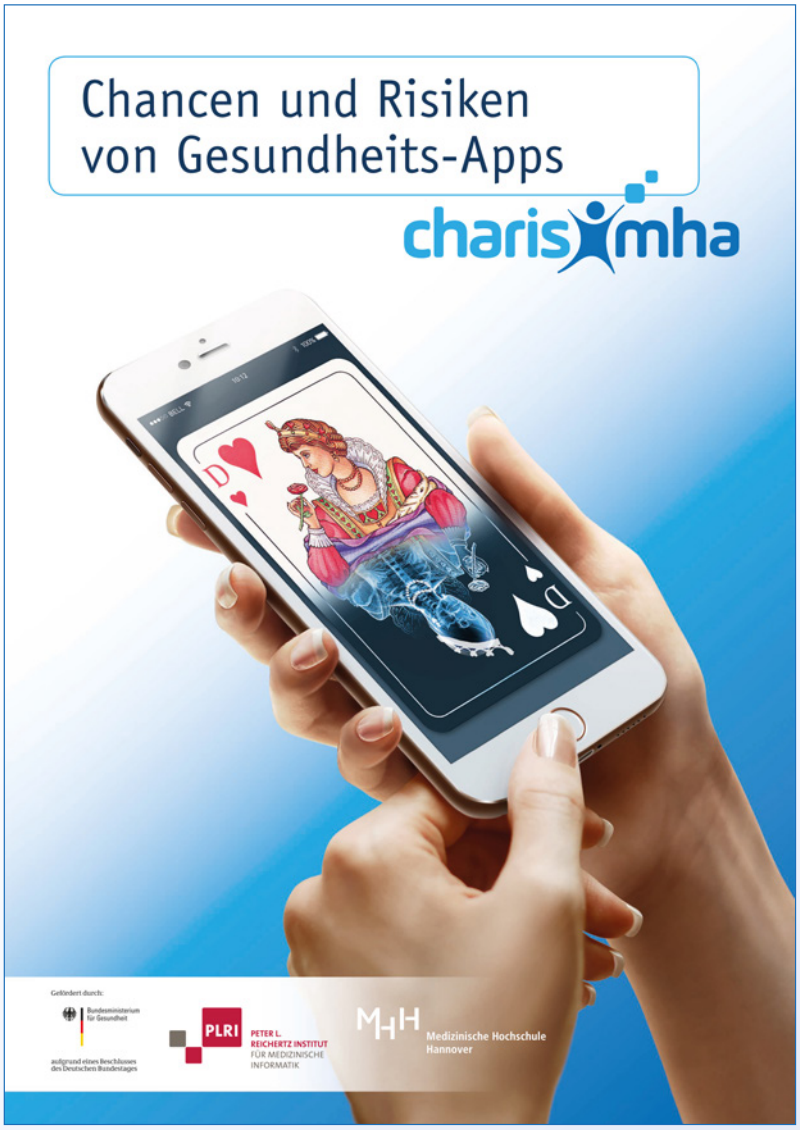
# Kapitel 10 **Gesundheits-Apps und Datenschutz**

Oliver Pramann

www.charismha.de

**aus:**




**Zitieren als:**
Pramann, O.: Kapitel 10. Gesundheits-Apps und Datenschutz. In: Albrecht, U.-V. (Hrsg.), Chancen und Risiken von Gesundheits-Apps (CHARISMHA). Medizinische Hochschule Hannover, 2016, S. 214–227. urn:nbn:de:gbv:084-16040811405.
http://www.digibib.tu-bs.de/?docid=60016

Version: V.01.3 - 20160424

Kapitel 10

# Gesundheits-Apps und Datenschutz

Oliver Pramann

**Zitieren als:**
**Pramann, O.: Kapitel 10. Gesundheits-Apps und Datenschutz. In: Albrecht, U.-V. (Hrsg.), Chancen und Risiken von Gesundheits-Apps (CHARISMHA). Medizinische Hochschule Hannover, 2016, S. 214–227. urn:nbn:de:gbv:084-16040811405. http://www.digibib.tu-bs.de/?docid=60016**

## 1 Ziele

Das vorliegende Kapitel beschreibt die aktuellen rechtlichen Rahmenbedingungen für den Schutz von Gesundheitsdaten in Deutschland in Bezug auf Gesundheits-Apps. Ausgehend vom Schutzgut und den Entwicklungen des Datenschutzrechts werden die maßgeblichen Rechtsgrundlagen des Datenschutzrechts allgemein und im Speziellen mit Gesundheitsbezug sowie die rechtlichen Voraussetzungen für die Datenerhebung und -verarbeitung und -nutzung sowie der spezielle Schutz vulnerabler Gruppen dargestellt. Abschließend wird auch in Ansehung des häufig gegebenen Auslandsbezugs bei Apps dieser Kontext beleuchtet. Auf dieser Grundlage sind folgernd die gegebenen Rechtsgrundlagen im Hinblick auf Gesundheits-Apps zu bewerten[1].

## 2 Einführung

Die Nutzung von Apps ist regelmäßig mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten verbunden. Der einfache Zugang zu entsprechenden Anwendungen, deren breite Nutzungsmöglichkeiten und die Undurchsichtigkeit der Vorgänge im Umgang mit den persönlichen Informationen der Nutzerinnen und Nutzer werfen viele Fragen im Hinblick auf die Zulässigkeit der Prozesse der Datenerhebung, -verarbeitung und -nutzung auf. Hinzu tritt, dass oftmals grenzüberschreitende Sachverhalte betroffen sind, was die Beantwortung dieser Fragen noch schwieriger gestaltet.

Die Bedeutung des Datenschutzes bekommt darüber hinaus noch eine andere Dimension, wenn über Apps sensible gesundheitsbezogene Informationen erhoben und verarbeitet werden. Beim Einsatz von medizinischen Apps/Gesundheits-Apps spielen mitunter datenschutzrechtliche Aspekte damit eine entscheidende Rolle. Die hiermit verbundenen Probleme sind Gegenstand der nachfolgenden Ausführungen.

## 3 Problemstellung

Im Allgemeinen wird die Nutzung von Apps mit Blick auf Datenschutz- und Sicherheitslücken sehr kritisch betrachtet. Auf eine kleine Anfrage an die Bundesregierung (Korte et al. 2012) wurde als Antwort konstatiert, dass Apps ein Sicherheitsrisiko für Smartphones seien (Bundesregierung 2012). Entsprechende weitere Äußerungen der Datenschutzgruppe, dem Beratungsgremium der Europäischen Union, haben einen identischen Tenor (Datenschutzgruppe 2013). Hiernach werden bei einer großen Anzahl von Apps auf die auf dem mobilen Endgerät gespeicherten Daten zugegriffen und Standort- und Sensordaten übermittelt, wobei dies oftmals nicht auf der Grundlage einer bewussten Entscheidung der Nutzerinnen und Nutzer stattfindet. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hatte etwa zum wiederholten Male im Rahmen einer internationalen Prüfung von Apps erhebliche Mängel bei der Information über den Umgang mit Daten festgestellt (Bayerisches Landesamtes für Datenschutzaufsicht 2015). Eine Untersuchung der Stiftung Warentest kam zuvor bereits zu dem Ergebnis, dass persönliche Informationen ungesichert und nicht anonymisiert an Datensammler weitergegeben werden. Davon betroffen sind

[1] Mit Dank an Herrn Prof. Dr. Ulrich Gassner und Herrn Julian Modi, LL.M., Forschungsstellen für Medizinprodukterecht (FMPR) und E-Health-Recht (FEHR), Universität Augsburg, für die Diskussion.

sowohl Benutzernamen und Passwörter als auch Adressverzeichnisse der Nutzerinnen und Nutzer bzw. Inhalte entsprechender Adressbücher (Die Welt 2015). Im Kontext von Gesundheits-Apps erscheinen entsprechende Lücken umso problematischer. Schließlich können hier sensible gesundheitsbezogene Daten betroffenen sein, die als besonders schutzbedürftig zu betrachten sind und insoweit auch nur unter strengen Voraussetzungen erhoben, verarbeitet oder genutzt werden dürfen.

