Daten & Recht

Schutz von Patienteninformationen

AK Medizinrecht des Berliner Anwaltsvereins

Berlin, 14.09.2015

Rechtsanwalt Norman Bäuerle | Daten & Recht

Daten & Recht

Themenüberblick

- Schutz von Patienteninformationen
  - Ärztliche Schweigepflicht/Patientengeheimnis
  - Datenschutz
    - Datenschutz und Informationssicherheit
    - Schutz von Gesundheitsdaten
    - Schutz von Sozialdaten
  - Offenbarungs- und Verarbeitungsbefugnisse
  - Folgen von Datenschutzvorfällen
- Praxisfall: Dioptrienwerte als Kündigungsgrund
- Kurz gehalten: Outsourcing und Praxisverkauf

Daten & Recht

Schutz von Patienteninformationen

Daten & Recht

Auszug aus dem Eid des Hippokrates

benannt nach dem griechischen Arzt Hippokrates von Kos (um 460 bis 370 v. Chr.):

„Was ich bei der Behandlung oder auch außerhalb meiner Praxis im Umgange mit Menschen sehe und höre, das man nicht weiterreden darf, werde ich verschweigen und als Geheimnis bewahren."

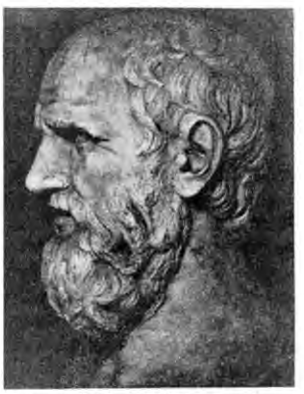


Image: Wellcome Library, London.

Datenschutz

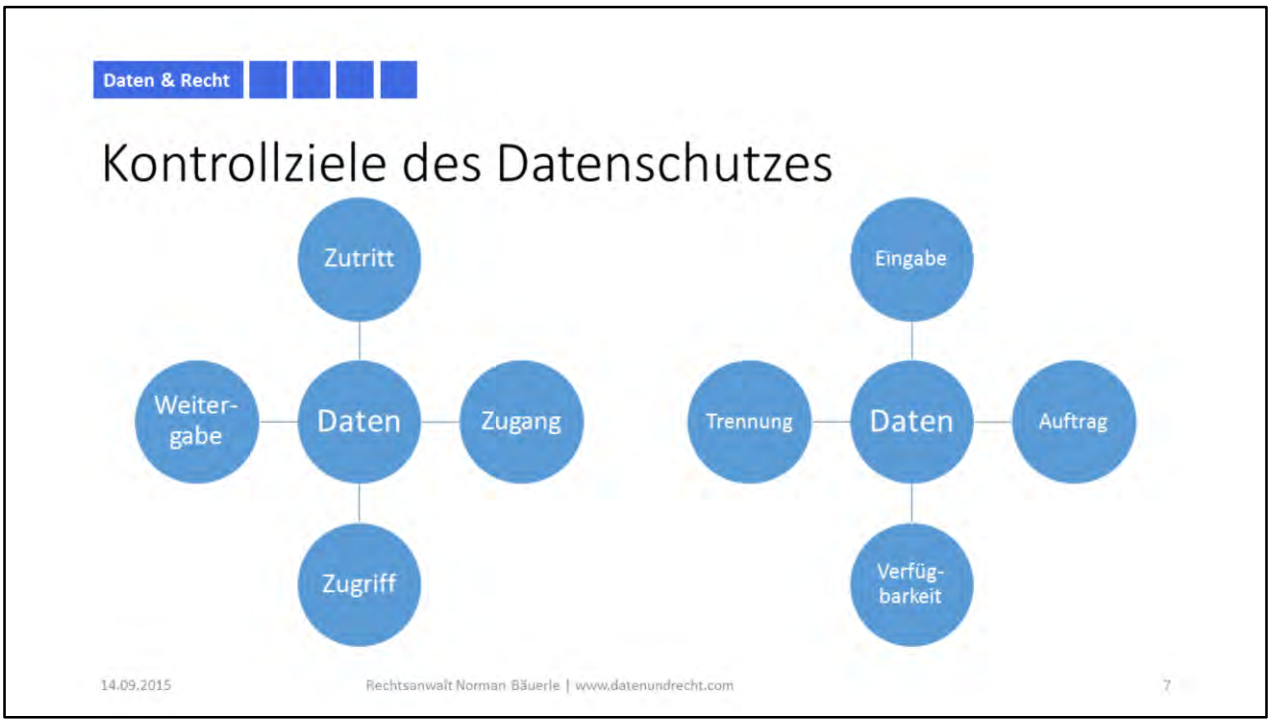
„Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen („informationelles Selbstbestimmungsrecht“).“

Bild: Datenschutz © Marco2811 – Fotolia.com

Daten & Recht

Informationssicherheit und Datenschutz

- **Informationssicherheit** bezeichnet den Schutz der Vertraulichkeit, Verfügbarkeit und Integrität aller (betrieblichen) Daten
- **Datenschutz** dient dem Schutz personenbezogener Daten vor Missbrauch. (Technische) Datensicherheit ist hierfür eine Voraussetzung.



§ 9 BDSG Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

- Unter **technischen Maßnahmen** sind alle Schutzversuche zu verstehen, die im weitesten Sinne physisch umsetzbar sind oder Maßnahmen die in Soft- und Hardware umgesetzt werden.
- Als **organisatorische Maßnahmen** sind solche Schutzversuche zu verstehen die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden.

Anlage (zu § 9 Satz 1) BDSG

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen

personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

§ 9 Berufsordnung: Schweigepflicht

(1) Ärztinnen und Ärzte haben über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt **anvertraut oder bekannt geworden** ist – auch über den Tod der Patientin oder des Patienten hinaus – zu schweigen.

(2) Ärztinnen und Ärzte sind zur Offenbarung befugt, soweit sie von der Schweigepflicht entbunden worden sind, soweit eine gesetzliche Vorschrift dies vorsieht oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist. Soweit gesetzliche Vorschriften die Schweigepflicht der Ärztin oder des Arztes einschränken, soll die Ärztin oder der Arzt die Patientin oder den Patienten darüber unterrichten.

(3) Mitarbeiterinnen und Mitarbeiter sowie die Personen, die zur Vorbereitung auf den Beruf an der ärztlichen Tätigkeit teilnehmen, sind über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und zur Einhaltung zu verpflichten.

§ 203 StGB: Schutz 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.

(3) […] Den in Absatz 1 und Satz 1 Genannten stehen ihre berufsmäßig tätigen **Gehilfen** und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind. Den in Absatz 1 und den in Satz 1 und 2 Genannten steht nach dem Tod des zur Wahrung des Geheimnisses Verpflichteten ferner gleich, wer das Geheimnis von dem Verstorbenen oder aus dessen **Nachlaß** erlangt hat.

