walderwyss rechtsanwälte

Walder Wyss AG
Seefeldstrasse 123
Postfach
8034 Zürich
Schweiz

Telefon +41 58 658 58 58
Telefax +41 58 658 59 59
www.walderwyss.com

Michael Isler
Partner
Dr. iur.
Rechtsanwalt
Direkt +41 58 658 55 15
michael.isler@walderwyss.com

Gutachten

an	eHealth Suisse Koordinationsorgan Bund-Kantone
von	Dr.iur. Michael Isler unter Mitarbeit von Dr.iur. David Vasella und Dr.iur. et Dr.med. Kerstin Noëlle Vokinger
Betrifft	**Datenschutz und Informationssicherheit im Bereich „mobile health“ (mHealth)**
Datum	19. Januar 2018 MIS / bme / 7480783v3

Inhaltsübersicht

1. Executive Summary

1.1. Ausgangslage und gutachterliche Fragestellung

1 Gemäss Art. 8 EPDG kann der Patient nicht nur auf seine Daten im elektronischen Patientendossier (**ePD**) zugreifen (Abs. 1), sondern er kann auch selber **eigene Daten erfassen** (Abs. 2). Es ist vorgesehen, dem Patienten diese Zugriffsmöglichkeiten grundsätzlich auch über mobile Applikationen im Gesundheitsbereich (sog. **mHealth Apps**) zu gewähren, wobei vorliegend die Bereitstellung von Daten durch den Patienten selber im Vordergrund steht. Diesbezüglich stellen sich verschiedene Fragen des Datenschutzes und der Datensicherheit.

2 Da der mHealth Markt international ausgerichtet und in der Europäischen Union (**EU**) und den Vereinigten Staaten (**USA**) weiter fortgeschritten ist als in der Schweiz, soll die Rechtslage in den USA und der EU dem juristischen Gutachten als Ausgangspunkt dienen. Auf der Grundlage entsprechend gewonnener Erkenntnisse sollen ein möglicher Nachholbedarf für das schweizerische Recht identifiziert sowie zielführende Massnahmen zur Lückenschliessung aufgezeigt werden.

1.2. Rechtslage in Sachen mHealth in der EU und den USA

1.2.1. Rechtslage in der EU

3 Eine spezifische Regulierung von mHealth auf EU Ebene existiert nicht. Die Europäische Kommission (**EU Kommission**) hat allerdings im Jahr 2014 den Regulierungsrahmen in einem Grünbuch über mobile Health-Dienste (**Grünbuch**) zusammengefasst.

4 Aus dem Grünbuch sind mehrere Projekte hervorgegangen, unter anderem hat die EU Kommission die Erarbeitung eines Datenschutzkodex für mHealth Apps (**EU Code of Conduct**) angestossen. Die Kommission will den Entwicklern von mHealth Apps damit eine Anleitung zur Einhaltung des europäischen Datenschutzrechts in die Hand geben und das Vertrauen der Konsumenten in solche Apps stärken. Die definitive Verabschiedung des EU Code of Conduct steht noch aus. Die Einhaltung des EU Code of Conduct soll freiwillig sein. Entwickler, die sich zertifizieren lassen, können aber in einem öffentlichen Register verzeichnet werden. Die Verwaltung des Codes obliegt einem Aufsichtsorgan.