Das Risiko ist zunächst der Missbrauch der Daten. (Gesundheits-)Daten könnten ohne Wissen der Nutzerinnen und Nutzer ausgewertet, mit anderen Daten zusammengeführt oder an Dritte weitergegeben bzw. verkauft oder in sozialen Netzwerken veröffentlicht werden. Vor diesem Hintergrund sind die Vorgaben zu Datenschutz und Datensicherheit für die Hersteller bzw. Anbieter von Gesundheits-Apps in Deutschland zu betrachten.

Weil Apps auch für Kinder und Jugendliche leicht zugänglich sind, sind nach Maßgabe der erhöhten Schutzbedürftigkeit von Minderjährigen Besonderheiten hinsichtlich der wirksamen Einwilligungserteilung zur Verarbeitung ihrer Daten zu berücksichtigen. Ein weiteres datenschutzrechtliches Problem ergibt sich daraus, dass Angebot und Nutzung von Apps häufig im internationalen Kontext zu betrachten sind. Es stellt sich hier die Frage, was bei einer Verarbeitung oder Speicherung der über entsprechende Apps erfassten Daten bei grenzüberschreitenden Sachverhalten, sowohl innerhalb als auch außerhalb der Europäischen Union speziell zu beachten ist.

# 4 Datenschutzrechtliche Aspekte im Zusammenhang mit Gesundheits-Apps

## 4.1 Schutzgut und Entwicklung des Datenschutzrechts

**Schutzgut und Entwicklung des Datenschutzrechts**

Der Datenschutz zielt darauf ab, den Einzelnen vor Beeinträchtigungen seiner Persönlichkeitsrechte durch den Umgang mit seinen personenbezogenen Daten zu schützen.[2] Das Recht des Datenschutzes bezweckt damit Persönlichkeitsschutz und insoweit auch Schutz der Privatsphäre[3].

Die verfassungsrechtliche Verankerung findet sich dem entsprechend in dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i. V. m. Art 1 Abs. 1 des Grundgesetzes[4] (GG) bzw. dem hieraus nach dem Urteil des Bundesverfassungsgerichts (BVerfG) zum Volkszählungsgesetz (sog. Volkszählungsurteil[5]) abgeleiteten Recht auf informationelle Selbstbestimmung. Das Gericht kam in diesem Sinne ausdrücklich zur Schlussfolgerung, dass die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraussetzt. Dies beinhaltet das Recht des Einzelnen, selbst darüber zu bestimmen, ob und welche persönlichen Daten er preisgibt und inwieweit diese verarbeitet werden dürfen. Eine Datenverarbeitung durch staatliche aber auch private Stellen soll unter Berücksichtigung dessen nur auf gesetzlicher Grundlage möglich sein.

Das Datenschutzrecht in seiner Ausprägung des grundrechtlich gewährleisteten Schutzes des Rechts auf informationelle Selbstbestimmung ist auf nationaler Ebene in den allgemeinen Datenschutzgesetzen des Bundes und der Länder, ferner in einer Vielzahl bereichsspezifischer Datenschutzbestimmungen geregelt.[6] Insofern liegt eine entsprechende fortschreitende Entwicklung der Datenschutzgesetzgebung vor(Gola, Klug und Körffer 2015, Rn. 1-29). Soweit diese bereichsspezifischen Regelungen Anwendung finden, verdrängen sie die allgemeinen Datenschutzgesetze.

---

[2] Siehe § 1 Abs. 1 des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162) geändert worden ist (BDSG).

[3] Vgl. EuGH – Digital Rights Ireland Ltd, Rs. C-293/12 – Slg 2014, Rn 32 ff; EuGH – Michael Schwarz, C-291/12 – Slg 2013, Rn. 26 ff.

[4] Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 23. Dezember 2014 (BGBl. I S. 2438) geändert worden ist.

[5] BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1-71.

[6] Siehe hierzu unten 4.2

Auf EU-Ebene geht die Regulierung des Datenschutzes zur Harmonisierung nationaler Datenschutzgesetze sowie als Reaktion auf den zunehmenden grenzüberschreitenden Datenfluss auf die sog. EG-Datenschutzrichtlinie[7] sowie speziell für den Fernmeldebereich auf die Richtlinie 97/66/EG[8] zurück. Ferner ist der Schutz der Privatsphäre und der Schutz personenbezogener Daten in den Artikeln 7 und 8 der Charta der Grundrechte der EU mit dem Vertrag von Lissabon rechtsverbindlich verankert worden.[9]

Bereits im Jahr 2012 wurden seitens der EU-Kommission zur Reformierung des europäischen Datenschutzrechts Entwürfe für eine Datenschutz-Grundverordnung (im Folgenden „DSGVO") (Europäische Kommission 2012, S. 11; Hornung 2012; Schneider und Härting 2012) sowie für eine Richtlinie zur Datenverarbeitung im Bereich der Strafverfolgung und Gefahrenabwehr (Europäische Kommission 2012, S. 10) vorgestellt. Die DSGVO soll die EG-Datenschutzrichtlinie von 1995 vollständig ersetzen. Eine Verabschiedung der DS-GV steht nunmehr für Anfang 2016 an, nachdem sich Ende 2015 das Europäische Parlament und der Rat im sog. „Trilog" hierüber geeinigt haben. (Europäische Kommission (2015). Damit sind die neuen Vorschriften zum Datenschutz gemäß Art. 91 Ziff. 2 DGSVO nach einer Umsetzungsfrist von zwei Jahren anwendbar. Inhalt ist namentlich als Beispiel auch hier der Grundsatz der informierten Einwilligung des Betroffenen. Schweigen oder fehlende Reaktionen sind keine Einwilligung. Weiter sind entsprechende Informationsrechte geregelt sowie mögliche Haftung und Sanktionen bei Rechtsverstößen. Kinder sollen besonders geschützt werden. Aufgrund der Tatsache, dass die Regelungen noch nicht final rechtlich bindend sind, wird zu klären sein, inwieweit und in welcher Ausprägung auch das deutsche Datenschutzrecht angepasst und reformiert werden muss. Hierbei wird insbesondere auch der Bereich von Apps aufgrund der weiten Verbreitung und dem sehr einfachen Zugriff für den Betroffenen weiter zu diskutieren sein.

## 4.2 Rechtsgrundlagen des Datenschutzrechts im Einzelnen und Voraussetzungen für die Datenerhebung, -verarbeitung und -nutzung

### 4.2.1 Bundesdatenschutzgesetz (BDSG)

**Bundesdatenschutzgesetz (BDSG)**

Das BDSG vermag nicht den Datenschutz unter Berücksichtigung aller etwaigen mit der Verwendung personenbezogener Daten verbundenen Gefahren abschließend zu kodifizieren. Ihm kommt vielmehr als Teil eines von bereichsspezifischen Vorschriften bestimmten Gesamtregelwerks eine „Auffangfunktion" zu (Simitis 2014, Rn. 23.) Es findet gemäß § 1 Abs. 3 BDSG hinsichtlich der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur Anwendung, soweit kein spezielleres Gesetz vorliegt – zu nennen sei etwa das Zehnte Buch Sozialgesetzbuch (SGB X)[10] für den Bereich der Sozialversicherung. Hiervon umfasst ist mithin auch die Regelung der Datenerhebung, -verarbeitung und -nutzung im Kontext der gesetzlichen Krankenversicherung.

Von dem in § 1 Abs. 1 BDSG festgehaltenen Regelungsziel, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, sind über § 3 Abs. 9 BDSG die besonderen Arten personenbezogener Daten erfasst. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse

---

7 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31.

