Ärztekammer Nordrhein

Die neue Datenschutzgrundverordnung

Informationen für die Handhabung in der ärztlichen Praxis

Claus-Hinrich Buschkamp, LL.M.
Ärztekammer Nordrhein
Syndikusrechtsanwalt
Fachanwalt für Medizinrecht

Einführung

- **24. Mai 2016: Inkrafttreten der DSGVO**
- **25. Mai 2018: Anwendungsbeginn der DSGVO und Inkrafttreten des neuen BDSG**
- **Ablösung einer EU-Richtlinie von 1995**
- **Kosten der Einführung: Sie als Unternehmer** **(Arztanfrage)**

Ärztekammer Nordrhein

Der Datenbegriff der DSGVO

- **Welche Daten sind überhaupt gemeint?**

- **→ personenbezogene Daten**
  - „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“

- **→ die verarbeitet werden**
  - automatisiert (per EDV)
  - nicht automatisiert, aber strukturiert gesammelt
    - d.h. auch Papier-Karteikarten und gegliederte Leitz-Ordner

Ärztekammer Nordrhein

Der Datenbegriff der DSGVO

- **Datenerhebung:**
  - **Beschaffung bei der betroffenen Person**
  - **Beschaffung bei Dritten (Dritterhebung)**

- **Datensparsamkeit**
  - **Nur so viele Daten erheben und nur so lange, wie es notwendig ist**
  - **Nur so viele Personen mit Zugang ausstatten, wie nötig**
    - Ggf. verschiedene Zugriffsrechte vergeben
    - Je größer die Praxis, desto eher vonnöten

Verarbeitung

- **„jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“**

Ärztekammer Nordrhein

Rechtmäßigkeit der Verarbeitung

- aus Vertrag
- durch Einwilligung
- durch Gesetz
- zur Wahrung von Grundrechten (fair trial)
- im Rahmen der Auftragsverarbeitung

Rechtmäßigkeit durch Vertrag

- **Behandlungsvertrag**
  - **egal ob Privat- oder Kassenpatient**
- **Liefervertrag**
- **Arbeitsvertrag**

- **bei Auftragsverarbeitung**
  - **Weisungsgebundenheit des Auftragnehmers**
    - Druckerei, Aktenvernichter, Lohnbuchhaltung
    - auch: Einfachlabor (Laborgemeinschaft)

Ärztekammer Nordrhein

Rechtmäßigkeit durch Einwilligung

(insbesondere Datenweitergabe an Dritte)

- **Früher: schriftlich**
- **Jetzt: nachweisbar**
  - **d.h.: wohl auch mündliche Frage und Notiz in Patientenakte ausreichend!**
  - **Ausnahme: §10 VI GOZ: Einwilligung schriftlich!**
  - **Ausnahme: (str.) Verdrängung von §73 Abs. 1b SGB V durch DSGVO? Unterscheidung Kassen-/Privatpatienten**
- **Abgabe freiwillig, in informierter Weise, unmissverständlich**
- **für festgelegten Zweck (keine Pauschal-EW)**
  - **auch keine „Befreiung“ von der DSGVO möglich (Arztanfrage)**
- **auch ohne EW in Datenweitergabe Behandlung möglich!**
- **kann widerrufen werden, bisherige DV bleibt rechtmäßig**
- **ungeklärt, wie oft EW eingeholt werden muss**
  - **„jedes Mal“ bis „einmal bis Widerruf“**

Rechtmäßigkeit durch Einwilligung

(insbesondere Datenweitergabe an Dritte)

- **Datenweitergabe - Beispielsfälle**
  - **Arztbrief an Hausarzt**
  - **Krankenhaus ruft an, braucht Infos**
    - Im Notfall: mutmaßliche Einwilligung! Datenweiterleitung auch ohne explizit abgegebene Einwilligung möglich, wenn dies im mutmaßlichen Interesse des Patienten liegt
  - **Angehöriger holt Rezept ab**
    - Kinder
    - Eltern eines volljährigen Kindes
    - Ehepartner (§1357 BGB)
  - **Rezept an Apotheke faxen**
  - **Altenheim braucht Mediplan/Rezept**
    - Keine Verpflichtung zur Überprüfung, ob Altenheim DSGVO einhält: jeder selber verantwortlich (Arztanfrage)

- **Einwilligungen können gescannt werden! Original aufbewahren unnötig (str.: ggf. TR-Resiscan, §73 SGB V-Problematik)**
- **Für jede Einzelpraxis innerhalb einer Praxisgemeinschaft gesondert**