5 Der EU Code of Conduct steht ganz im Zeichen der EU Datenschutz-Grundverordnung (**DSGVO**), welche auf den 25. Mai 2018 die europäische Datenschutz-Richtlinie (**Datenschutz-RL**) und die entsprechenden nationalen Datenschutzgesetze ablöst. Die wichtigsten Grundätze der DSGVO im mHealth-Kontext sind die folgenden:

- Für **Gesundheitsdaten** gilt ein strenges **Bearbeitungsverbot mit Erlaubnisvorbehalt**. Jede Bearbeitung bedarf somit eines Rechtfertigungsgrunds; dieser kann in einer ausdrücklichen Einwilligung der betroffenen Person bestehen;

- Der Grundsatz von **Privacy by Design** (Datenschutz durch Technikgestaltung) beinhaltet die Pflicht, nicht erst bei der konkreten Datenverarbeitung, sondern bereits in einem früheren Stadium die erforderlichen Massnahmen vorzusehen, um die Datenschutzgrundsätze einzuhalten;

- Der Grundsatz von **Privacy by Default** (datenschutzfreundliche Voreinstellung) sieht im Wesentlichen vor, dass ein Produkt oder Dienst bereits beim ersten Aufruf durch den Nutzer die datenschutzfreundlichsten Einstellungen aufzuweisen hat;

- Die **Datensicherheit** ist zu gewährleisten. Jeder Verarbeiter ist verpflichtet, mit technischen und organisatorischen Massnahmen ein dem Risiko angemessenes Schutzniveau sicher zu stellen. Datensicherheit ist somit nicht nur technisch, sondern als umfassendes Konzept zu verstehen.

6 Die für mHealth besonders wichtigen Grundsätze von Privacy by Design, Privacy by Default und Datensicherheit gelten allerdings nicht für **Hersteller** von Systemen (bspw. Softwarehersteller von Apps), sofern sie nicht gleichzeitig Datenverarbeiter sind. Diese Lücke will der EU Code of Conduct schliessen, indem er eine **Datenschutz-Zertifizierung von Produkten** auf der Herstellungsstufe forciert.

1.2.2. Rechtslage in den USA

7 In den USA wird die Entwicklung und Integration von mHealth sowohl von der Wissenschaft als auch von verschiedenen staatlichen Behörden, unter anderem der *Food und Drug Administration* (**FDA**) gefördert. Der Schwerpunkt liegt auf der Medizinprodukteregulierung, doch kommt auch dem Datenschutz ein hoher Stellenwert zu.

8 Datenschutz wird in den USA diametral anders verstanden als in Europa. Im Vordergrund steht nicht der Schutz der Persönlichkeit der Datensubjekte, sondern die freie Verwertbarkeit der Daten als Wirtschaftsgut. Dennoch gibt es in den USA eine Fülle von sektor- oder ereignisspezifischen Datenschutzvorschriften auf Bundes- wie auch auf einzelstaatlicher Ebene. Im Gesundheitsbereich sind dies auf Bundesebene primär die Health Insurance Portability and Accountability Act (**HIPAA**) sowie die Health Information Technology for Economic and Clinical Health Act (**HITECH**). Diese Gesetzeswerke regeln, wie nicht-anonymisierte Gesundheitsdaten (sogenannte *„protected health information*“, **PHI**) zu schützen sind und Zuwiderhandlungen sanktioniert werden sollen. Drei Prinzipien stehen im Vordergrund:

– Die **Privacy Rule** setzt Minimalvorschriften in Bezug auf den Datenschutz, die Nutzung sowie die Offenlegung von PHI;

– Die **Security Rule** will auf vier Ebenen (administrative Schutzmassnahmen, physische Schutzmassnahmen, organisatorische Schutzmassnahmen, Richtlinien und Prozesse) die Sicherheit für elektronische Gesundheitsdaten gewährleisten;

– Die **Breach Notification Rule** besagt, dass die betroffenen Patienten und das zuständige Aufsichtsorgan über Verletzungen der Datensicherheitspflichten aufzuklären sind.

9 Die vorstehenden Pflichten gelten nicht für sämtliche mHealth Apps. Bedingung ist, dass diese PHI verarbeiten. Dies ist nur dann der Fall, wenn Mitarbeiter von Gesundheitsdiensten entweder auf die App zugreifen oder dem Patienten über die App Informationen mitteilen. Somit unterliegen Apps, die lediglich dazu dienen, Daten des Patienten in das Gesundheitssystem zu übermitteln, nicht den strengen Vorgaben von HIPAA und HITECH. In der Praxis werden allerdings durch die *Federal Trade Commission* auch bei der Untersuchung von Verletzungen der Datensicherheit **in anderen Sektoren ähnliche Standards** herangezogen.