8 Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation ABl. L 0 24 vom 30.01.1998, S. 1. Sie wurde als sog. als sog. EG-Telekommunikations-Datenschutzrichtlinie 2002/58/EG (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. L 201 vom 31.7.2002, S. 37), novelliert und nochmals überarbeitet durch die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der RL 2002/58/EG (ABl. 2006 L 105/54).

9 Die EU-Charta ist seit dem 1.12. 2009 mit Inkrafttreten des Vertrags von Lissabon für fast alle europäischen Staaten (Ausnahme England und Polen) rechtsverbindlich geworden.

10 Das Zehnte Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), das durch Artikel 32 des Gesetzes vom 20. November 2015 (BGBl. I S. 2010) geändert worden ist.

einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Besondere Arten von personenbezogenen Daten sind insofern Daten, die als besonders sensibel gelten, weil sie etwa Angaben über die Gesundheit, politische Überzeugungen, rassische oder ethnische Herkunft, religiöse oder philosophische Überzeugung oder das Sexualleben enthalten (§ 3 Abs. 9 BDSG). Die Erhebung, Verarbeitung oder Nutzung besonderer personenbezogener Daten ist nur unter erhöhten Anforderungen gestattet (§§ 13 Abs. 2, 14 Abs. 5 und 6, 28 Abs. 6–9, 29 Abs. 5 BDSG). Unter Gesundheitsdaten werden zum Teil nur Informationen über Krankheiten, Beschwerden oder Störungen oder aus diesem Anlass erfolgte Behandlungen, Untersuchungen und auch Beratungen, einschl. des Ablaufs und Ergebnisses, verstanden, aber auch Umstände, die auf ein physisches oder psychisches Leiden oder dessen Fehlen schließen lassen (Rehmann und Heimhalt 2014, S. 253).

Die Regeln des Datenschutzes beruhen auf einer Abwägung von öffentlichen und privaten Interessen.[11] Das BDSG basiert dabei u.a. auf folgenden wichtigen Grundsätzen:

- Grundsatz der Datenvermeidung und Datensparsamkeit
- Grundsatz der Direkterhebung beim Betroffenen
- Grundsätzliches Datenverarbeitungsverbot.

Nach dem sog. Territorialprinzip fällt in den Anwendungsbereich des BDSG jede verantwortliche Stelle, die personenbezogene Daten in Deutschland erhebt, verarbeitet oder nutzt. Für Telemedien- bzw. Telekommunikationsdienste enthalten die §§ 11 ff. Telemediengesetz (TMG)[12] sowie §§ 91 ff. Telekommunikationsgesetz (TKG)[13] spezielle Datenschutzregeln.[14] Nach § 1 Abs. 3 BDSG gehen diese dem BDSG vor. § 1 Abs. 3 BDSG bestimmt, dass, soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, diese den Vorschriften dieses Gesetzes vorgehen. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnis, die nicht auf gesetzlichen Vorschriften beruhen, bleiben unberührt.

### 4.2.1.1 Begriffe

**Betroffene**

Nach § 3 Abs. 1 BDSG ist die Nutzerin oder der Nutzer einer App der „Betroffene“ im Sinne des Gesetzes. Diese betroffene Person gilt es zu schützen. Verantwortlich ist derjenige, der die datenschutzrelevante Stelle betreibt. § 3 Abs. 7 BDSG definiert die verantwortliche Stelle als „die Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“. Die EG-Datenschutzrichtlinie[15] sieht in Art. 2 eine ähnliche Definition vor.

**Entwickler**

Zu differenzieren sind ferner die Begriffe des „Entwicklers“ und des „Anbieters“. Die Begriffe sind nicht zwingend parallel mit der Begriffsdefinition des Herstellers und Inverkehrbringers im Sinne des MPG zu sehen, sondern datenschutzrechtlich zu fassen. Je nach Rechtsgebiet ist eine separate Betrachtung und Bewertung erforderlich. Sofern der Entwickler mit dem Anbieter identisch ist, ist diese Person verantwortlich. Wenn jedoch der Entwickler die technische Entwicklung der App vornimmt und der Anbieter dieses bei ihm in Auftrag gegeben hat, ist der Anbieter die verantwortliche Stelle im Sinne von § 3 Abs. 7 BDSG. (Baumgartner 2013, Rn. 462)

**Personenbezogene Daten**

Wesentlich ist weiter der Begriff der personenbezogenen Daten. Dies sind, wie vorstehend bereits ausgeführt[16], nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Die Rechtsprechung nimmt hier eine weite Auslegung vor (Baumgartner 2013, Rn. 212).

**EU-Datenschutzrichtlinie**

Die EU-Datenschutzrichtlinie definiert in Art. 2 a personenbezogene Daten als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person‘); als bestimmbar

[11] BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83 –, BVerfGE 65, 1-71.

[12] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 4 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist.

[13] Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 5 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist.

[14] Die Anwendbarkeit sonstiger Datenschutzbestimmungen des TMG oder TKG folgt den Regeln über die Anwendbarkeit des BDSG; vgl. Stadler, ZD 2011, 57, 58.

[15] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046&from=de [Zugriff 03. Jan. 2016].

[16] Siehe oben 4.2.1

wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die "Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind; In der Literatur wird das Beispiel einer Kreditkarte genannt, wonach zur Identifizierung entsprechendes Zusatzwissen neben der Kreditkartennummer erforderlich ist (Baumgartner 2013, Rn. 214).

Wichtig sind ferner die Begriffe der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten, geregelt in § 3 BDSG.

„(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
   a) die Daten an den Dritten weitergegeben werden oder
   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt."

### 4.2.1.2 Zulässigkeit der Datenerhebung, -nutzung und -verarbeitung

Ausgehend von dem Grundsatz, dass das Recht des Einzelnen auf informationelle Selbstbestimmung zu schützen ist, stellt sich die Frage der Zulässigkeit der Datenerhebung, -nutzung und -verarbeitung. Es gilt das Grundprinzip des Verbots mit Erlaubnisvorbehalt nach § 4 Abs. 1 BSDG. Jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist hiernach grundsätzlich verboten, außer es greift eine gesetzliche Erlaubnis oder der Betroffene hat wirksam eingewilligt. (Baumgartner 2013, Rn. 225). Für die Möglichkeit der Datenerhebung und -verarbeitung ist also ein Legitimationstatbestand erforderlich.

### 4.2.1.3 Einwilligung

**Einwilligung**

Für die Einwilligung der Nutzerin oder des Nutzers ist § 4a BDSG sowie für Telemediendienste § 13 Abs. 1 TMG heranzuziehen. Die Einwilligung muss freiwillig, also ohne Druck gegeben werden. Sie muss ausdrücklich und aktiv erfolgen (Baumgartner 2013, Rn. 236). Ohne Einwilligung der Nutzerin oder des Nutzers ist eine Erhebung, Verarbeitung oder Nutzung der Gesundheitsdaten nicht zulässig (Rehmann und Heimhalt 2014, S. 253). Wenn beispielsweise Gesundheits-Apps über den Verkauf von Nutzungsdaten mit Personenbezug ohne entsprechende Legitimation finanziert werden, wäre dies nicht zulässig. Eine umfangreiche Aufklärung und Einwilligung wäre im Detail erforderlich.

§ 4 a BDSG nennt die Voraussetzungen der Einwilligung: Die Einwilligung ist hiernach nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Dies gilt auch für die Nutzung von Apps. Nach § 13 TMG ist, soweit das Gesetz einschlägig ist, im elektronischen Rechtsverkehr eine elektronische Form ausreichend. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben, § 4 a Abs. 1 BDSG. Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen, § 4 a Abs. 3 BDSG. Jede Art der Verwendung muss im Vorfeld

von der Aufklärung und der Einwilligung umfasst sein. Der Zweck muss hinreichend bestimmt sein, Veränderungen im Nachgang sind insofern ohne Zustimmung nicht möglich.