Ärztekammer Nordrhein

Rechtmäßigkeit qua Gesetz

- **Eine Datenverarbeitung bzw. die Datenweitergabe ist immer dann zulässig, wenn dies ein Gesetz oder eine andere Norm vorsieht:**
  - **Abrechnung mit der KV (§294ff. SGB V)**
  - **Krankenkassen (§§294ff. SGB V)**
  - **Gesetzliche Unfallversicherung (§201 SGB VII)**
  - **Prüfungsstellen (§106 IV SGB V)**
  - **MDK (§276 II SGB V)**
  - **Gesetzliche Meldepflichten (Infektionsschutz: §6 IfSG, Krebsregister: §4 I KRG-NRW, Röntgen: §§17a, 28 VIII RöV, Strahlenschutz: §42 StrlSchV, Betäubungsmittel: §5b BtMVV, Gesetz zur Kooperation und Information im Kinderschutz: §4 III KKG…)**

Ärztekammer Nordrhein

Rechtmäßigkeit in besonderen Fällen

- **Offenbarung gegenüber anderen Berufsgeheimnisträgern (Rechtsanwälte, Steuerberater…) bei Wahrung berechtigter Interessen**
  - **Verteidigung in Haftungsfällen**
  - **Forderungsdurchsetzung**
  - **Steuerberatung**
- **Kurzum: immer, wenn Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen**
  - **Auch: Bank, Post (nur ausgelagerte Nebenleistungen)**
- **Rechtfertigender Notstand (§34 StGB)**

Informationspflichten in der Praxis

- z.B. mit Info-Blatt (Muster auf www.aekno.de/dsgvo)
- Infos präzise, transparent, verständlich, leicht zugänglich
  - d.h. auch kein Medienbruch (kein Verweis auf Homepage zur Information)
- schriftlich oder in anderer Form
  - Im Gegensatz zur Einwilligung: Scannen sicher ausreichend!
- übermitteln / zur Verfügung stellen
  - Praxisaushang ausreichend? → Notiz in Akte!
  - LDI: „aktives Anbieten“, Sicherstellung des Verständnisses nicht verlangt
- gilt auch für Bestandspatienten
- Info einmal ausreichend
  - Vermerken, dass Info ausgehändigt wurde!

Ärztekammer Nordrhein

Informationspflichten in der Praxis

- Name und Kontaktdaten des Arztes/des MVZ
- ggf. Name und Kontaktdaten des DSB
- Zwecke der DV
- Rechtsgrundlagen
- Empfänger der Daten
- Hinweis auf Drittstaatsübermittlung
- Dauer der Speicherung
- Rechte des Patienten
- Quelle der Daten

Informationspflichten in der Praxis

- **Informationspflicht entfällt nur, wenn**
  - **Patient bereits über Infos verfügt**
  - **ausschließlich analoge unkategorisierte Handhabung**
  - **Zuwiderlaufen gg. öffentlichen Zweck**
  - **Gefährdung öfftl. Sicherheit**
  - **Landeswohl**
  - **Vereitelung einer Anspruchsdurchsetzung**
  - **Vertrauliche Übermittlung an öfftl. Stelle**

Informationspflichten in der Praxis

- **Konsequenzen, wenn Patient**
  - **Informationen zum Datenschutz nicht zur Kenntnis nehmen will**
    - In der Akte vermerken, Behandlung trotzdem möglich
  - **Einwilligungen nicht abgeben will**
    - Nachteile für die Behandlung
    - Muss Arztbriefe selber abholen

Ärztekammer Nordrhein

Informationspflichten auf der Homepage

- **gesonderte Informationen vonnöten**
  - **„Ansurfen“ bedingt bereits Datenerhebung (auch bei „Einfachst-Homepages“)**
    - IP-Adresse
    - Datenmenge
    - Ursprung des Surfvorgangs…
- **angepasst an Homepage-Umgebung**
  - **Google-Analytics?**
  - **Social Media?**
  - **Newsletter?**
  - **Kontaktformulare?**
  - **Routenplaner (Google Maps)?**
- **Trennungspflicht Impressum/Datenschutzerklärung nicht ersichtlich**
- **Muster auf www.aekno.de/dsgvo**