1.2.3. Gesamtwürdigung

10 Sowohl in der EU wie auch in den USA kommt dem **Schutz von Gesundheitsdaten hohes Gewicht** zu, wobei in den USA der Anwendungsbereich von HIPAA und HITECH nur eine begrenzte Zahl von mHealth Apps direkt betrifft, vergleichbare Sicherheitsstandards aber auch in anderen Sektoren mit notorisch sensitiver Datenverarbeitung herangezogen werden.

11 In der EU gilt demgegenüber für die Verarbeitung von Gesundheitsdaten ein strenger allgemeingültiger Regulierungsrahmen. Es wird sich zeigen, ob die DSGVO im globalen Kontext effektiv durchgesetzt werden kann. Gerade im Bereich mHealth ist zu erwarten, dass die Anbieter von mHealth Apps dem Datenschutz inskünftig mehr Beachtung schenken werden. Datenschutz-Compliance dürfte zum Wettbewerbsvorteil werden, gerade auch, wenn sich der EU Code of Conduct zu einem Instrument mausern sollte, an dem für seriöse mHealth-Anbieter kein Weg vorbeiführt.

1.3. Anpassungsbedarf für das schweizerische Recht

1.3.1. Schweizerischer Datenschutzrahmen für mHealth Apps

12 Auch wenn sich die Anbieter von mHealth Apps in einem globalen Umfeld bewegen und selten in der Schweiz ansässig sind, sind die schweizerischen Datenschutzvorschriften dennoch anwendbar, wenn Daten von Personen in der Schweiz bearbeitet werden.

13 Das schweizerische Datenschutzgesetz (**DSG**) wird derzeit umfassend revidiert, um es in Einklang mit den Vorgaben der DSGVO zu bringen. Die Revision des Datenschutzgesetzes wird daher bei den weiteren Ausführungen mitberücksichtigt.

14 Das DSG verfolgt einen grundsätzlich anderen Ansatz als das europäische Pendant. Es herrscht kein Bearbeitungsverbot mit Erlaubnisvorbehalt wie im europäischen Recht, sondern ein **Transparenzgebot mit Verbotsvorbehalt**. Für die Datenbearbeitung bedarf es also in der Regel keiner Einwilligung der betroffenen Person. Es müssen jedoch die wesentlichen **Datenbearbeitungsgrundsätze** eingehalten werden, nämlich:

- Grundsatz der Transparenz;
- Grundsatz der Zweckbindung;
- Grundsatz der Verhältnismässigkeit;
- Grundsatz der Datenintegrität;
- Grundsatz der Datensicherheit.

15 Gesundheitsdaten sind **besonders schützenswerte Daten**, weshalb qualifizierte Transparenzvorschriften für deren Bearbeitung gelten. Darüber hinaus ist die Bekanntgabe von Gesundheitsdaten an Dritte untersagt, bedarf also stets der Einwilligung der betroffenen Person oder eines anderen Rechtfertigungsgrunds.

16 Der schweizerische Ansatz ist folglich liberaler als der europäische, doch ist deswegen das **Schutzniveau nicht geringer**. Geht die Datenbearbeitung nämlich über den primären Zweck der Bearbeitung gesundheitsbezogener Informationen im Rahmen der Kernfunktionen der mHealth App hinaus, ist sie entweder nicht mehr verhältnismässig oder – im Falle einer Bekanntgabe von Gesundheitsdaten an Dritte – ohnehin untersagt, weshalb für exorbitante Bearbeitungszwecke auch nach schweizerischem Recht stets die Einwilligung der betroffenen Person erforderlich ist. Es besteht somit kein Anpassungsbedarf.