Arbeitgeber dürfen hiernach nicht ohne Weiteres Daten Ihrer Angestellten verwenden, wenn diese über eine App erhoben werden. Ggf. wäre hier an eine individualvertragliche Abrede zu denken, wonach dann eine ausdrückliche Zustimmung des Arbeitnehmers gegeben wäre. Wegen des Abhängigkeitsverhältnisses ist hier jedoch der Einzelfall sehr sorgfältig zu überprüfen.

Technisch muss die Umgebung so hergestellt sein, dass der Datenschutz gewährleistet sein kann. Für die Arztpraxis hat die Bundesärztekammer einer Handreichung herausgegeben, die Empfehlungen zur ärztlichen Schweigepflicht und dem Datenschutz und der Datenverarbeitung in der Arztpraxis enthält; enthalten ist ebenfalls eine technische Anlage (Bundesärztekammer 2015). § 9 BDSG regelt die technischen und organisatorischen Maßnahmen. Hiernach haben öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG, insbesondere die in der Anlage zum BDSG genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Folgende Voraussetzungen sind nach der Anlage zum BDSG einzuhalten:

„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.

Wenn Softwareapplikationen so gestaltet sind, dass die Datenverarbeitung durch Dritte erfolgt, also eine Auftragsdatenverarbeitung vorliegt, sind die Anforderungen des § 11 BDSG einzuhalten. Hiernach muss der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind: 1. der Gegenstand und die Dauer des Auftrags, 2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen, 3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen, 4. die Berichtigung, Löschung und Sperrung von Daten, 5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen, 6. die

etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen, 7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers, 8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen, 9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält, 10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.[17]

#### 4.2.1.4 Gesetzliche Erlaubnistatbestände

**Gesetzliche Erlaubnistatbestände**

Unter bestimmten Voraussetzungen kann die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu bestimmten Zwecken gesetzlich gestattet sein. Insbesondere können die besonders Praxis relevanten gesetzlichen Erlaubnistatbestände des § 28 Abs. 1 BDSG eingreifen.

Zum einen kann hiernach die Erhebung, Verarbeitung und Nutzung von Daten für die Begründung, Durchführung und Beendigung eines Vertrages zwischen der verantwortlichen Stelle und den Betroffenen erforderlich und damit zulässig sein (Baumgartner 2013, Rn. 245). Zum anderen kann dies zulässig sein, wenn schutzwürdige Interessen an dem Ausschluss der Verarbeitung oder Nutzung hinter den berechtigten Interessen der verantwortlichen Stelle offensichtlich zurückzustehen haben. Hier ist eine Interessenabwägung vorzunehmen (Baumgartner 2013, Rn. 247).

**Einwilligung**

Ohne Einwilligung wäre die Datenerhebung und -verarbeitung von besonderen Daten im o.g. Sinne nur unter den Voraussetzungen des § 28 Abs. 6 BDSG zulässig. Diese sind gegeben, wenn „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 (Nr. 1), es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat (Nr. 2), 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 (Nr. 3), oder 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 (Nr. 4).

### 4.2.2 Telemediengesetz (TMG)

**Telemediengesetz (TMG)**

Das TMG gilt nach § 1 Abs. 1 TMG für alle elektronischen Informations- und Kommunikationsdienste. Damit zählen ggf. auch Apps hierzu.[18]

Im TMG existieren ebenfalls gesetzliche Erlaubnistatbestände für die Datenerhebung, -verarbeitung und -nutzung. Hier wird zwischen insbesondere zwischen Bestandsdaten und Nutzungsdaten nach § 14 bzw. § 15 TMG unterschieden. Der Umfang der Bestandsdaten hängt ab von der Gestaltung des Telemediendienstes (Kamps 2011, Rn. 186). Zu nennen sind hier beispielsweise: Name und Anschrift, E-Mail-Adresse, Zugangsdaten, Zahlungsangaben bei kostenpflichtigen Angeboten (Konto- und Kreditkartennummer und deren Gültigkeitsdauer) und sonstige von der Nutzerin oder vom Nutzer gemachte Angaben. Hinsichtlich des Umfangs der Bestandsdaten gestattet § 14 Abs. 1 TMG nur die Erhebung, Verarbeitung und Nutzung der Daten, die für den genannten Zweck erforderlich bzw. unerlässlich sind. Hinsichtlich der Erforderlichkeit ist auf das konkrete Vertragsverhältnis zwischen Anbieter und Nutzerin oder Nutzer und auf die Eigenschaften und Merkmale des angebotenen Dienstes abzustellen (Kamps 2011, Rn. 187).

[17] So der Wortlaut der Vorschrift, die im Einzelfall zu prüfen ist.

[18] Der BGH hat mit aktuellen Urteilen vom 26. November 2015 - I ZR 3/14 und I ZR 174/14 entschieden, dass auch ein Telekommunikationsunternehmen für die Bereitstellung von Internetseiten in Anspruch genommen werden kann. In der Pressemitteilung ist hierzu wie folgt ausgeführt: „Ein Telekommunikationsunternehmen, das Dritten den Zugang zum Internet bereitstellt, kann von einem Rechteinhaber grundsätzlich als Störer darauf in Anspruch genommen werden, den Zugang zu Internetseiten zu unterbinden, auf denen urheberrechtlich geschützte Werke rechtswidrig öffentlich zugänglich gemacht werden.“, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2015&Sort=3&nr=72928&pos=1&anz=196

Im Unterschied dazu beziehen sich Nutzungsdaten auf alle Aspekte der Nutzung eines Dienstes. (Kamps 2011, Rn. 191). Nutzungsdaten sind dabei alle Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen, § 15 Abs. 1 TMG. Dabei ist die Aufzählung in § 15 TMG nicht als abschließend zu betrachten. Das TGM umfasst dabei jedoch nicht die Verkehrsdaten gem. § 96 TKG, also diejenigen Daten, die sich aus der Nutzung von Telekommunikationsdienstleistungen ergeben; diese sind ausschl. nach telekommunikationsrechtlichen Gesichtspunkten zu beurteilen (Kamps 2011, Rn. 192).

Der Umfang der Erhebung von Nutzungs- und Bestandsdaten ist auf das erforderliche Maß zu beschränken und dass Nutzungsdaten zu löschen sind, wenn sie für die Inanspruchnahme des Dienstes nicht mehr nötig sind und die weitere Speicherung und Nutzung nicht durch andere Bestimmungen erlaubt ist (Kamps 2011, Rn. 194).

## 4.3 Spezieller Schutz von Gesundheitsdaten und Voraussetzungen für die Datenerhebung und -verarbeitung

### 4.3.1 Gesundheitsdaten im Allgemeinen

**Gesundheitsdaten allgemein**

Gesundheitsdaten nach § 3 Abs. 9 BDSG[19] und § 67 ff. SGB X[20] geschützt. Auch hier ist die besondere Sensibilität der Daten genannt. Für den Bereich der privaten Krankenversicherung ist das SGB X nicht einschlägig. § 1 SGB X bestimmt den Anwendungsbereich wie folgt: "Die Vorschriften dieses Kapitels gelten für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden, die nach diesem Gesetzbuch ausgeübt wird." Die Zulässigkeit der Datenverwendung richtet sich also nach dem BDSG.

§ 3 Abs. 9 BDSG definiert die besonders geschützten Daten wie folgt: „Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit“ oder Sexualleben. Hierunter fallen also auch Gesundheitsdaten, die durch mobile Endgeräte und Apps erhoben werden können.