Datenschutz in der Kommunikation

- **Verwendung von cloudbasierten Diensten mit Servern in Drittstaaten**
  - **nur zulässig, wenn im Drittland vergleichbares Schutzniveau (Angemessenheitsbeschluss)**
  - **oder wenn Garantien gegeben wurden (Binding Corporate Rules/EU-Standarddatenschutzklauseln)**
  - **oder bei ausdrücklicher Einwilligung (Risikoaufklärung!)**
- **Automatische Datenübermittlung durch Apps**
  - **Abgleich der gesamten Telefonbuchkontakte bei Whatsapp**
  - **Scan der E-Mails bei Gmail auf werberelevante Inhalte**

Datenschutzbeauftragter

- **Wann benötige ich einen Datenschutzbeauftragten?**
  - **1. ab 10 Beschäftigten**
    - Zählung inkl. Praxisinhaber
    - Jeder Beschäftigte zählt als 1, unabhängig von der Stundenzahl
    - sofern regelmäßig mit der Datenverarbeitung befasst (nicht: Hausmeister, Putzfrau)
  - **2. wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Datenkategorien besteht**
    - DV=Kerntätigkeit des Arztes? Wohl (+, umstr., aber Dokupflicht!)
    - Umfangreich?
      - Einzelpraxis (-)
      - Laut DSK bei BAG: in der Regel (-)

        Ausnahme: sehr große BAG
        hohes Risiko für Rechte und Freiheiten (neue Technologien)
  - **3. wenn Datenschutzfolgenabschätzung vorzunehmen ist**
    - schon dann, wenn umfangreiche Verarbeitung

Datenschutzbeauftragter

- **Wer kann Datenschutzbeauftragter werden?**
  - **Externe Datenschutz-Unternehmen**
  - **Rechtsanwälte**
  - **geschulte Angestellte (nicht Praxisinhaber)**
  - **Idee: ein DSB für mehrere Praxen, z.B. im Qualitätszirkel/Hausärzteverbund**
- **Wann ist jemand qualifiziert genug?**
  - **Strittig! Einerseits Jura- + Informatikstudium, andererseits: keine geregelte Ausbildung, kein anerkannter Abschluss: „Je mehr, desto besser.“**

Ärztekammer Nordrhein

Datenschutzbeauftragter

- **Aufgaben**
  - **Beratung des Verantwortlichen in Sachen Datenschutz**
  - **Überwachung der Einhaltung der Datenschutz-Gesetze**
  - **Zusammenarbeit mit der Aufsichtsbehörde**
- **Stellung**
  - **Gewisser arbeitsrechtlicher Schutz, auch bis 1 Jahr nach Ende der Tätigkeit als DSB**
  - **Weisungsungebundenheit**
  - **unterliegt der Schweigepflicht**
- **Haftung: es haftet der Verantwortliche, nicht der DSB**
- **Meldung der Personalien**
  - **NRW: LDI (bis 31.12.2018)**

Ärztekammer Nordrhein

Verzeichnis der Verarbeitungstätigkeiten

- **Erstellung: Darlegung aller Datenverarbeitungsvorgänge in übersichtlicher Liste**
  - **grds. erst ab 250 Mitarbeitern, aber anders bei DV von Gesundheitsdaten (besondere Kategorie)**
  - **keine Veröffentlichungspflicht mehr**
- **Prüfung, ob bei den Vorgängen Daten gefährdet sind**
- **Maßnahmenergreifung zur Reduzierung bzw. Minimierung dieser Gefahren**
  - **Passwörter**
  - **Schlüssel**
  - **PC-Schutz (Antiviren, Firewall, Backups)**
  - **Erstellung einer Maßnahmenübersicht, wenn sich Betroffene an die Praxis wenden**

Ärztekammer Nordrhein

Verzeichnis der Verarbeitungstätigkeiten

- **Gliederung nach Verarbeitungszwecken**
  - **Behandlungsvertrag/-dokumentation**
  - **Abrechnung**
    - Inkassodienstleister/Abrechnungsstellen
    - Kassenärztliche Vereinigung
    - Factoring
  - **Buchhaltung**
  - **Allgemeiner Schriftverkehr**
  - **Personal**
  - **EDV**
  - **Aktenvernichtung**

Verzeichnis der Verarbeitungstätigkeiten

- **Ermittlung der darzulegenden Punkte**
  - **Zweck der Verarbeitung**
  - **Kategorien der betroffenen Personen**
    - Patienten
    - Angestellte
    - Andere (Lieferanten usw.)
  - **Kategorie der Daten**
    - Stammdaten
    - Gesundheitsdaten
    - Personaldaten
  - **Kategorie der Empfänger**
  - **Löschfrist (grds. 10 Jahre oder Verjährungsfrist)**
  - **Angabe des Landes bei Drittlandsbezug**
  - **Maßnahmen zur Datensicherheit (TOM)**
    - Externe Festplatten nicht verlieren (Arztanfrage)
- **Ggf. ergänzen mit Anlagen (Dienstanweisungen usw.)**