Offenbarungsbefugnis

1. § 11 BDSG Datenverarbeitung im Auftrag: nein
2. **Wirksame Einwilligung des Geheimnisgeschützten**, Entbindung von der Schweigepflicht (Fischer, StGB, § 203 Rn. 32 ff.)
    1. Ausdrückliche und konkludente Einwilligung
        1. Fähigkeit, die Bedeutung der Erklärung zu verstehen, sodass auch

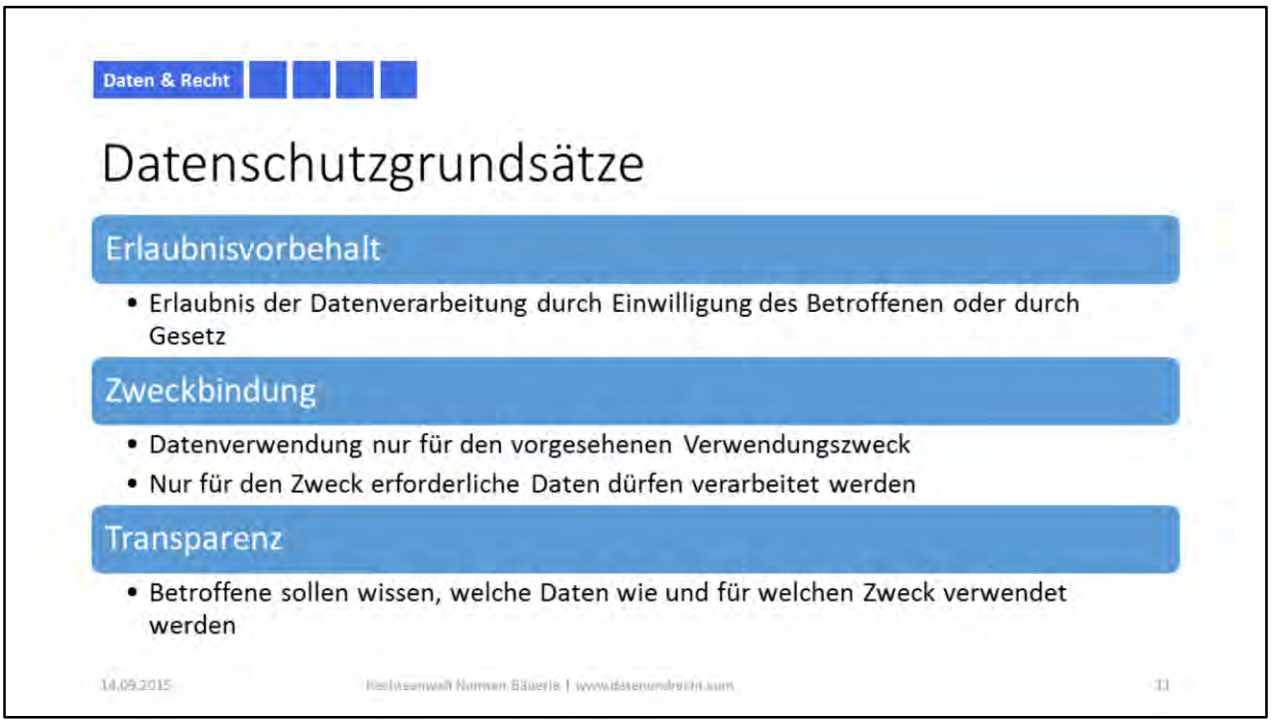
Minderjährige – auch gegen den gesetzlichen Vertreter – die Einwilligung wirksam erklären kann.
2. Grds. keine Formerfordernisse, sodass auch eine konkludente Einwilligung möglich ist, beispielsweise wenn der Betroffene an Abläufen mitwirkt, die ihrer Natur nach das Offenbaren von Geheimnissen voraussetzen (z. B. Überweisung an Facharzt zur Klärung eines Verdachts) oder ohne Offenbarung ihren Sinn verlieren würden (z. B. Mitteilung der fachärztlichen Feststellungen an den überweisenden Hausarzt).

1. Mutmaßliche Einwilligung
    1. Jede – auch konkludente – Erklärung des Berechtigten fehlt oder ist unmöglich, beispielsweise wegen Unerreichbarkeit, krankheitsbedingter Unfähigkeit oder Tod.
    2. Offensichtliches Interesse des Betroffenen.

3. Gesetzliche Offenbarungspflichten

Bild: Strafakte mit Gesetzbuch © Gerhard Seybert – Fotolia.com

Schutz des Persönlichkeitsrechts



Verbot mit Erlaubnisvorbehalt

Die Verarbeitung von personenbezogenen Daten steht unter einem Erlaubnisvorbehalt (§ 4 Abs. 1 BDSG).

Jede Verarbeitung personenbezogener Daten bedarf demnach einer besonderen **Legitimierung**:

- Einwilligung des Betroffenen
- Gesetzliche Erlaubnis oder Anordnung

Zweckbindung

Daten dürfen nur für einen bestimmten Zweck erhoben und verwendet werden. Jede zweckwidrige Nutzung ist unzulässig.

Anforderungen:

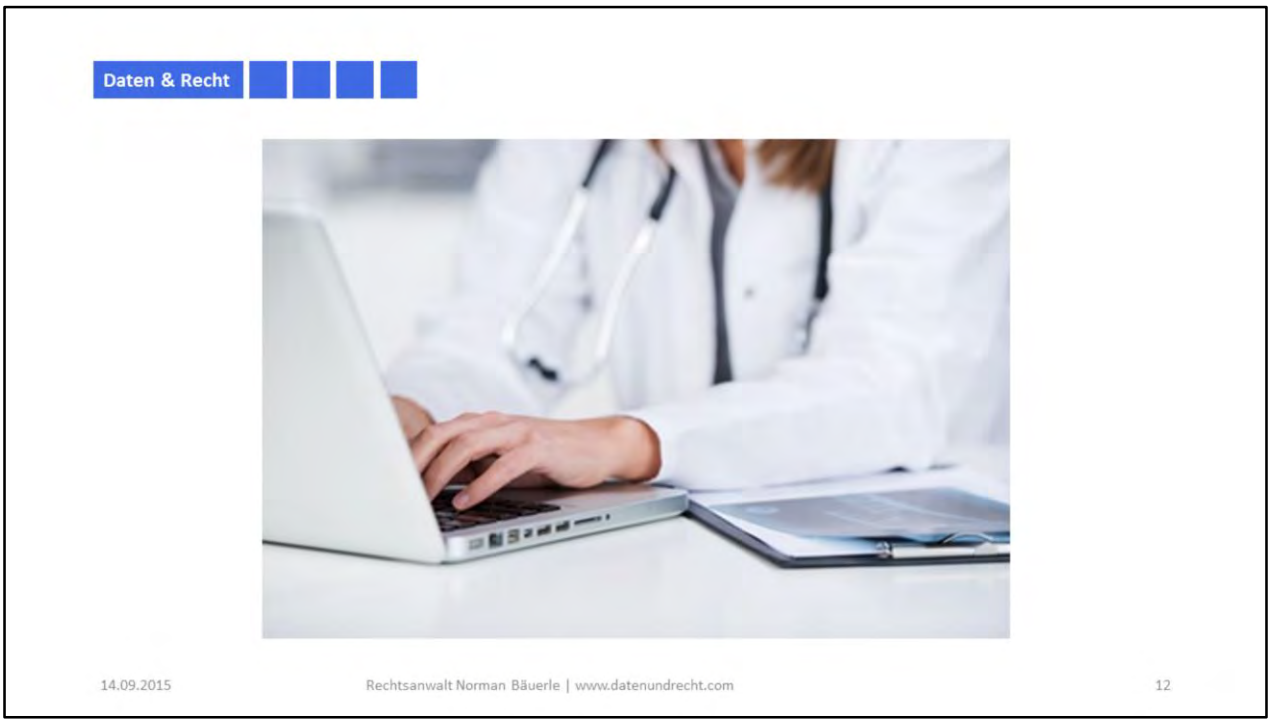
- Zweckbestimmung
- Erforderlichkeit, intern „Need-to-know-Prinzip“
- Grundsätzlich Zweckbindung, Zweckänderung nur mit Einwilligung des Betroffenen oder gesetzlicher Befugnis (beispielsweise § 28 Abs. 2 BDSG)
- Datenlöschung nach Erfüllung des Zwecks (§ 35 BDSG)