Hinzu kommt, dass im Geheimnisträger im Sinne des § 203 Strafgesetzbuch (StGB), wie beispielsweise Ärztinnen und Ärzte, zusätzlich der strafrechtlich sanktionierten und zivilrechtlich gebotenen Pflicht zur Gemeinhaltung von Privatgeheimnissen unterfallen, wozu namentlich die Angaben zur Gesundheit gehören. Geschützt werden soll das Vertrauensverhältnis Arzt-Patient und das Selbstbestimmungsrecht des Patienten, also das Geheimhaltungsinteresse des Patienten. (Spickhoff 2014, Rn. 1 m. w. N.). Informationen über die Gesundheit dürfen nicht den „Kreis der Wissenden“ verlassen, soweit diese in der Eigenschaft als speziell genannte Person (z. B. Ärztin oder Arzt) erfahren wurde, § 203 StGB (Spickhoff 2014, Rn. 26 m. w. N.) Letztlich war schon im Eid des Hippokrates die ärztliche Schweigepflicht niedergelegt und ist heutzutage — landesrechtlich vermittelt — berufsrechtliche Pflicht.[21] Weitere Grundlage des Datenschutzes ist auch der Behandlungsvertrag der Ärztin oder des Arztes mit den eigenen Patientinnen und Patienten, wo die Schweigepflicht als wesentliche Nebenpflicht anerkannt ist (Katzenmeier 2015, Rn. 6 m. W. N.)

### 4.3.2 Gesundheitsdaten im SGB X

**Gesundheitsdaten im SGB X**

Die Datenerhebung in der GKV verfolgt im Wesentlichen die Zwecke der „Bewilligung und Abrechnung von Leistungen, die Prüfung der Leistungserbringer und die Weiterentwicklung der Versorgung sowie der Abrechnungssysteme“ (Michels 2014, Rn. 1). Hierbei ist das in § 35 SGB X verankerte Sozialgeheimnis zu beachten. Danach hat jeder Anspruch darauf, dass die ihn betreffenden Sozialdaten nach § 67 Abs. 1 SGB X von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden. Maßgeblich ist also im Wesentlichen das zweite Kapitel

[19] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162) geändert worden ist.

[20] Das Zehnte Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), das zuletzt durch Artikel 10 des Gesetzes vom 11. August2014 (BGBl. I S. 1348) geändert worden ist.

[21] (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997 – in der Fassung des Beschlusses des 118. Deutschen Ärztetages 2015 in Frankfurt am Main, Dt. ÄBl. doi:10.3238/arztebl.2015.mbo_daet2015.

des SGB X, Schutz der Sozialdaten.[22] Im Bereich der GKV ist im 10. Kapitel des SGB V ein bereichsspezifisches Datenschutzrecht für die GKV enthalten.

Gemäß § 67 Abs. 1 SGB X sind Sozialdaten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, die vom Gesetz Betroffener genannt wird, die von einer in § 35 SGB I im Hinblick auf ihre Aufgaben nach diesem Gesetz erhoben, verarbeitet oder genutzt werden. Hierbei handelt es sich um die Leistungsträger in der gesetzlichen Krankenversicherung, damit auch die gesetzlichen Krankenkassen.

Die Aufgaben, zu deren Erfüllung eine Datenerhebung- und Verarbeitung möglich ist, sind in § 70 Abs. 2 SGB X geregelt. Aufgaben nach diesem Gesetzbuch sind, soweit das Kapitel angewendet wird, auch Aufgaben aufgrund von Verordnungen, deren Ermächtigungsgrundlage sich im Sozialgesetzbuch befindet, Aufgaben aufgrund von über- und zwischenstaatlichem Recht im Bereich der sozialen Sicherheit, Aufgaben aufgrund von Rechtsvorschriften, die das 1. und 10. Buch des Sozialgesetzbuches für entsprechend anwendbar erklären und Aufgaben aufgrund des Arbeitssicherheitsgesetzes und Aufgaben, soweit sie in den § 5 SGB I genannten Stellen durch Gesetz zugewiesen sind. Die Aufgaben der gesetzlichen Krankenversicherung sind beispielsweise in § 1 SGB V definiert. Hiernach hat die Krankenversicherung als Solidargemeinschaft die Aufgabe, die Gesundheit der Versicherten zu erhalten, wiederherzustellen oder ihren Gesundheitszustand zu bessern.

Automatisiert im Sinne des Sozialdatenschutzes ist die Erhebung, Verarbeitung oder Nutzung von Sozialdaten, wenn sie unter Einsatz von Datenverarbeitungsanlagen durchgeführt wird (automatisierte Verarbeitung), § 67 Abs. 3 SGB X. Eine nicht-automatisierte Datei ist jede nicht automatisierte Sammlung von Sozialdaten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

Erheben ist das Beschaffen von Daten über den Betroffenen, Abs. 5. Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen von Sozialdaten. Nutzung ist jede Verwendung von Sozialdaten, soweit es sich nicht um Verarbeitung handelt, auch die Weitergabe der verantwortlichen Stelle. Anonymisieren ist das Verändern von Sozialdaten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Weiter definiert ist der Begriff des Pseudonymisierens der verantwortlichen Stelle, des Empfängers, der nicht-öffentlichen Stelle und einer besonderen Art der personenbezogenen Daten. Diese sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

Nach § 67 a SGB X ist die Datenerhebung nur zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetz erforderlich ist. Dies gilt auch für besondere Arten personenbezogener Daten, wie eben ausgeführt. Angaben über die rassische Herkunft dürfen ohne Einwilligung nicht erhoben werden. Des Weiteren muss sich die Einwilligung ausdrücklich hierauf beziehen.

Im Hinblick auf die Anwendung von medizinischer Software-Applikationen ist daher im Ergebnis im Einzelfall zu prüfen, ob die Daten, die mit der entsprechenden Software-Applikationen erhoben werden, vom Anwendungsfeld der Vorschriften über das Sozialgeheimnis umfasst sind:

[22] Geregelt werden hier die nachfolgenden Punkte: § 67 Begriffsbestimmungen, § 67a Datenerhebung, § 67b Zulässigkeit der Datenverarbeitung und -nutzung, § 67c Datenspeicherung, -veränderung und -nutzung, § 67d Übermittlungsgrundsätze, § 67e Erhebung und Übermittlung zur Bekämpfung von Leistungsmissbrauch und illegaler Ausländerbeschäftigung, § 68 Übermittlung für Aufgaben der Polizeibehörden, der Staatsanwaltschaften, Gerichte und der Behörden der Gefahrenabwehr, § 69 Übermittlung für die Erfüllung sozialer Aufgaben, § 70 Übermittlung für die Durchführung des Arbeitsschutzes, § 71 Übermittlung für die Erfüllung besonderer gesetzlicher Pflichten und Mitteilungsbefugnisse, § 72 Übermittlung für den Schutz der inneren und äußeren Sicherheit, § 73 Übermittlung für die Durchführung eines Strafverfahrens, § 74 Übermittlung bei Verletzung der Unterhaltspflicht und beim Versorgungsausgleich, § 74a Übermittlung zur Durchsetzung öffentlich-rechtlicher Ansprüche und im Vollstreckungsverfahren, § 75 Übermittlung von Sozialdaten für die Forschung und Planung, § 76 Einschränkung der Übermittlungsbefugnis bei besonders schutzwürdigen Sozialdaten, § 77 Übermittlung ins Ausland und an über- oder zwischenstaatliche Stellen, § 78 Zweckbindung und Geheimhaltungspflicht eines Dritten, an den Daten übermittelt werden, § 78a Technische und organisatorische Maßnahmen, § 78b Datenvermeidung und Datensparsamkeit, § 78c Datenschutzaudit, § 79 Einrichtung automatisierter Abrufverfahren, § 80 Erhebung, Verarbeitung oder Nutzung von Sozialdaten im Auftrag, § 81 Rechte des Einzelnen, Datenschutzbeauftragte, § 82 Schadensersatz, § 83 Auskunft an den Betroffenen, § 83a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Sozialdaten, § 84 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht, § 84a Unabdingbare Rechte des Betroffenen, § 85 Bußgeldvorschriften, § 85a Strafvorschriften.

Je nachdem welche Daten über die Software-Applikationen erhoben werden, sind die jeweiligen Spezialvorschriften im Regelungswerk der Vorschriften des Sozialdatenschutzes zu beachten. Eine pauschale Bewertung sämtlicher Möglichkeiten von Datenerhebungen und-verarbeitungen ist nicht möglich.