Verzeichnis der Verarbeitungstätigkeiten

- **Technische und organisatorische Maßnahmen (TOM)**
  - **Pseudonymisierung**
  - **Verschlüsselung**
  - **Passwortschutz**
  - **Zugangsbeschränkungen**
  - **Gewährleistung der**
    - Integrität (kein nachträgliches Verändern von Daten)
    - Verfügbarkeit (Stromausfall?)
    - ausreichenden Systemkapazität (Hackerangriff, DDOS)
    - möglichen Datenwiederherstellung

Ärztekammer Nordrhein

Verzeichnis der Verarbeitungstätigkeiten

Wie tiefgreifend? So wohl nicht ausreichend:

Verzeichnis von Verarbeitungstätigkeiten

(nach Artikel 30, Absatz 1 Datenschutz-Grundverordnung)

Verarbeitungstätigkeit	Zweck der Verarbeitung	Kategorie der Personen	Kategorie der Daten	Kategorie von Empfängern	Erstellungs-datum	Löschungs-frist
Einsatz und Nutzung des Praxisverwaltungs-systems	Dokumentation, Abrechnung, Terminvergabe	Patienten	Personenbezogene Daten Gesundheitsdaten Genetische Daten	Praxismitarbeiter (Ärzte, MFA), KV, Ärztekammer, GKV, PKV, private Abrechnungsstellen, Versorgungsämter	07.04.2018	10 Jahre
Führen von Personalakten	Beschäftigung von Mitarbeitern	Angestellte der Praxis	Personenbezogene Daten, Personaldaten	Praxisinhaber, Steuerberater, Krankenkassen, Finanzämter, Rentenversicherer	07.04.2018	10 Jahre
Versenden von Befunden	Übermittlung von Gesundheitsdaten	Patienten	Gesundheitsdaten	Arztpraxen, Krankenhäuser, Rentenversicherungen, Berufsgenossenschaften, Versorgungsämter, Sonstige Versicherungen	07.04.2018	10 Jahre
Abrechnung mit der KV	Übermittlung von Gesundheits- und Abrechnungsdaten	Patienten	Gesundheits- und Abrechnungsdaten	Mitarbeiter der KV	07.04.2018	10 Jahre
Abrechnung mit der privaten Abrechnungsstelle	Übermittlung von Gesundheits- und Abrechnungsdaten	Patienten	Gesundheits- und Abrechnungsdaten	Mitarbeiter der privaten Abrechnungsstelle	07.04.2018	10 Jahre
Tägliche Datensicherung	Sicherung der Behandlungs- und Abrechnungsdaten	Patienten	Gesundheits- und Abrechnungsdaten	Praxismitarbeiter (Ärzte, MFA)	07.04.2018	10 Jahre
Erstellung und Versendung von Gutachten	Dokumentation und Bewertung von Gesundheitsdaten	Patienten	Gesundheitsdaten	Mitarbeiter von Versicherungen, Gerichten, Berufsgenossenschaften, Medizinischen Diensten	07.04.2018	10 Jahre

Ärztekammer Nordrhein

Datenschutzfolgeabschätzung

- **Siehe Paper unter www.aekno.de/dsgvo**
- **Eher nicht relevant für Ärzte**
- **Immer dann durchzuführen, wenn Art, Umfang, Umstände und Zwecke der DV voraussichtlich ein hohes Risko für Rechte und Freiheiten der Betroffenen zur Folge hat**
  - **Wenn physischer, materieller oder immaterieller Schaden für Person droht**
  - **Einzelkategorien (2 notwendig)**
    - Profiling
    - Automatisierte Entscheidungsfindung
    - *Systematische Überwachung*
    - Höchstpersönliche Daten
    - *DV in großem Umfang*
    - Abgleich/Zusammenführung von Datensätzen
    - *Schutzbedürftige Betroffene*
    - *Neue Technologien*
    - DV verhindert Rechtsausübung

Datenschutzfolgeabschätzung

- schutzbedüftige Betroffene
  - bei Machtungleichgewicht (Kinder, Senioren, Ausländer, Kranke…)
- neue Technologien
  - umfassendere Praxissoftware
- systematische Überwachung
  - weitreichende Videoüberwachung
- umfangreiche Datenverarbeitung
  - EW 91: nicht Einzelpraxis!
  - Andere? Wohl eher keine „Verarbeitungsvorgänge, die dazu dienen, auf regionaler, nationaler, supranationaler Ebene eine große Zahl von Personen betreffend, hohes Risiko aufgrund der Sensibilität der Daten (Gesundheitsdaten!)…“
  - → wohl für große Konzerne gedacht, aber großes überörtliches MVZ??? Strittig!