1.3.2. Vorgaben des EPDG

17 Für die Anbindung von mHealth Apps an das ePD existieren keine spezifischen Vorschriften. Da der Grad der Einbindung von mHealth Apps nach den gegenwärtig vorliegenden Lösungsansätzen in der Regel geringer sein dürfte als bei den stärker mit dem ePD interagierenden Primärsystemen, können die Anforderungen für die Anbindung von **Primärsystemen** (Inventarisierung; Sicherstellung des Datenschutzes und der Datensicherheit) **nicht *tel quel* für mHealth Apps** übernommen werden. Dennoch ist es erforderlich, dass mHealth Apps, die über ein mobiles Gateway an das ePD angebunden sind, minimalen Anforderungen an den Datenschutz und die Datensicherheit gerecht werden.

18 Vorläufig ist angedacht, dass die über mHealth Apps bereitgestellten Daten erst dann als Dokumente in den Vertrauensraum des ePD gelangen können, wenn der Patient im Einzelfall in den Datentransport eingewilligt hat. Dies ist nicht besonders nutzerfreundlich. Sollte allerdings eine **automatische Bereitstellung der Daten** einer mHealth App über das patientenseitige Zugangsportal direkt in das ePD vorgesehen sein (*machine-to-machine*-Authentifizierung), müssten sowohl die einer solchen automatisierten Datenbereitstellung **vorgelagerte globale Einwilligung** des Patienten wie auch die weiteren Anforderungen an die Datensicherheit und den Datenschutz für die fraglichen mHealth Apps zwingend auf einem hohen Schutzniveau festgelegt werden. Gegenwärtig stehen einer solchen Lösung allerdings Art. 23 lit. b und c EPDV entgegen, wonach das Identifikationsmittel für die Patienten so aufgebaut sein muss, dass es nur von der berechtigten Person selber verwendet werden kann, und ein Authentifizierungsverfahren mit mindestens zwei Authentifizierungsfaktoren vorgesehen ist.

19 Schliesslich sind die Stammgemeinschaften verpflichtet, den Patienten Datenschutz- und Datensicherheitsmassnahmen zu empfehlen. Diese **Informations- und Aufklärungspflicht** erstreckt sich auch auf den Umgang mit mHealth Apps.

1.3.3. Gegenüberstellung

20 Eine Gegenüberstellung des schweizerischen Datenschutzrahmens (unter Berücksichtigung der DSG-Revision) mit der Rechtsordnung in der EU und den USA ergibt folgendes Bild:

Aspekt	EU (DSGVO)	USA (HIPAA)	CH (E-DSG)
Regulierungsansatz	Kombination aus regel- und prinzipienbasierter allgemeingültiger Regulierung; zahlreiche mHealth-Initiativen	Regelbasiert und sektorspezifisch; in Bezug auf die allgemeine Informationssicherheit ebenfalls prinzipienbasierter *„reasonableness"* Ansatz mit ziemlich konkreten, durch die FTC-Aufsicht vorgegebenen Leitplanken	Prinzipienbasiert und allgemeingültig
Bearbeitungsgrundsätze für Gesundheitsdaten	Qualifiziertes Bearbeitungsverbot mit Erlaubnisvorbehalt	Transparenzgebot und Bekanntgabeverbot	Qualifiziertes Transparenzgebot und Bekanntgabeverbot
Privacy by Design / Privacy by Default	Ja	HIPAA-Vorgaben müssen implementierbar sein	Ja
Datensicherheit	Prinzipienbasierte Regulierung, keine verbindlichen	Spezifische Vorgaben; NIST Information Security Standard (nicht	Prinzipienbasierte Regulierung, keine verbindlichen