auch

- Erforderlichkeit/Verhältnismäßigkeit
- Datenvermeidung und Datensparsamkeit, § 3a BDSG

Transparenz

- Grundsatz der Betroffenenerhebung/Direkterhebung
- Betroffenenrechte (§§ 6, 33,34, 35 BDSG, dazu später)
- Informationspflicht der verantwortlichen Stelle bei unrechtmäßiger Kenntniserlangung von Daten (§ 42a BDSG)
- Verfahrensverzeichnisse (§ 4g Abs. 2 BDSG)



Schutz von Patienteninformationen

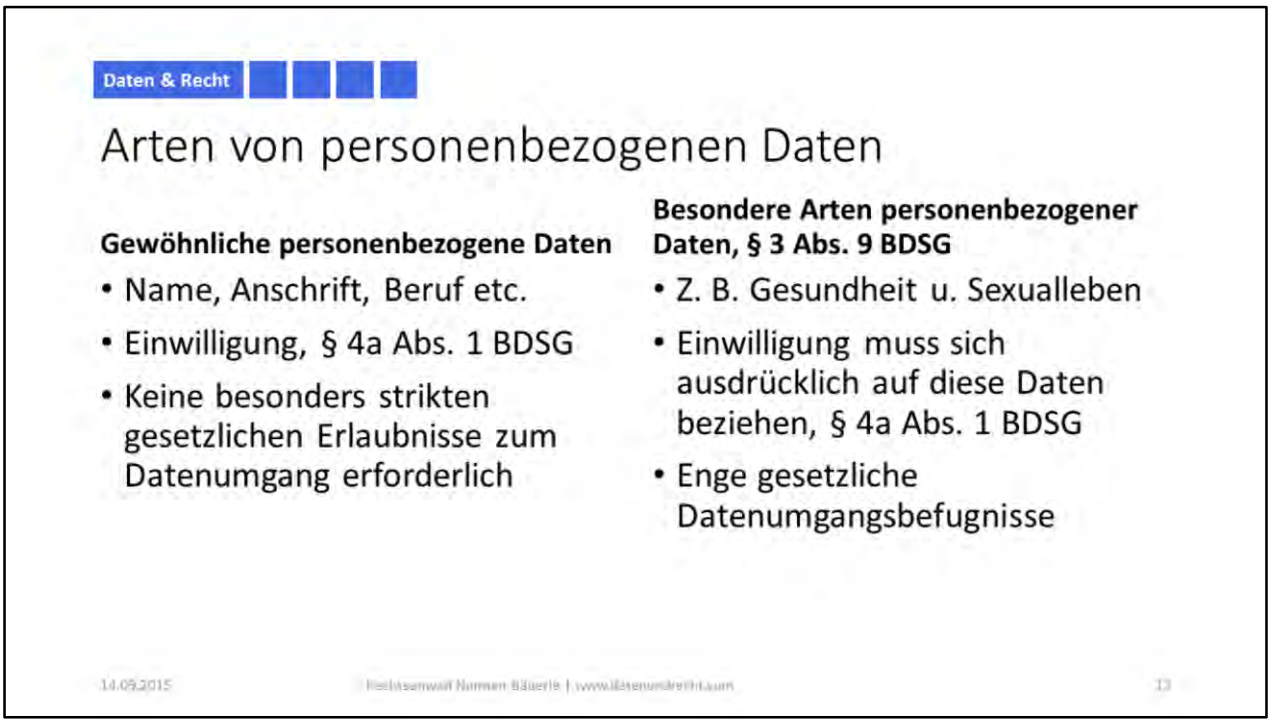
1. Ärztliche Verschwiegenheitspflicht (§ 9 Berufsordnung), Patientengeheimnis (§ 203 StGB)

2. Datenschutz besonderer Arten personenbezogener Daten

- Legaldefinition (§ 3 Abs. 9 BDSG): „Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben."
- **Kritik:** Abstrakte Kategorisierungen verleiten leicht zu falschen Schlüssen. Ob Daten „trivial" oder „sensitiv" sind, lässt sich nicht an wie immer zusammengestellten Listen ablesen, sondern allein dem Verwendungszusammenhang entnehmen (Simitis, Bundesdatenschutzgesetz, BDSG § 3 Rn. 250 - 265, beck-online).
- Verarbeitung: § 28 Abs. 6 bis 9 BDSG