- **Wenn DSFA: immer Datenschutzbeauftragter!**

Auftragsverarbeitung

- **Dienstleister verarbeitet personenbezogene Daten ausschließlich auf Weisung des Auftraggebers**
  - **z.B. EDV-Dienstleister prüft die Systeme**
  - **Druckerei versendet Recall-Postkarten**
  - **Laborgemeinschaft (nicht: Speziallabor!)**
    - Unterschied: LG: Ich befunde selber, SL: Anderer Arzt befundet.

- **dann keine gesonderte Einwilligung des Betroffenen notwendig!**

Auftragsverarbeitung

- **Meistens stellen Dienstleister bereits den AV-Vertrag**
- **Wenn nicht: Muster unter daebl.de/CS39**
  - **schriftl. oder elektr. möglich**
  - **Notwendig – sonst: Schweigepflichtverstoß.**
- **Vorlage aktueller Zertifizierungen des Auftragnehmers verlangen!**
- **Kein Bruch der Schweigepflicht mehr (§203 StGB neuerlich geändert)!**
  - **→ Auftragnehmer auf Schweigepflicht verpflichten**

Rechte des Patienten

- **1. Auskunftsrecht**
  - **„Antrag“ des Patienten formfrei**
  - **Auskunft verständlich, transparent**
  - **keine Medienbrüche!**
  - **Überprüfung der Identität**
  - **Kostenfrei (anders als Einsichtnahme gem. BGB)**
  - **innerhalb eines Monats**
  - **bei Ablehnung: Gründe, Hinweis auf Beschwerde- und Klagerecht**
    - z.B. aus therapeutischen Gründen, überwiegende Interessen Dritter, Speicherung nur noch wg. anderweitiger Aufbewahrungspflichten, Beeinträchtigung von Forschungszwecken
  - **→ ob und wie eigene Daten verarbeitet werden**

Rechte des Patienten

- **Inhalt**
  - **eigene gesundheitsbezogene Daten**
    - Anamnese, Diagnose, Untersuchungsergebnisse, Befunde, Angaben zu Behandlungen und Eingriffen
  - **Verarbeitungszwecke der Patientendaten**
  - **Kategorien der verarbeiteten Daten (Gesundheitsdaten)**
  - **Empfänger oder Kategorien der Empfänger der Daten**
  - **Speicherdauer bzw. Kriterien („so lange wie nötig“)**
  - **Aufzeigung der Rechte des Patienten**
    - Berichtigung
    - Löschung
    - Einschränkung der Verarbeitung
    - Widerspruch gegen Verarbeitung
    - Beschwerderecht bei Landesdatenschutzbeauftragter
  - **Herkunft der Daten bei Dritterhebung**
  - **Garantien bei Drittlandsübermittlung**

Rechte des Patienten

- **2. Recht auf Korrektur/Vervollständigung**
  - **bei unrichtigen/unvollständigen Daten**
  - **eher selten bei medizinischen Daten**
  - **ACHTUNG: Änderungen müssen erkennbar bleiben (§630f BGB)**

Rechte des Patienten

- **3. Recht auf Löschung**
  - **Daten dürfen nur solange gespeichert werden bis**
    - der Zweck, für den sie erhoben wurden, erreicht oder entfallen ist (bei „lebenslangen Patienten“ auch mal lebenslang!)
    - es gesetzliche Vorschriften vorsehen
    - sie zur eigenen Verteidigung notwendig sind
  - **Sofortige Löschung nur, wenn**
    - Einwilligung widerrufen und kein sonstiger Grund für Speicherung vorliegt (z.B. Gesetz)
    - Daten unrechtmäßig verarbeitet worden sind
  - **einfacher Antrag des Betroffenen möglich**
    - elektronisch gestellt, elektronisch beantwortet
    - grds. unentgeltlich

Rechte des Patienten

- **3. Recht auf Löschung**
  - **Was bedeutet Löschen?**
    - Daten können ohne unverhältnismäßigen Aufwand nicht wiederhergestellt werden
    - Ordentliche Akten-/Datenträgervernichtung!

Fehlende Einwilligung? Daten im Hausmüll? Das wird teuer!