Ohne Rechtsgrundlage ist aber eine Datenerhebung- und -verarbeitung durch die gesetzlichen Krankenkassen nicht möglich.

## 4.4 Beteiligung speziell geschützter Gruppen

### 4.4.1 Minderjährige

**Gesundheits-Apps und Minderjährige**

Beim Einsatz von Gesundheits-Apps bei Minderjährigen ist im Hinblick auf den Datenschutz zu beachten, dass die Einwilligung zur Datenerhebung- und Verarbeitung erforderlich ist. Dies ist im Einzelfall durchaus kritisch. So ist teilweise zu finden, dass die Einwilligung von den Sorgeberechtigten einzuholen ist, wie ein App-Anbieter in der Praxis die Einwilligung der Eltern erhält, wenn sich die Minderjährigen die App eigenständig herunterladen, wird dort kritisch gesehen (Baumgartner 2013, Rn. 326). Diese Auffassung setzt jedoch voraus, dass die datenschutzrechtliche Einwilligung eine rechtsgeschäftliche Erklärung ist oder Teil eines Vertrages, wie beim Kauf einer Lizenz. Regelmäßig wird von der Einsichtsfähigkeit des Minderjährigen in die Tragweite der Entscheidung ausgegangen, wenn die datenschutzrechtliche Komponente betroffen ist.[23] Es kommt darauf an, ob die datenschutzrechtliche Einwilligung Teil eines Vertrages ist, der die volle Geschäftsfähigkeit erfordert. Nur wenn ausschließlich das Persönlichkeitsrecht betroffen ist, eröffnet sich die Frage, ob die Einsichtsfähigkeit genügt (Buchner 2006, S. 247). In jeden Fall ist jedoch das tatsächliche Problem aufgeworfen, dass durchaus Minderjährige ohne Zustimmung der Sorgeberechtigten und ggf. auch ohne entsprechende Einsichtsfähigkeit datenschutzrechtliche Einwilligungen abgeben werden.

Minderjährige sind auch außerhalb des Datenschutzrechts besonders geschützt, was namentlich auch Auswirkungen auf Apps hat, insbesondere, was die Inhalte betrifft. Jugendschutz hat Verfassungsrang und wird aus dem allgemeinen Persönlichkeitsrecht in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG hergeleitet (Baumgartner 2013, Rn. 408). Im Bereich des Jungendschutzes finden sich unterschiedliche gesetzliche Regelungen. Eine grundsätzliche Regelung findet sich im Jugendmedienschutz-Staatsvertrag der Länder (JMStV), welcher auch auf Telemedien und Rundfunk Anwendung findet, § 2 Abs. 1 JMStV. Die Regelungen des TMG bleiben hierbei unberührt und auch das Jugendschutzgesetz (JuSchG) findet Anwendung (Nordmann 2011, Rn. 148). Nichtsdestotrotz gilt für schwere Fälle und unabhängig vom gewählten Medium der geregelte Jugendschutz des StGB (Nordmann 2011, Rn. 149). Hier werden Kinder und Jugendliche ebenfalls besonders geschützt, beispielsweise, dürfen ihnen keine nicht für sie erlaubten Filme und Schriften zugänglich gemacht werden.

Hinsichtlich der Eigenart der Apps ist auch hier nicht eindeutig, welches Gesetz Anwendung findet. Das Jugendschutzgesetz findet Anwendung nur im Bereich der Trägermedien (Baumgartner 2013, Rn. 409). § 1 Abs. 2 JuSchG definiert Trägermedien als Medien mit Texten, Bildern oder Tönen auf gegenständlichen Trägern, die zur Weitergabe geeignet, zur unmittelbaren Wahrnehmung bestimmt oder in einem Vorführ- oder Spielgerät eingebaut sind. Der Jugendmedienstaatsvertrag gilt gem. § 2 Abs. 1 JMStV insbesondere für Rundfunk und Telemedien. Die Abgrenzung zwischen Jugendschutzgesetz und Jugendmedienstaatsvertrag erfolgt nach Online- (dann Jugendmedienstaatsvertrag) und Offlinebereich (dann Jugendschutzgesetz); wobei bei Unsicherheiten im Zweifel der Jugendmedienstaatsvertrag Anwendung findet (Baumgartner 2013, Rn. 410). Wenn Apps genutzt werden wird dies bedeuten, dass beim Streaming der Jugendmedienstaatsvertrag gilt.

Verantwortlicher nach dem Jugendmediendienststaatsvertrag ist hierbei grundsätzlich der App-Anbieter (Baumgartner 2013, Rn. 417), der wiederum nicht zwingend Hersteller im medizinprodukterechtlichen Sinne sein muss, wenn dieses Anwendung findet. Die zentrale Kontrollinstanz ist die Kommission für Jugendmedienschutz der Landesmedienanstalten (KJM).[24] Verstöße gegen

[23] So hat der Bundesgerichtshof entschieden, dass eine gesetzliche Krankenkasse gegen das Verbot verstößt, die geschäftliche Unerfahrenheit von Jugendlichen auszunutzen, wenn sie im Zusammenhang mit der Durchführung eines Gewinnspiels von den Teilnehmern im Alter zwischen 15 und 17 Jahren umfangreiche personenbezogene Daten erhebt, BGH NJW 2014, 2282-2285.

[24] http://www.kjm-online.de/die-kjm.html [Zugriff 09. Nov. 2015].

den Jugendmedienstaatsvertrag werden gem. § 24 JMStV als Ordnungswidrigkeiten verfolgt, wobei § 23 JMStV einen Straftatbestand enthält, wenn Angebote verbreitet oder zugänglich gemacht werden, die offensichtlich geeignet sind, die Entwicklung von Kindern und Jugendlichen schwer zu gefährden.

Hinsichtlich der Anwendbarkeit des Jugendschutzrechts auf Apps, die nicht aus Deutschland kommen, ist anzumerken, dass das deutsche Jugendschutzrecht auch für ausländische Anbieter Geltung entfaltet, wenn das entsprechende Angebot in Deutschland abrufbar ist, egal, ob der entsprechende Anbieter seinen Sitz in der EU oder einem Drittstaat hat (Koreng 2013, Rn. 176).

Unabhängig davon, wo der Anbieter der App seinen Sitz hat, unterliegt er den Anforderungen deutschen Jugendschutzrechts, sofern die App in Deutschland erhältlich ist, jedoch ist es unwahrscheinlich, dass die entsprechende Behörde ordnungsrechtliche Maßnahmen auch gegenüber einem im Ausland sitzenden Anbieter ergreifen oder durchsetzen können wird (Koreng 2013, Rn. 118).

Problematisch gestaltet sich dabei die Umsetzung der Jugendschutzmaßnahmen. App-Anbieter und App Stores sollten zusammen arbeiten, da nur so ein wirksamer Jugendschutz gewährleistet werden kann (Baumgartner 2013, Rn. 433). Aktuell wird folgendes Procedere durchgeführt. Die gängigen App-Stores verlangen, dass die Anbieter der App die App vor Veröffentlichung klassifizieren und dieses auch an die Endnutzer weiter geben. Dafür muss der Anbieter der App die Inhalte nach einem vorgegebenen System dem Inhalt nach beschreiben und damit einer vorgegebenen Alterskategorie zuwiesen. Dem Kunden wird dann die Möglichkeit gegeben, den Zugang zum App Store so einzurichten, dass nur Apps für bestimmte Stufen des entsprechenden Alters-Klassifizierungssystems zugänglich sind. Inwieweit die App-Store-Betreiber prüfen, ob ihre Vorgaben eingehalten werden, ergibt sich nicht aus den entsprechenden Verträgen bzw. Richtlinien.