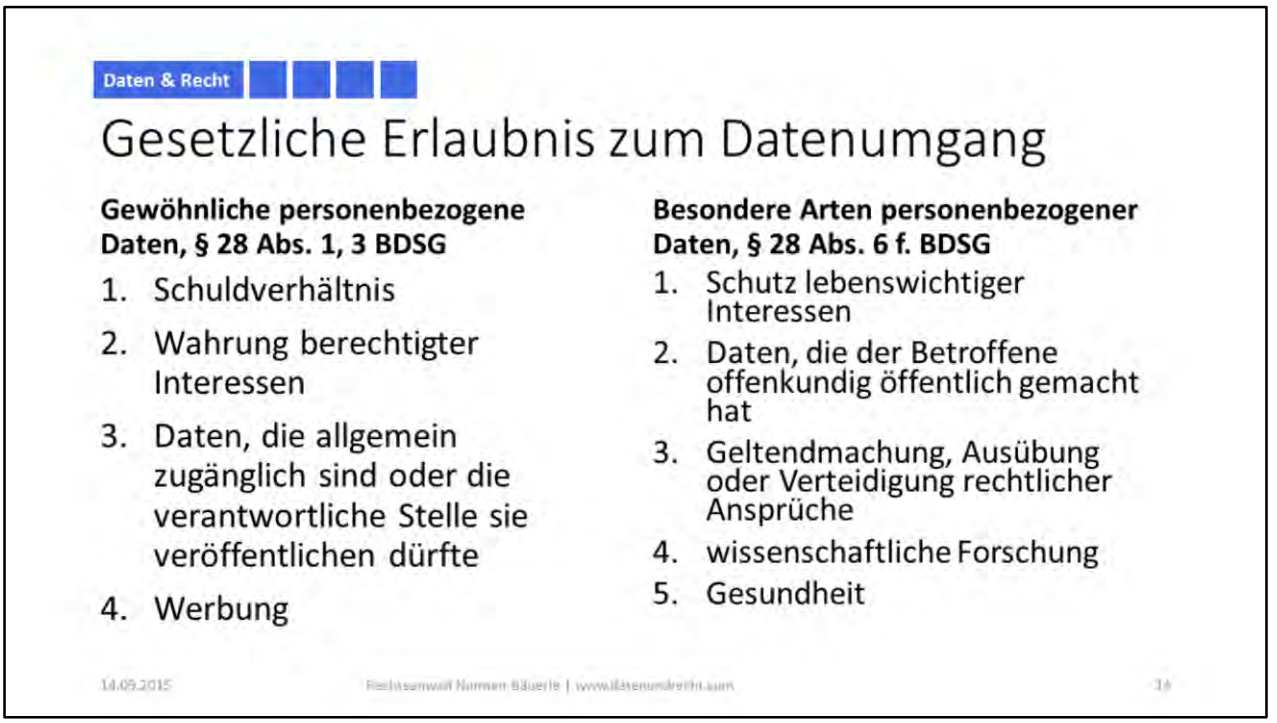
3. Sozialgeheimnis (§ 35 SGB 1), Sozialdatenschutz (§§ 67 ff. SGB 10)
gesetzlich versicherter Patienten: Erstes, Fünftes und Zehntes Buch Sozialgesetzbuch.

Bild: Ärztin schreibt am Laptop: © contrastwerkstatt – Fotolia.com



§ 3 Abs. 9 BDSG

„Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben."



Datenverarbeitungsbefugnisse

Nach Art. 8 Abs. 1 RL 95/46/EG ist die Verarbeitung besonderer Kategorien personenbezogener Daten grds. untersagt. Dieses Verbot wird durch einzelne gesetzliche Erlaubnistatbestände durchbrochen, etwa wenn die Verarbeitung zum Zweck der Gesundheitsvorsorge oder der medizinischen Diagnostik erforderlich ist und die Verarbeitung durch ärztliches Personal erfolgt.

Gewöhnliche personenbezogene Daten, § 28 Abs. 1 bis 5 BDSG

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die **Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses** mit dem Betroffenen erforderlich ist,
2. soweit es zur **Wahrung berechtigter Interessen** der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die **Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte**, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

[…]

Besondere Arten personenbezogener Daten, § 28 Abs. 6 bis 9 BDSG

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum **Schutz lebenswichtiger Interessen** des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
2. es sich um Daten handelt, **die der Betroffene offenkundig öffentlich** gemacht hat,
3. dies **zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche** erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
4. dies zur **Durchführung wissenschaftlicher Forschung** erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der **Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten** erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuchs genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

[…]

<u>Zweckänderungen</u>

Normale personenbezogene Daten, § 28 Abs. 2 BDSG

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 [Wahrung berechtigter Interessen] oder Nummer 3 [allgemein zugängliche Daten],
2. soweit es erforderlich ist,
    a) zur Wahrung berechtigter Interessen eines Dritten oder
    b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten

   und kein Grund zu der Annahme besteht, dass der Betroffene ein

schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Besondere Arten personenbezogener Daten, § 28 Abs. 8 BDSG

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

Daten & Recht

Mitteilung gemäß § 42a Bundesdatenschutzgesetz

Im Kreiskrankenhaus Rastatt, Baden-Württemberg, wurden am Mittwoch, den 19.09.2012, zur Archivierung vorgesehene Datensicherungsbänder durch eine bislang unbekannte Person entwendet. Die Datensicherungsbänder konnten trotz intensiver Bemühungen bis heute nicht zurückerlangt werden. Der Vorfall ist dem Kreiskrankenhaus Rastatt am 27.09.2012 bekannt geworden.

Betroffene Daten:

Betroffen sind Daten der Patienten des Kreiskrankenhauses Rastatt, sowie des Medizinischen Versorgungszentrums der Klinikum Mittelbaden (MVZ) GmbH, jeweils Engelstraße 39, 76437 Rastatt.

Art der Daten:

Betroffen sind alle im Rahmen der Behandlung bzw. des Aufenthalts in den genannten Häusern angefallenen und erfassten Daten, somit Namen, Adressen, Kontaktdaten, Geburtsdaten, Befunde, ärztlicher Briefwechsel, klinkinterner Schriftwechsel und dergleichen.

Getroffene Maßnahmen:

Strafanzeige gegen Unbekannt wurde erstattet. Maßnahmen zur Wiedererlangung der Bänder, sowie zur Verhinderung eines Wiederholungsfalles sind in die Wege geleitet. Die zuständige Aufsichtsbehörde ist informiert.

Empfehlungen von Maßnahmen zur Minderung möglicher nachteiliger Folgen:

Alle aktuellen oder früheren Patienten der genannten Häuser sollten in der nächsten Zeit besonders aufmerksam auf verdächtige oder unerwartete Kenntnis Dritter von ihren Daten, insbesondere auch den Gesundheitsdaten, achten.

Alle Unregelmäßigkeiten sollten bitte den genannten Häusern zur Aufklärung des Sachverhalts und Schadensminderung mitgeteilt werden.