Neue Datenschutz-Bußgelder zielen auf gesetzeskonformes Verhalten – nicht auf Existenzvernichtung

Medical-Tribune-Recherche

Fachtagung „Datenschutz in der Medizin – Update 2018"

WIESBADEN. Ab dem 25. Mai 2018 gilt die neue EU-Datenschutzgrundverordnung auch in Deutschland. Sie soll europaweit gleichwertigen Datenschutz gewährleisten. Um das durchzusetzen, bringt sie einen knackigen Sanktionenkatalog mit sich. Was heißt das für die Praxis?

Berechnung des Bußgeldes an einem fiktiven Fall

Bei der Entscheidung über den Betrag einer Geldbuße werden in jedem Einzelfall Zumessungskriterien (siehe Kasten unten) berücksichtigt. Beispiele zur Bußgeld-Festsetzung können deswegen nicht verbindlich sein. Der folgende **fiktive Fall** macht das Prinzip anschaulich:

3) Der Bußgeldbetrag wird den Zumessungskriterien der DSGVO folgend angepasst:

Dauer: über gewissen Zeitraum	+ 30 %
Vorsatz: fahrlässig	– 50 %
Maßnahmen zur Minderung: regulär	± 0 %
Grad der Verantwortlichkeit: regulär	± 0 %

© Medical Tribune

Rechte des Patienten

- **3. Recht auf Löschung**
  - **Keine Löschung, wenn Aufbewahrungspflicht noch nicht abgelaufen ist**
    - 10 Jahre Patientenunterlagen (§630f III BGB)
    - 3 Jahre BtM-Rezepte/-Buch (§§8, 13 BtMVV)
    - 30 Jahre Röntgenaufnahmen (§28 RöV)
    - 5 Jahre Mitarbeiterunterweisung (§36 RöV)
  - **andere Löschfristen auch bei Daten, die keine Patientendaten sind**
    - 2 Jahre Arbeitszeitnachweise (§16 ArbZG)
    - 2 Jahre Beschäftigung werdender Mütter (§27 MuSchG
    - 5 Jahre Unfallanzeige/Verbandbuch (§24 DGUV)
    - 2 Jahre nach letzter Eintragung Verzeichnis der beschäftigten Jugendlichen (§50 JArbSchG)
    - 10 Jahre Steuerunterlagen, Gehaltslisten, Quittungen, Kassenbücher, -berichte (§147 AO, §14b UStG)
    - 6 Jahre Bestell-/Auftragsunterlagen, Reisekostenabrechnungen (§147 AO)
  - **ansonsten: Löschpflicht!**
    - Es sei denn: eigene Rechte betroffen (Verteidigung gegen Behandlungsfehler-Vorwurf)
  - **EuGH-Urteil zum Vergessenwerden nur einschlägig beim „Öffentlichmachen“ → irrelevant für Ärzte wegen Schweigepflicht**

Rechte des Patienten

- **4. Recht auf Verarbeitungseinschränkung**
  - **für die Dauer der Überprüfung, ob Löschungs-/Berichtigungsansprüche bestehen**
  - **wenn nur Verarbeitungseinschränkung verlangt wird**
  - **wenn der Verantwortliche löschen darf und muss, der Betroffene aber die Daten weiterhin benötigt**

  - **→ nur noch Speicherung**
  - **→ Verarbeitung nur bei ausdrücklicher Einwilligung, zur Geltendmachung von Ansprüchen oder zur Verteidigung**

Rechte des Patienten

- **5. Recht auf Datenübertragbarkeit („Portabilität“)**
  - **generell eher gedacht für Internetdiensteanbieter (eMail-Dienste, soziale Netzwerke usw.), damit man von einem zum anderen Anbieter „umziehen“ kann**
  - **ggf. in Arztpraxen relevant, wenn Patient seine Patientenakte digital mit zu einem anderen Arzt nehmen möchte (und dieser eine kompatible Software verwendet)**
  - **trifft nur auf selber bereitgestellte Daten zu, nicht auf eigene Daten des Arztes!**

Ärztekammer Nordrhein

Datenschutzbehörde

- **Die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW**
- **Kavalleriestr. 2-4**
- **40213 Düsseldorf**

Datenschutzbehörde

- 1. Aufgaben
  - Überwachung/Durchsetzung der Normen
  - Öffentlichkeitsarbeit
  - Beschwerdewesen
  - Aufzeichnung von Verstößen
  - Sicherung einheitlicher Gesetzesanwendung
  - Beratung, auch für Datenschutzbeauftragte
  - Akkreditierung/Zertifizierung