Bisher ist hier nicht geklärt, inwieweit diese haften. Es gestaltet sich vielmehr so, dass in den entsprechenden Entwicklervereinbarungen Klauseln zu finden sind, nach denen ausschließlich die Anbieter der App für die Einhaltung der Gesetze verantwortlich sind (Baumgartner 2013, Rn. 434). Viele Nutzungsbedingungen der App Stores sehen darüber hinaus vor, dass eine Nutzung erst ab 13 Jahre zulässig ist (Baumgartner 2013, Rn. 448). Des Weiteren wird ein Altersklassifizierungssystem angeboten, das dem Kunden ermöglicht, den Zugang zum App Store so zu beschränken, dass nur Apps einer entsprechenden Altersklassifizierung geladen werden können und dies dementsprechend durch einen selbst gewählten PIN gesichert werden kann (Baumgartner 2013, Rn. 449). Die Entscheidung darüber, ob und wie eine entsprechende Sicherung aktiviert wird, wird demnach nicht vom Anbieter der App sondern von den Kunden selbst getroffen.

### 4.4.2 Einwilligungsunfähige

**Einwilligungsunfähige**

Bei Einwilligungsunfähigen ist das Problem der fehlenden Möglichkeit einer selbständigen Zustimmung parallel zu den Minderjährigen zu betrachten. Ggf. müsste hier ein Betreuer die Zustimmung erteilen. Die Frage wird im Einzelfall zu beantworten sein, ob Einsichtsfähigkeit gegeben sein kann.

## 4.5 Auslandsbezug

**Auslandsbezug**

Apps werden häufig im internationalen Kontext angeboten. Die Datenerhebung wird bei der Nutzung in Deutschland auch dort stattfinden. Ob die Speicherung und Nutzung jedoch auch in Deutschland stattfindet ist nicht zwingend, diese könnte auch im Ausland erfolgen.

Dem BDSG liegt das sog. Territorialprinzip zu Grunde. Gemäß Art. 4 Abs. 1 lit. c EU-Datenschutzrichtlinie kommt es hiernach auf den Ort an, an dem die datenschutzrechtlich verantwortliche Stelle ihren Sitz hat. Generell findet insoweit jeweils das dortige Datenschutzrecht Anwendung.

Wenn demnach sowohl Nutzerin oder Nutzer als auch Anbieter in Deutschland und die Nutzung der Daten im Inland stattfindet, finden die Bestimmungen des BDSG Anwendung. Wenn der Anbieter der App in einem anderen EU-Mitgliedstaat sitzt, gilt das sog. Sitzprinzip nach § 1 Abs. 5 S. 1 BDSG: „Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union“ oder in einem anderen Vertragsstaat des Abkommens über den Europäischen

Wirtschaftsraum gelegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland.

Außerhalb der EU gilt wieder das Prinzip des Ortes der Datenerhebung, -nutzung, und -verarbeitung. Damit wäre bei einer Erhebung von Daten mittels einer App in Deutschland deutsches Datenschutzrecht anwendbar. § 1 Abs. 5 S. 2 BDSG: „Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt."

Es darf bezweifelt werden, ob und inwieweit im letzteren Fall das deutsche Datenschutzrecht sich auch tatsächlich wirksam gegenüber App-Anbietern außerhalb der EU durchsetzen lässt (Baumgartner 2013, Rn. 201).

Wenn der Datenserver außerhalb der EU befindlich ist, wird folgendes Beispiel beschrieben: „Sitzt der App-Anbieter" in einem anderen EU-Mitgliedstaat, so ist das Datenschutzrecht dieses Staates maßgebend. Wird eine App dagegen in Deutschland von einem im EWR-Ausland ansässigen Anbieter angeboten und von einem deutschen Nutzer installiert, so werden dabei auch personenbezogene Daten des deutschen Nutzers im Inland zumindest erhoben. Auch wenn die weitere Nutzung und Verarbeitung dieser Daten dann außerhalb des EWR erfolgt – weil dort z.B. die Server des App-Anbieters stehen – gilt zumindest für die Erhebung der Daten deutsches Recht. (Gola, Klug und Körffer, Rn. 29 zitiert nach Baumgartner 2013, Rn. 198).

## 5 Folgerung

Es existiert ein umfassendes Datenschutzrecht in Deutschland und eine Vereinheitlichung der Regulation in Europa ist kurz vor der Umsetzung. Rechtlich sind hier namentlich Gesundheitsdaten besonders geschützt. Wenn die Rechtsgrundlagen konsequent im Zusammenhang mit der Nutzung von Apps umgesetzt werden, ist das schon vorgesehene Schutzniveau auf den Bereich der Apps übertragbar. Die Schwächen dürften in der Umsetzung durch die Anbieter und der mangelnden Transparenz bei der Einholung der Einwilligung und der Aufklärung sowie der Sensibilität der Anwenderinnen und Anwender im Zusammenhang mit datenschutzrechtlichen Fragen gegeben sein. Der Schutz Minderjähriger in Bezug auf die Datennutzung ist problematisch, unabhängig davon, ob in Ansehung der möglichen Einsichtsfähigkeit auch Heranwachsende Jugendliche ihre Einwilligung erteilen können. Die Minderjährigen können faktisch bei der von ihnen genutzten App selbst der Datenerhebung, -verarbeitung und -nutzung zustimmen, wobei in vielen Fällen die Zustimmung der Sorgeberechtigten fehlten dürfte oder eine entsprechende Einsichtsfähigkeit in die Tragweite der Entscheidung nicht gegeben ist. Damit läge keine wirksame Einwilligung vor. Soweit Daten von im Ausland niedergelassenen Verantwortlichen verarbeitet werden, ist der Ort der Niederlassung entscheidend. Bei einer Niederlassung im EWR ist die Niederlassung der für die Datenverarbeitung verantwortlichen Stelle entscheidend. Wenn die Datenverarbeitung im EWR-Ausland stattfindet, gilt deutsches Datenschutzrecht, weil die Daten im Inland erhoben werden.

Eine konsequente Umsetzung der vorhandenen Regelungen sowie die Schaffung entsprechender Deutlichkeit und Transparenz bei der Aufklärung und Einwilligung würde die Ausübung des individuellen Rechts auf informationelle Selbstbestimmung befördern. Hier ist namentlich zu diskutieren, ob eine formelle Vorgabe der Aufklärung und Einwilligung entsprechende Transparenz schaffen kann. Weil der Vertrieb regelmäßig über App-Stores erfolgt, erscheint eine entsprechende gemeinsame Verpflichtung, ggf. eine Pflicht zur Prüfung durch die App-Stores ebenfalls zu diskutieren.

## 6 Schlüsselergebnisse

- Der Datenschutz im Zusammenhang mit Apps wird im Allgemeinen kritisch betrachtet.
- Es wird beschrieben, dass die datenschutzrechtlichen Anforderungen häufig nicht eingehalten werden.
- Da bei Gesundheits-Apps rechtlich besonders geschützte und sensible Gesundheitsdaten betroffen sind, ist hier eine besondere Relevanz der Einhaltung des Datenschutzes gegeben.

- Das Datenschutzrecht ist mit dem Recht auf informationelle Selbstbestimmung in Deutschland verfassungsrechtlich verankert.
- Mit der Europäischen Datenschutzgrundverordnung wird künftig eine einheitliche europäische Regulierung erfolgen.
- Zur rechtmäßigen Erhebung, Verarbeitung und Nutzung von Daten ist jedenfalls entweder ein gesetzlicher Legitimationstatbestand aus dem grundlegenden Bundesdatenschutzgesetz oder einer ggf. spezielleren Regelung erforderlich oder es liegt die Einwilligung des Rechteinhabers vor.
- Das Datenschutzrecht enthält besondere Anforderungen an die Aufklärung und Einwilligung, die auch bei Apps einzuhalten sind, hierbei muss auch auf den Schutz der Minderjährigen besonders Rücksicht genommen werden.
- Bei Datenverarbeitung mit Auslandsbezug ist der Sitz der für die datenverarbeitende Stelle maßgeblich.
- Bei vollständiger Umsetzung der datenschutzrechtlichen Vorgaben ist auch bei Gesundheits-Apps entsprechender Datenschutz gewährleistet.
- Missbrauch und fehlende Umsetzung der Vorgaben sowie die weltweite Verbreitung von Apps sowie ein dementsprechendes Angebot scheinen die besagten Probleme zu begründen.
- Es ist zu erwägen, die Aufklärung und Einwilligung noch transparenter und ggf. einfacher zu gestalten und eine entsprechende Sensibilität der Nutzerinnen und Nutzer durch Aufklärung zu schaffen.