Vielen Dank

Die Träger:

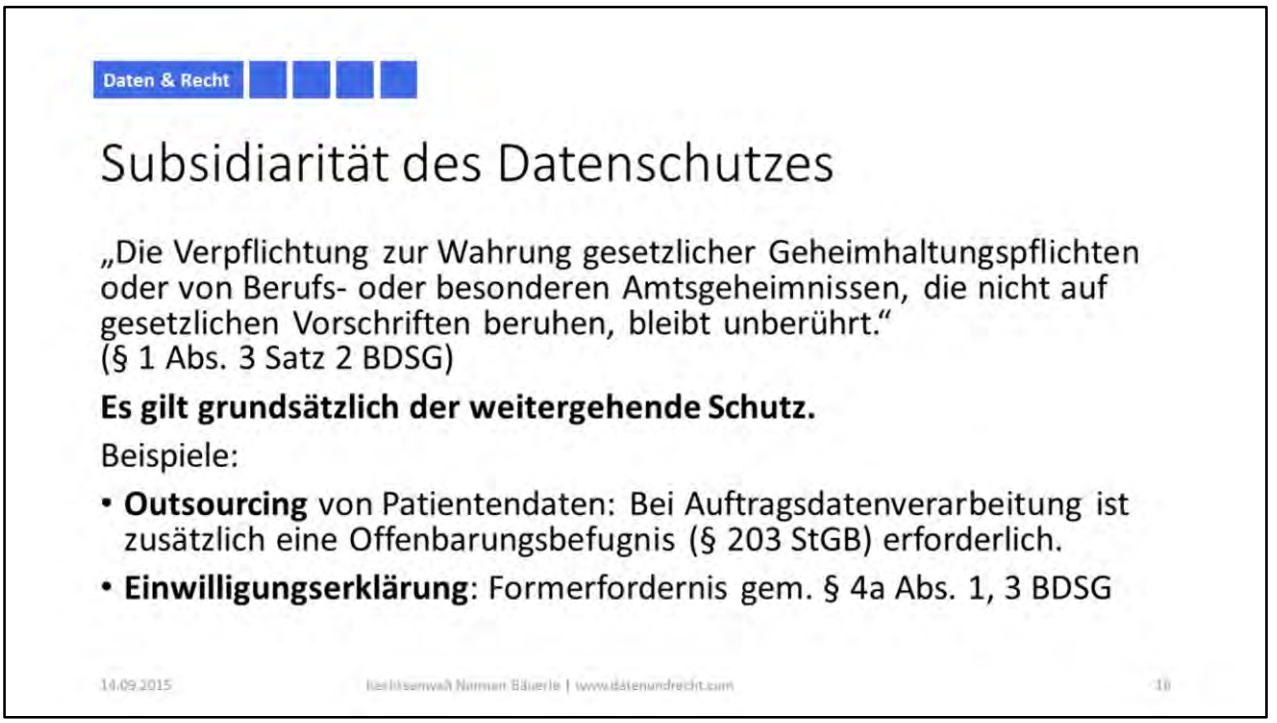
KLINIKUM MITTELBADEN

Klinikum Mittelbaden gGmbH
Balger Straße 50
76532 Baden-Baden
(Träger des Kreiskrankenhauses Rastatt)

MVZ MEDIZINISCHES VERSORGUNGS-ZENTRUM GMBH

Klinikum Mittelbaden MVZ GmbH
Balger Straße 50
76532 Baden-Baden
(Träger des Medizinischen Versorgungszentrums Rastatt)

http://www.klinikum-mittelbaden.de/internet/pdf/Mitteilung-KKH-RA-in-FR.pdf



Verhältnis Datenschutz und besondere Geheimhaltungspflichten

- Wo der Schutz der besonderen Geheimhaltungspflichten weitergehend als der des BDSG ist, gilt dieser weitergehende Schutz.
- Ist das Schutzniveau gleich, gibt es keine Besonderheiten.
- Ist das Schutzniveau der speziellen Geheimhaltungsregelung geringer, gilt für Daten, die unter das BDSG fallen, dieses Gesetz.
- In allen anderen Fällen gilt der Schutz der speziellen Geheimhaltungsregelung.

(Gola/Schomerus/Klug/Körffer/Gola BDSG § 1 Rn. 23-25, beck-online)

