung aufgrund einer Einwilligung oder eines Vertrags?
Voraussetzung für ein Recht auf Übertragbarkeit der Daten ist gem. Art. 20 Abs. 1 lit. a D SGVO entweder die Verarbeitung auf der Grundlage einer Einwilligung gem. Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a D SGVO oder auf der Grundlage eines Vertrags gem. Art. 6 Abs. 1 lit. b D SGVO.

Zu 3: Verarbeitung in automatisierten Verfahren?
Das Recht auf Datenübertragbarkeit gilt gem. Art. 20 Abs. 1 lit. b D SGVO nur für Daten, die in automatisierten Verfahren (EDV) verarbeitet werden. Daten, die in manuellen Verfahren, z. B. in Karteien, Film-, Papier-Unterlagen verarbeitet werden, sind von diesem Recht ausdrücklich ausgeschlossen.

Zu 4: Verarbeitung für eine Aufgabe im öffentlichen Interesse?
Das Recht auf Datenübertragbarkeit gilt gem. Art. 20 Abs. 3 D SGVO nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt, die dem Verantwortlichen übertragen wurde.

Zu 5: Verarbeitung in Ausübung öffentlicher Gewalt?
Das Recht auf Datenübertragbarkeit gilt gem. Art. 20 Abs. 3 D SGVO nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe in Ausübung öffentlicher Gewalt erforderlich ist, die dem Verantwortlichen übertragen wurde.

Zu 6: Rechte und Freiheiten anderer Personen beeinträchtigt?
Durch die Datenübertragung gem. Art. 20 Abs. 2 D SGVO dürfen die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden.

Zu 7: Kein Recht auf Datenübertragbarkeit
Es besteht kein Recht auf Datenübertragbarkeit.

Zu 8: Recht auf Datenübertragbarkeit
Der Betroffene kann ein Recht auf Datenübertragbarkeit geltend machen.

Zu 9: Recht auf automatisierte Übertragung an einen anderen Verantwortlichen
Die betroffene Person hat das Recht, soweit dies technisch machbar ist, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen an einen anderen Verantwortlichen in einem gängigen, strukturierten z.B. XML-, CSV-, BDT-Format übermittelt werden.

Folie 14

Art.25:
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 …… die dafür ausgelegt sind, die Datenschutzgrundsätze …… umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Erwägungsgründe 78:
Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden.
Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by Design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.

DSGVO als Wettbewerbsvorteil nutzen
Die nachweisliche Einhaltung hoher Schutzstandards bei der Verarbeitung personenbezogener Daten kann sich für Unternehmen als echter Wettbewerbsvorteil erweisen.

Aus der Last eine Tugend machen
Dabei ist es eigentlich ganz falsch, die DSGVO mit ihren erhöhten Anforderungen an eine sichere Verarbeitung personenbezogener Daten als lästige Pflicht oder gar Schikane anzusehen. Mit der fortschreitenden Digitalisierung und der beginnenden IoT-Revolution (Internet of Things), bedeuten Sicherheitslücken nicht nur mögliche Verstöße gegen die DSGVO, sondern vor allem einen Vertrauensverlust gegenüber den Geschäftspartnern und Verbrauchern. Die Unternehmen müssen lernen, Nutzen aus dem achtsamen Umgang mit personenbezogenen Daten zu schöpfen und hohe Datenschutzstandards als möglichen Wettbewerbsvorteil zu sehen.

Das sollte eine Arztprogramm bei der DSGVO unterstützen:

1. DSGVO-Patienten-Rechte
- Recht auf Information
- Recht auf Auskunft
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Datenübertragbarkeit

2. Zentrale Benutzerverwaltung (ZBV)

3. Zugriffsrechtemanager (ZRM)

4. Protokollfunktionen im Bereich medizinische Daten und Stammdaten
5. Datensicherung: Rückspielbarkeits-Test

Folie 15

Vertrag zur Auftrags-Verarbeitung:
Anlage 2: Unterauftragnehmer
Unterauftragnehmer sind solche Dienstleister, die die Dienstleistung des Hauptauftragnehmers im Sinne des Auftraggeber-Vertrages ergänzen.
D. h., ein Unterauftragnehmer wird im Namen des Auftragsverarbeiters beim Arzt mit einer Teilleistung tätig.
Dem Unterauftragnehmer müssen dieselben Verpflichtungen weitergegeben und kontrolliert werden, wie sie vom Arzt definiert worden sind.
In der Dokumentation der Unterauftragnehmer-Liste ist zu dokumentieren:
Name der Firma, Kontaktdaten, Beschreibung der Teilleistung die zu erbringen ist.
Achtung: Der Arzt hat das Recht die Vertragsunterlagen zum Unterauftragnehmer einzusehen.

<u>Typische Unterauftragnehmer:</u>
- Unterlieferanten von Diagnosen-Systemen, die sich zur Wartung aufschalten
- vor Ort-EDV-Techniker, der die Region betreut
- Cloud-Provider, bei dem virtuelle Maschinen, oder Speicherplatz angemietet wurden (zum Beispiel: Wortmann, Worxeasy)

Häufiger Fehler:
Es werden sämtliche Dienstleister und Vertragspartner aufgelistet die zwar mit dem Auftragsverarbeiter etwas zu tun haben, aber nichts mit dem Arzt.

Keine Unterauftragnehmer sind:
- Microsoft für Betriebssystem und Office Produkte
- HZV oder andere Verbände
- Marketing, Webseiten-Designer,
- Teamviewer oder ähnliche VPN-Lösungen

Usw.