## 7 Zusammenfassung

Es wird beschrieben, dass die rechtlichen Vorgaben des Datenschutzes bei vielen Apps nicht ordnungsgemäß umgesetzt werden. Dies erscheint insbesondere bei Gesundheits-Apps problematisch, weil hier besonders sensible Daten berührt sind. Die existierenden Regeln enthalten bereits allgemeine sowie spezielle Vorschriften, auch zum besonderen Schutz von Gesundheitsdaten. Wenn also trotz dieser Regulation fehlerhafter respektive rechtswidriger Umgang mit personenbezogenen Daten konstatiert wird, erscheinen entweder Missbrauch, Unkenntnis oder ähnlich gelagerte Problem bei der Umsetzung bzw. Kontrolle zu sehen ist.

Maßgebliche Regelungswerke sind die einschlägige europäische Datenschutzrichtlinie und in Deutschland das BDSG sowie wichtige spezielle Regelungen im SGB V, SGB X, TMG und TKG. Die Erhebung, Verarbeitung und Nutzung ist nur mit Einwilligung der Rechteinhaber oder einer gesetzlichen Grundlage möglich. Hier ist insbesondere die Aufklärung und Einwilligung des Rechteinhabers problematisch. Dieser muss umfassend und transparent über die Datenerhebung, -verarbeitung und -nutzung aufgeklärt werden. Dies gilt auch für Minderjährige, die unter Umständen schon ohne entsprechende Einsichtsfähigkeit in die Tragweite der datenschutzrechtlichen Einwilligung eine solche abgeben. Diese wäre dann nicht wirksam. Auch die denkbare Datenverarbeitung und -nutzung im Ausland muss entsprechend bekanntgegeben werden.

## 8 Summary

When it comes to apps, often, manufacturers do not adequately comply with data protection regulations. Especially in a health context, this is an alarming issue due to the sensitivity of the data involved. There are comprehensive data protection laws in Germany that also cover data used in a health context. Unfortunately, these are not always observed. This may be due to an improper application of the existing laws and regulations as well as the lack of knowledge about how they should be applied.

Relevant regulations and directives in this context are especially the European data protection directive as well as, for Germany, the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) as well as applicable rules of the Social Code (SGB), Book 10, the German Telemedia Act (TMG) and the Telecommunications Act (TKG). The collection, processing and utilization of data is only allowed with the consent of those holding the rights to the data or based on if permitted by laws and regulations, which can be problematic. Adequate and comprehensive information about

the collection, processing and utilization of any data is obligatory. This also includes underage persons as well as those who represent them, since minors may potentially give their consent without being aware of the consequences. Data processing and utilization that takes place abroad must also be entered into all considerations and the rights holders need to be informed about this.

## 9 Literatur


Baumgartner, U. (2013), in: Baumgartner, U.; Ewald, K., Apps und Recht, C.H. Beck

Bayerisches Landesamtes für Datenschutzaufsicht (2014), Pressemitteilung vom 26.05.2014. Verfügbar unter https://www.lda.bayern.de/media/pm2014_08.pdf [Zugriff 15. Dez. 2015].

Bundesärztekammer (2015), Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Verfügbar unter http://www.bundesaerztekammer.de/richtlinien/empfehlungenstellungnahmen/schweigepflichtdatenschutz/ [Zugriff 29. Nov. 2015].

Buchner, B. (2006), Informationelle Selbstbestimmung im Privatrecht, Mohr Siebeck.

Bundesregierung (2012), Antwort der Bundesregierung vom 20.11.2012 auf eine Kleine Anfrage der Korte, J.; Hein, R.; Jelpke, U.; Petermann, J.; Sitte, P.; Tempel, F.; Wawzyniak, H.; die Fraktion DIE LINKE, BT-Drucksache 17/11539.

Datenschutzgruppe gemäß Artikel 29 der Europäischen Union (2013), Stellungnahme 2/2013 vom 27. 02.2013 zu Apps auf intelligenten Endgeräten (WP 202). Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_de.pdf [Zugriff 03. Jan. 2015].

Die Welt (2015), Stiftung Warentest bemängelt Datenschutz bei Apps. Verfügbar unter http://www.welt.de/wirtschaft/webwelt/article106371914/Stiftung-Warentest-bemaengelt-Datenschutz-bei-Apps.html [Zugriff 14. Okt. 2015].

Europäische Kommission (2015), Pressemitteilung vom 15.12.2015, Einigung über die EU-Datenschutzreform der Kommission wird digitalen Binnenmarkt voranbringen. Verfügbar unter http://europa.eu/rapid/press-release_IP-15-6321_de.htm [Zugriff 22. Dez. 2015].

Europäische Kommission (2012), Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM 2012 (KOM Jahr 2012 Seite 10) endgültig.

Gola, P.; Klug, C. & Körffer, B. (2015) in: Gola, P.; Klug, C.; Körffer, B. & Schomerus, R., Bundesdatenschutzgesetz, Kommentar, 12. Aufl. 2015, Einleitung, Rn. 1-29, C.H. Beck.

Hornung, G. (2012), Eine Datenschutz-Grundverordnung für Europa? – Licht und Schatten im Kommissionsentwurf vom 25.1.2012, ZD 3/2012, S. 99 ff. Verfügbar unter http://www.uni-passau.de/fileadmin/dateien/fakultaeten/jura/lehrstuehle/hornung/Hornung__Eine_Datenschutz-Grundverordnung_fuer_Europa__ZD_20.pdf [Zugriff 03. Jan. 2016].

Kamps, M. (2011), in: Lehmann, M. & Meents, J.-G., Informationstechnologierecht, Kapitel 20, Carl Heymanns Verlag.

Katzenmeier, C. (2015), in: Laufs, A.; Katzenmeier; C. & Lipp, V., Arztrecht, 7. Auflage 2015, IX. Berufsgeheimnis und Dokumentation, C.H. Beck.

Koreng, A. (2013), in: Solmecke, C.; Taeger, J. & Feldmann, T., Mobile Apps, Kapitel 4, De Gruyter

Korte, J.; Hein, R.; Jelpke, U.; Petermann, J.; Sitte, P.; Tempel, F.; Wawzyniak, H.; die Fraktion DIE LINKE (2012), Kleine Anfrage an die Bundesregierung, BT-Drucksache 17/11276.

Michels, J. (2014), in: Becker, U. & Kingreen, T., SGB V Gesetzliche Krankenversicherung, 4. Aufl. 2014, Vor § 284, C.H. Beck.

Nordmann, M. (2011) in: Lehmann, M. & Meents, J.-G., Informationstechnologierecht, Kapitel 16, Carl Heymanns Verlag.

Rehmann, W. & Heimhalt, D. (2014), Rechtliche Aspekte von Health-Apps; Arzneimittel und Recht, 253.

Schneider, J. & Härting, N. (2012), Wird der Datenschutz nun endlich internettauglich? Warum der Entwurf einer Datenschutz-Grundverordnung enttäuscht, ZD, S. 199 ff.

Simitis, S. (2014), in: Simitis, S. (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 8. Aufl., Nomos.

Spickhoff, A. in: Spickhoff, A. (Hrsg.), Medizinrecht, 2. Aufl. 2014, StGB § 205, C.H. Beck.

Stadler, T. (2011), Verstoßen Facebook und Google Plus gegen deutsches Recht? – Ausschluss von Pseudonymen auf Social-Media-Plattformen, *Zeitschrift für Datenschutz*, 57 ff.