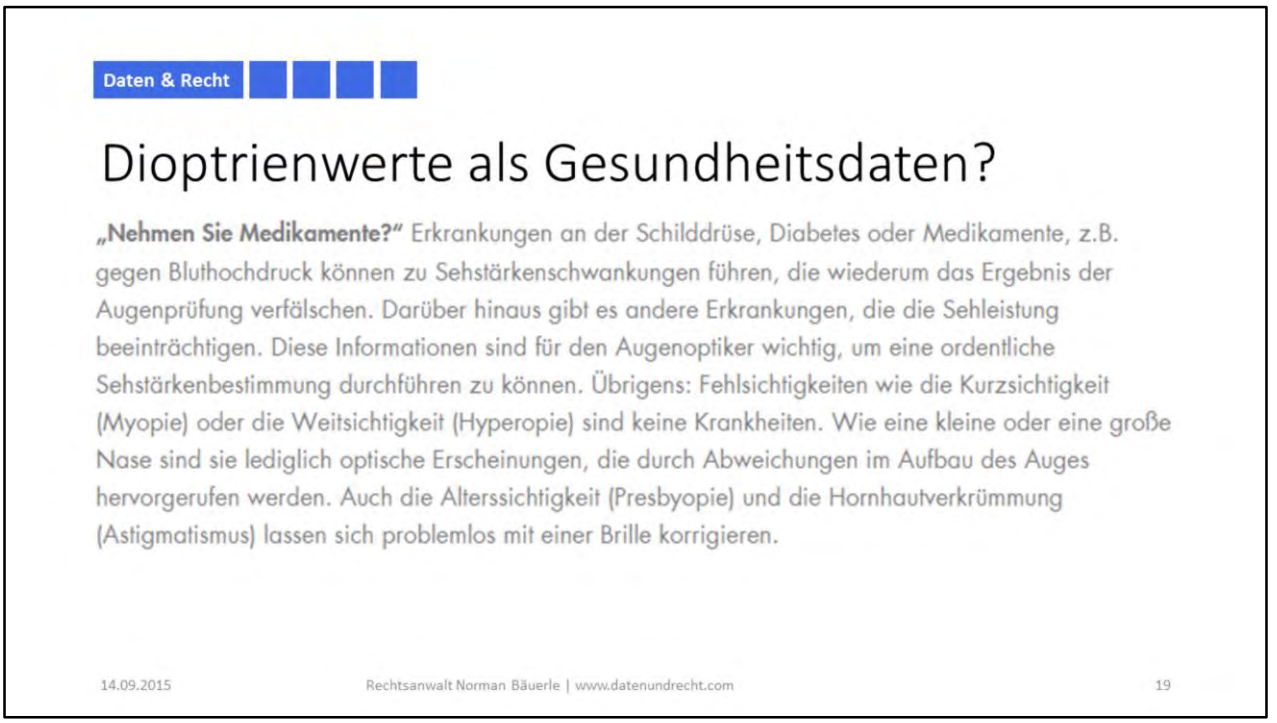
Daten & Recht

Praxisfall:
Dioptrien als Kündigungsgrund

Daten & Recht

Sachverhalt

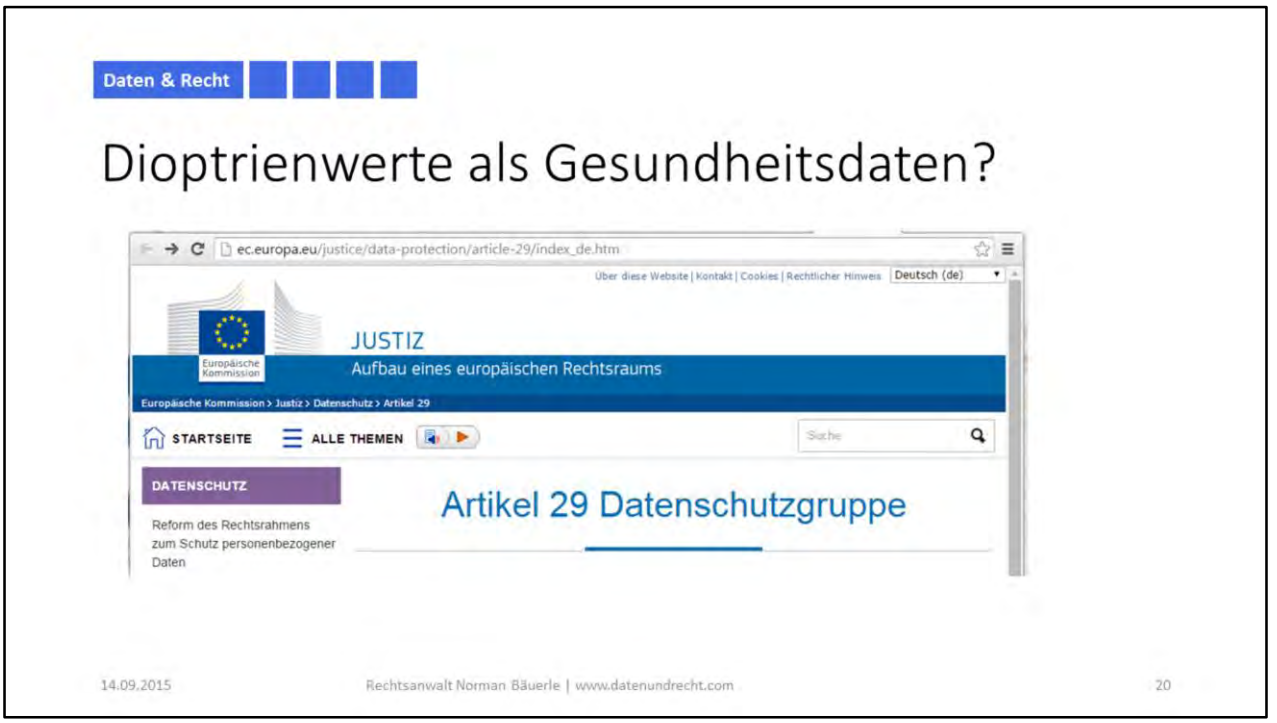
- Angestellter Augenoptiker bestellt mit dem nur ihm persönlich gewährten Mitarbeiterrabatt Kontaktlinsen für seine Ehefrau.
- Der Arbeitgeber sucht nach einem Kündigungsgrund. Bei einem Abgleich der Dioptrien, bei dem auch die Dioptrienwerte der Ehefrau herangezogen werden, fällt der Betrug des Mitarbeiters auf. Es folgt die fristlose Kündigung.
- Der Arbeitgeber vertritt die Auffassung, die Dioptrienwerte seien reine Verkaufsdaten. Der Abgleich sei zulässig gewesen.



Quelle: fielmann.de, http://www.fielmann.de/brillen/weg-zur-brille/augenglasbestimmung/

Brille als Gesundheitsdatum?

- Sitzt auf der Nase.
- Ist auf jedem Foto sichtbar.



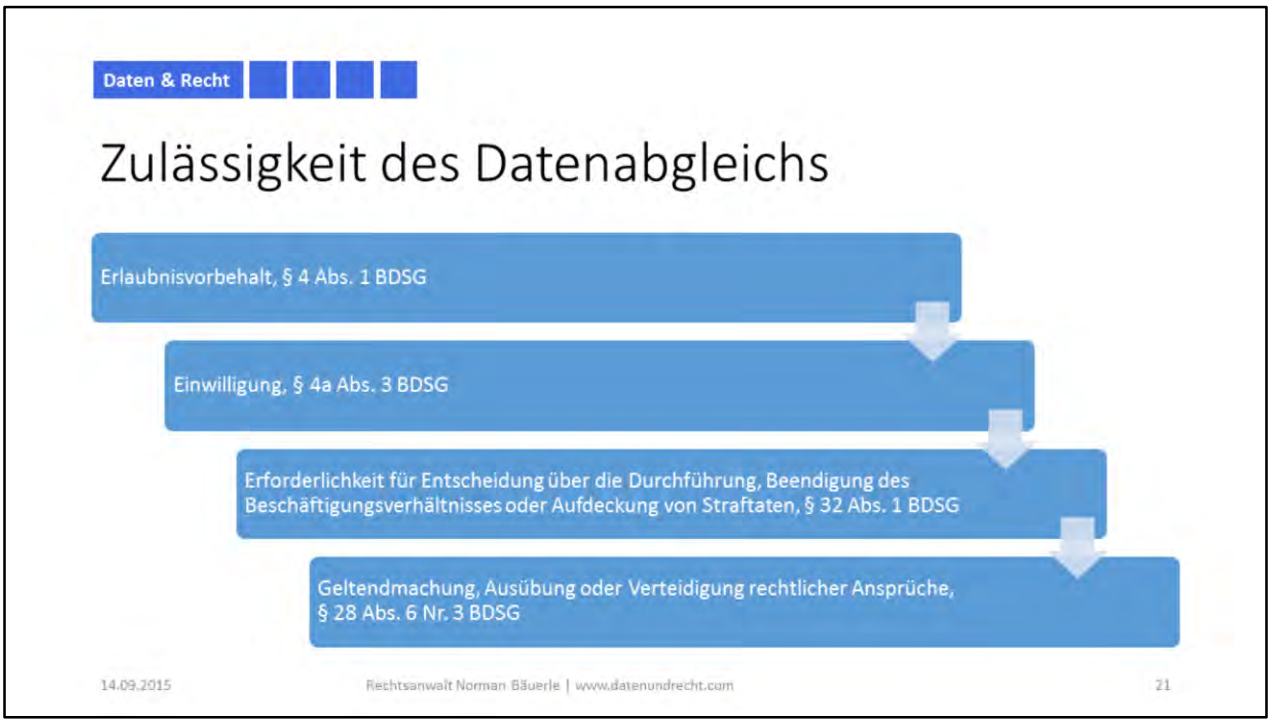
Art. 29-Datenschutzgruppe: Stellungnahme zu Gesundheitsdaten

Die Art. 29-Datenschutzgruppe hat eine Stellungnahme zu Gesundheitsdaten veröffentlicht, in der neben der Definition die möglichen Risiken einer Verarbeitung dieser Daten und die gesetzlichen Grundlagen behandelt werden.