Datenschutzbehörde

- **2. Befugnisse**
  - **Untersuchungsrechte**
    - Kein Einsichtsrecht bei Daten, die der Schweigepflicht unterliegen
  - **Abhilferechte**
    - Warnung, Verwarnung, Anweisung, Verbot der Datenverarbeitung, Geldbußen
    - Abberufung eines DSB bei mangelnder Fachkunde
    - Anweisung zur Löschung/Berichtigung
  - **Genehmigungen/Beratungen**
    - z.B. durch Stellungnahmen, Erarbeitung von Standardklauseln…

Datenschutzbehörde

- **3. Pflichten gegenüber der Behörde**
  - **Benennung des Datenschutzbeauftragten, sofern vorhanden**
    - über Onlineformular ab dem 25.05.2018
  - **bei Datenpannen innerhalb von 72h über**
    - Art der Verletzung
    - Zahl der betroffenen Personen
    - Kontaktdaten des DSB
    - Beschreibung der Folgen
    - Beschreibung der ergriffenen Maßnahmen
    - bei hohem Risiko für das Persönlichkeitsrecht der Personen (z.B. bei Gesundheitsdaten!)
      - Aufzeigung, dass notwendige und ausreichende Maßnahmen zum Schutz ergriffen worden sind
      - Maßnahmen nach der Panne, dass kein Risiko mehr besteht
      - Benachrichtigung der betroffenen Personen oder öffentliche Bekanntmachung
    - Jedenfalls interne Dokumentationspflicht

Ärztekammer Nordrhein

Kommunikation

- **eMail**
  - **inhalts- und transportverschlüsselt**
    - oder: verschlüsselte PDF
  - **Identität des Gegenübers absichern**
  - **keine Verantwortung für unverlangt übersandte Mails**
- **Telefon**
  - **Identitätsabklärung durch**
    - Nummer bekannt
    - Stimme bekannt
  - **Rezeptbestellung: einfach möglich, sofern nur Bestellung aufgenommen wird und Rezept persönlich oder durch Bevollmächtigten abgeholt wird**
- **Fax**
  - **Keine Notwendigkeit, abzuklären, ob Faxgerät der Gegenstelle vor Einsichtnahme geschützt wird**
  - **Keine Notwendigkeit, vorher ein Deckblatt zu versenden wie: „Achtung, jetzt kommt ein datengeschütztes Fax!“**
  - **Wichtig ist, sicherzustellen, dass jene Faxnummer zu dem Empfänger gehört, den ich erreichen will**
  - **Unbeantwortet: VoIP-Problematik…**
- **Anrufbeantworter**
  - **erst Hinweise auf Datenschutz vorlesen: Lebensfremd!**
- **Videokonferenz**
  - **Sichere Verbindung! Fernbehandlungsverbot beachten!**
- **NAS-Server/VPN zur Praxissoftware**
  - **auf ausreichende Verschlüsselung achten!**
- **Näheres: Technische Anlage, DÄBl. 2008, 1, Heft 19, 09.05.2008 (kommt bald neu heraus!)**

Sanktionen

© Medical Tribune

Sanktionen

- **Werden wohl sparsam und mit Augenmaß eingesetzt**

Sanktionen

- **Panikmache oder berechtigte Befürchtungen?**
- Thomas Hoeren, Professor an der Universität Münster, ist hingegen überzeugt, dass die Auswirkungen nicht so groß sein werden wie befürchtet: "Ich bin entsetzt über die ganze Panikmache." Und er fragt: "Warum haben wir eigentlich so eine schlechte Haftung gegen Falschberatung?" Auch Michael Ronellenfitsch, hessischer Datenschutzbeauftragter, warnt davor, auf die Horrorszenarien mancher Anwälte hereinzufallen. "In kaum einem Bereich ist die Kenntnis so defizitär."
- **Seehofer setzt auf Verwarnungen statt Geldstrafen**
- Bundesinnenminister Seehofer will Betroffene schützen. Am Dienstag wandte er sich mit einem internen Schreiben an die Landesdatenschutzbeauftragte NRW, Helga Block. In dem Schreiben, das dem *SWR* exklusiv vorliegt, wirbt Seehofer für "verhältnismäßige Sanktionen mit Augenmaß".Es bestehe "Zweifel, ob die kleineren und mittelständischen Betriebe, Vereine oder auch die ehrenamtlich Tätigen, die eben nicht die Möglichkeit haben, sich ausreichend juristisch beraten zu lassen, gleichermaßen gut und schnell konform mit der Grundverordnung agieren werden", heißt es darin. Daraus folgert Seehofer: "Gerade in der Anfangsphase mögen Verwarnungen und Hinweise natürlich unter Berücksichtigung der Umstände und Auswirkungen der Verstöße ausreichend sein, um die Rechtskonformität herzustellen.“ (Tagesschau v. 23.05.2018)

Keine Panik!