Die *Art. 29-Datenschutzgruppe* definiert Gesundheitsdaten als Daten über den physischen oder psychischen Zustand, die (auch nur bedingt) im Zusammenhang mit einem medizinischen Kontext entstehen können. Darunter fallen auch Information über Unfälle (Beinbruch), **Sehverhalten (Brille oder Kontaktlinsen)**, über intellektuelle oder mentale Fähigkeiten (IQ), zu Trink- oder Rauchverhalten, Allergien oder Beteiligung an einer Selbsthilfegruppe (Weight Watchers, Anonyme Alkoholiker etc.).

https://beck-online.beck.de/Default.aspx?vpath=bibdata/zeits/zdaktuell/2015/cont/zdaktuell.2015.04548.htm

„Ich willige ein, dass zu diesem Zweck ein Porträtfoto von mir ins Internet eingestellt und in gedruckte Werbematerialien aufgenommen wird. Soweit sich aus meinem Foto Hinweise auf meine ethnische Herkunft, Religion oder **Gesundheit** ergeben (z. B. Hautfarbe, Kopfbedeckung, **Brille**), bezieht sich meine Einwilligung auch auf diese Angaben.“ (Bergt in Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, Einwilligungserklärung zur Veröffentlichung von Mitarbeiterfotos)



Zu klären: Liegt möglicherweise eine (konkludente) Einwilligung der Ehefrau in den Datenabgleich vor?

§ 32 BDSG: Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

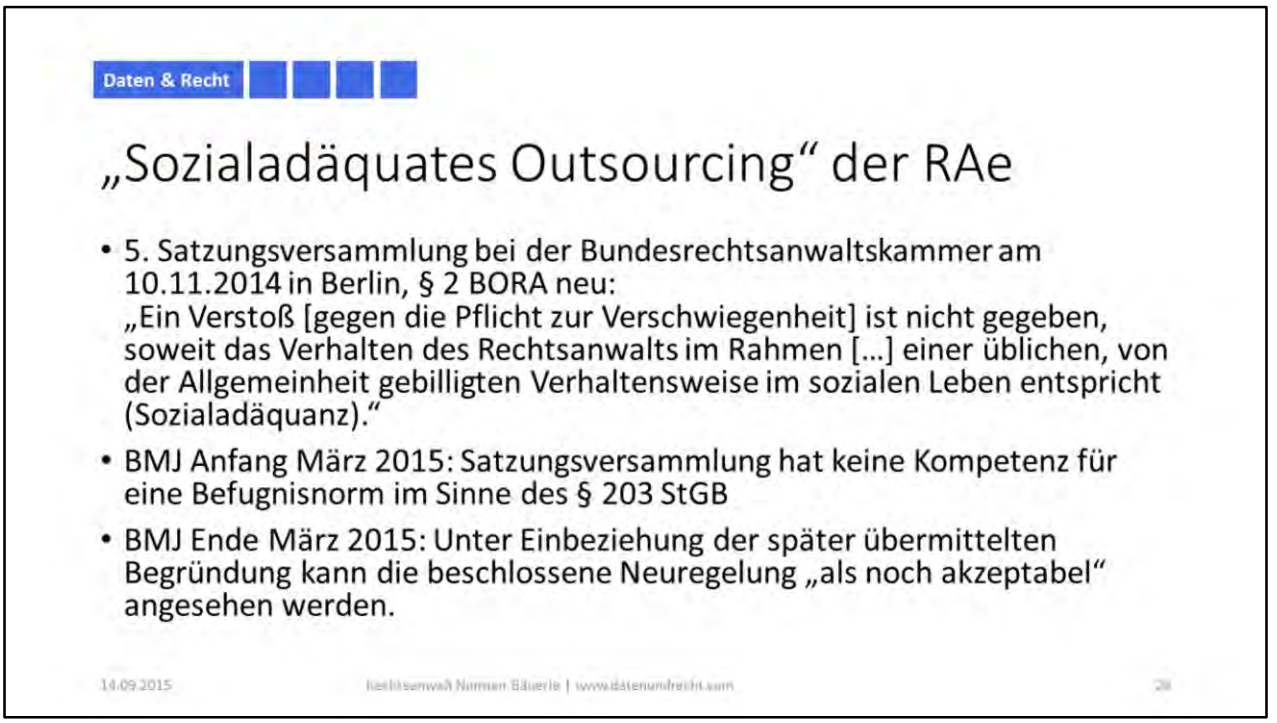
Daten & Recht

Praxisfall: Dioptrien als Kündigungsgrund

- Schadensersatzpflichten
  - § 7 BDSG
  - § 280 Abs. 1 BGB i.V.m. § 32 Abs. 1 BDSG
  - § 823 Abs. 1 BGB (allgemeines Persönlichkeitsrecht)
  - § 823 Abs. 2 i.V.m. § 32 BDSG
- Unterlassungs- und Beseitigungsansprüche, § 1004 BGB analog
- Beweisverwertungsverbot
- Eingreifen der Aufsichtsbehörde, § 38 BDSG

Daten & Recht

Kurz gefasst:
Outsourcing und Praxisübergabe



5. Satzungsversammlung bei der Bundesrechtsanwaltskammer am 10./11.11.2014 in Berlin zu § 2 BORA

„Sozialadäquates Outsourcing“

§ 2 BORA neu: „Ein Verstoß [gegen die Pflicht zur Verschwiegenheit] ist nicht gegeben, soweit das Verhalten des Rechtsanwalts im Rahmen der Arbeitsabläufe der Kanzlei einschließlich der Inanspruchnahme von Leistungen Dritter erfolgt und objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht (Sozialadäquanz).“

BRAK, Nachrichten aus Berlin, Ausgabe 6/2015 v. 20.3.2015

Teilbeanstandung zu § 2 BORA

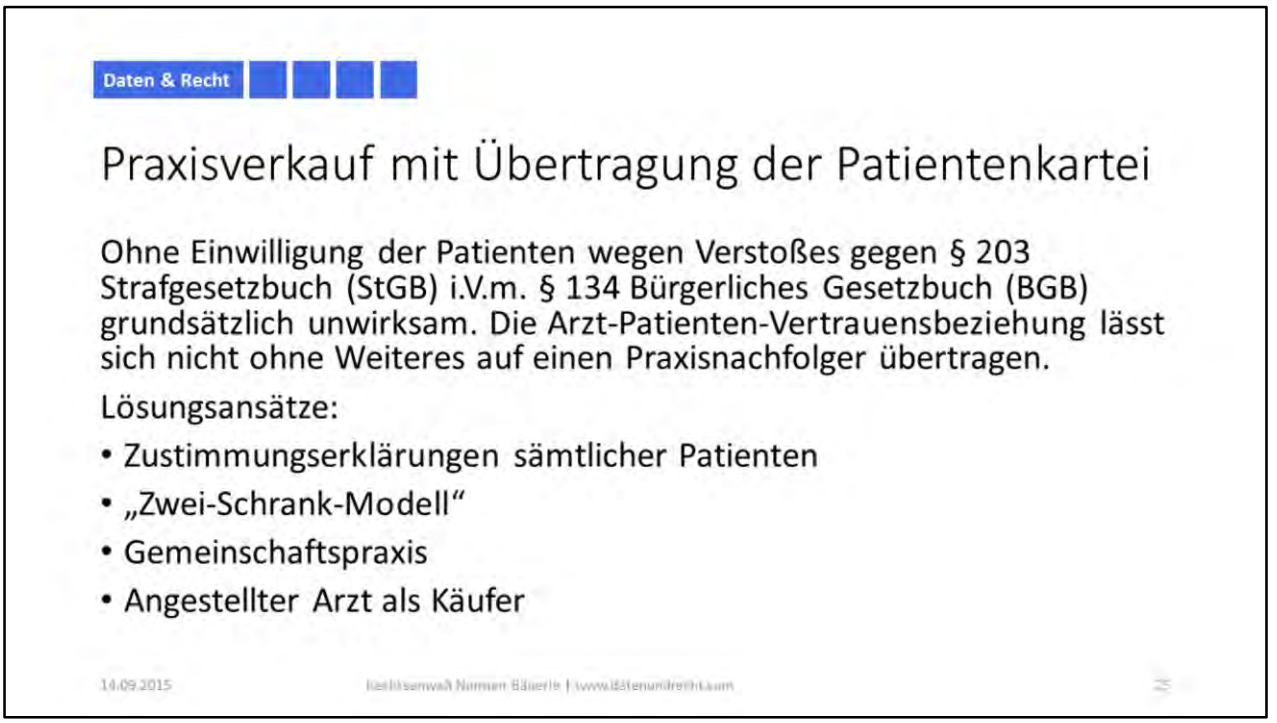
Der Bundesjustizminister hat den im November gefassten Beschluss der Satzungsversammlung zur Neuregelung des § 2 BORA (Anwaltliche Verschwiegenheit) teilweise beanstandet und aufgehoben. […] Nach Ansicht des Bundesjustizministeriums enthält diese Regelung jedoch eine Befugnisnorm im Sinne des § 203 StGB, zu deren Erlass der Satzungsversammlung die Kompetenz fehle. Da ein „sozialadäquates Verhalten“ auch kein anerkannter Rechtsfertigungsgrund im Rahmen des § 203 StGB sei, könne der Gedanke der Sozialadäquanz allenfalls Grundlage eine gesetzliche Befugnisnorm im Sinne des § 203 StGB sein, heißt es im Schreiben des Ministeriums. Der Minister bietet jedoch gleichzeitig Gespräche über eine mögliche gesetzliche Regelung an.

BRAK, Nachrichten aus Berlin, Ausgabe 7/2015 v. 10.04.2015

§ 2 BORA-neu

Bundesjustizminister Maas hat in einem Schreiben vom 31.03.2014 mitgeteilt, dass der Teilaufhebungsbescheid des im vergangenen November von der Satzungsversammlung beschlossenen neuen § 2 BORA aufgehoben wird. […] In dem Schreiben vom 31.03.2015 heißt es jetzt, dass eine erneute Prüfung unter Einbeziehung der später übermittelten Begründung der Beschlussvorlage ergeben habe, dass die beschlossene Neuregelung „als noch akzeptabel“ angesehen werden könne und deshalb der frühere Aufhebungsbescheid aufgehoben wird. Damit tritt § 2 BORA, wie auch die anderen Beschlüsse der Novembersitzung am 01.07.2015 in Kraft.

Quellen:
http://www.brak.de/w/files/01_ueber_die_brak/5sv/141117-beschluesse-7-sitzung-5-sv_fuer-internet-1.pdf
http://www.brak.de/zur-rechtspolitik/newsletter/nachrichten-aus-berlin/2015/ausgabe-7-2015-v-10042015.news.html
http://www.brak.de/zur-rechtspolitik/newsletter/nachrichten-aus-berlin/2015/ausgabe-6-2015-v-2032015.news.html



Praxisübergabe

Offenbarungsbefugnis (Fischer, StGB, § 203 Rn. 33a)

Keine konkludente Einwilligung der Patienten:

- Das Schweigen auf die Anzeige der Übernahme einer Praxis in der Tagespresse reicht – selbst wenn jeder Patient davon Kenntnis genommen hätte – als konkludente Erklärung des Einverständnisses nicht aus (a. A. werden vertreten).
- Bei Praxisübergaben kann eine konkludente Einwilligung der Patienten nicht angenommen werden.

„Zwei-Schrank-Modell“

ULD, Übergabe einer Arztpraxis mit Patientenakten, https://www.datenschutzzentrum.de/material/themen/gesund/uebergab.htm

„Aus Praktikabilitätsgründen wurde für die Praxisübergabe bei manuell geführten Patientenkarteien das **"Zwei-Schrank-Modell"** entwickelt, das **vom ULD toleriert** wird. Der Veräußerer behält grds. die informationsrechtliche Verfügungsbefugnis an den Altakten und übergibt sie in einem verschlossenen Schrank dem Erwerber, der sich wiederum im Übernahmevertrag speziell verpflichtet, die Kartei für den Veräußerer zu verwahren und nur fallbezogen Zugriff auf einzelne Akten zu nehmen, wenn eine frühere Patientin oder ein früherer Patient ihn zur Behandlung aufsucht. Die alte Akte darf dann bei einem entsprechenden Einverständnis dieses Patienten entnommen und durch den Erwerber fortgeführt werden bzw. mit einer laufenden

Patientenkartei des Erwerbers zusammengeführt werden. Das Einverständnis ist in der Akte zu dokumentieren. Dies bedeutet, dass für den Nachfolger die datenschutzrechtliche Verfügungsbefugnis über die Alten nur eingeschränkt besteht, unabhängig davon, ob bzw. für welchen Zeitpunkt ein sachenrechtlicher Eigentumsübergang verabredet wird.

Bei diesem Modell wird also unterschieden zwischen der Übertragung des generellen **Gewahrsams an dem Gesamtaktenbestand** und der daten-/patientenschutzrechtlich wesentlich sensibleren **konkreten Einsichtnahme**."

Daten & Recht

Links zum Vortrag: https://datenundrecht.com/?p=686

Rechtsanwalt Norman Bäuerle
IT-Recht | Compliance | Datenschutz
Schloßstraße 41A
12165 Berlin
baeuerle@datenundrecht.com
+49 30 577055240