„Unser Ziel als Aufsichtsbehörde in NRW ist es dabei, dass die Verantwortlichen rechtskonform handeln. Das ist manchmal schon durch Beratung zu erreichen. Sanktionen wie Geldbußen sind nicht das erste Mittel der Wahl. Geldbußen sind dann erforderlich, wenn unserem Rat nicht gefolgt wird oder wenn es um einen erheblichen Datenschutzverstoß geht. Also: Vorsicht – aber keine Panik! (aus einer eMail der LDI an die KVNO)

GANZ FRISCH:

- **Unionsfraktion hat am 13.06.2018 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages im Rahmen der Empfehlung zum Gesetzentwurf der Fraktionen der CDU/CSU und der SPD zur zivilprozessualen Musterfeststellungsklage einen Ergänzungsantrag vorgestellt, mit dem Abmahnmissbrauch bei mutmaßlichen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) verhindert werden soll. Nachdem die SPD die Sofortmaßnahmen im Zuge des Gesetzes zur Einführung der Musterfeststellungsklage abgelehnt hat, soll nunmehr ein separater Gesetzentwurf hierzu bis zum 1. September 2018 vorgelegt werden.**

Ärztekammer Nordrhein

Einzelfragen Anmeldungsbogen

- **Darf ich Rückrufe tätigen?**
  - **Ja, wenn Patient identifiziert werden kann**
- **Rezepte an bekannten Ehepartner aushändigen?**
  - **Ja, §1357 BGB und mutmaßliche Einwilligung**
- **Nachträgliche Information des Patienten über Kommunikation zwischen Ärzten?**
  - **Nein, Einwilligung vorher nötig**
  - **Anders nur bei mutmaßlicher Einwilligung, wenn Patient einwilligungsunfähig.**
- **Patienten mit Namen aufrufen?**
  - **Jein – eigentlich geschützt. Aber: eigentlich dürften sich auch Patienten in der Praxis nicht begegnen → „Service-Rooms“?**
  - **wohl keine Notwendigkeit, „Abreissnummern“ wie beim Straßenverkehrsamt einzuführen (haben Kollegen gemacht!)**

Einzelfragen Anmeldungsbogen

- **Demente Patienten bisher ohne Betreuer?**
  - **Einwilligungsfähigkeit ≠ Geschäftsfähigkeit**
  - **natürliches Verständnis maßgeblich**
    - wenn (-), Betreuung bei Gericht anregen
- **ausländische Patienten? Aufklärung in anderen Sprachen?**
  - **Wohl ähnlich wie bei der OP-Aufklärung, Thieme-Bögen auch in allen möglichen Sprachen vorhanden**
  - **Kommentar Gola: Deutsch ist Verkehrssprache, *sogar: „In Deutschland ansässige Sprachminderheiten sind nicht zwingend zu berücksichtigen.“***
    - → wenn schon keine Verpflichtung, auf Obersorbisch oder Dänisch zu informieren, dann wohl keinesfalls auf Arabisch

Einzelfragen Anmeldungsbogen

- unverlangt zugesandte Arztbriefe über unbekannte Patienten
  - Information an Absender, sofortiges Shreddern
- Telematikinfrastruktur? Daten bei KV sicher?
  - KV fragen!
- Rezeptbestellung online möglich
  - Ja.
- Gruppentherapie: freiwillige Teilnahme, bedingt stillschweigende Einwilligung in Mitteilung an andere Mittherapierte

Einzelfragen Anmeldungsbogen

- **Versicherung gegen Datenschutzverstöße**
  - **ja, ich habe davon gehört, dass die Versicherungswirtschaft sich hier mit Angeboten vorbereitet (keine Namensnennung)**

Ärztekammer Nordrhein

„Wir schaffen das“

Vielen Dank für die Aufmerksamkeit

Ärztekammer Nordrhein
Rechtsabteilung
Syndikus-RA Claus-Hinrich Buschkamp, LL.M.
Fachanwalt für Medizinrecht
Tersteegenstr. 9
40474 Düsseldorf
0211/4302-2320
Claus.Buschkamp@aekno.de