Aspekt	EU (DSGVO)	USA (HIPAA)	CH (E-DSG)
	Standards; Datenschutz-Folgenabschätzung als Instrument zur Risikoprävention	verbindlich)	Standards; Datenschutz-Folgenabschätzung als Instrument zur Risikoprävention
Meldepflichten bei Datensicherheitsverletzungen	An Behörde und ggf. betroffene Personen	An Behörde und betroffene Personen (unterhalb Erheblichkeitsschwelle: jährliche Meldung)	An Behörde und ggf. betroffene Personen
Zertifizierungsverfahren für Produkte (z.B. mHealth Apps)	Vorgesehen, aber kaum genutzt EU Mobile Code of Conduct	Nicht vorgesehen	Vorgesehen, aber bislang nicht umgesetzt

1.4. Durchsetzungsmechanismen

1.4.1. Präventive Schutzmassnahmen

21 Der griffigste Durchsetzungsmechanismus ist die präventive Kontrolle. Die **Stammgemeinschaften** nehmen diesbezüglich als **Gatekeeper** im Rahmen der Anbindung von mHealth Apps an das EDP eine zentrale Rolle wahr. Es liegt deshalb grundsätzlich an den Stammgemeinschaften, die zu erarbeitenden Kriterien für die Anbindung von mHealth Apps anzuwenden und durchzusetzen.

22 Folgende Instrumente kommen hierfür in Frage:

– **Verwaltungsrechtliche Massnahmen** (Prüfkriterien und Standards bei der Anbindung von mHealth Apps);

– **Vertragsrechtliche Massnahmen** (vertragliche Regelung der Integration der mHealth Apps an das ePD);

– **Technische und organisatorische Massnahmen** (Audits, Monitoring der mHealth-Landschaft).

23 Fraglich ist allerdings, ob die Stammgemeinschaften diese **anspruchsvolle Rolle** ausfüllen können und wollen; eine unterschiedlich gehandhabte Zugangspolitik für mHealth Apps könnte überdies den ohnehin kleinen mHealth-Markt in der Schweiz noch weiter fragmentieren. Dieses Defizit liesse sich möglicherweise beheben, indem

– im Gesetz und im Ausführungsrecht **externe Zugangsportale** mit Schreibrecht für die Patienten zugelassen würden; und/oder

– das Bundesamt für Gesundheit (**BAG**) eine über das Aufstellung von Zertifizierungsvoraussetzungen hinausgehende **unterstützende Funktion** wahrnehmen würde.

In beiden Fällen wären voraussichtlich **Anpassungen auf Gesetzes- und Verordnungsstufe** erforderlich.

1.4.2. Rechtsbehelfe der Endnutzer

24 Der Datenschutz baut in erster Linie darauf, dass sich die Rechtsunterworfenen an die rechtlichen Vorgaben halten. Die abschreckende Wirkung von Sanktionen sowie die öffentliche Prangerwirkung von Datenschutzverstössen tragen ebenfalls zur Compliance bei. Den Endnutzern stehen zwar durchaus auch Rechtsbehelfe zur Verfügung, mit denen sie ihre persönlichen Schutzinteressen durchsetzen können, doch ist vor allem der **zivilrechtliche Klageweg** für den einzelnen **teuer** und aufgrund der über weite Strecken beim Kläger liegenden Beweislast auch mit **Risiken** verbunden. Im Einzelfall stehen dem Nutzer aber auch die Mittel des **Strafrechts** oder eine **Anzeige bei der Datenschutzaufsicht** als Rechtsbehelfe zur Verfügung.

1.5. Empfohlene Massnahmen

25 Nachstehend folgt eine tabellarische Zusammenfassung der empfohlenen Massnahmen:

Nr.	Massnahme	Gesetzl. Grundlage
1	Überdenken der dezentralen Bereitstellung der Zugangsportale für Patienten durch die Stammgemeinschaften; Evaluation einer Zulassung externer Zugangsportale, die nebst dem Leserecht auch eine Datenbereitstellung durch die Patienten gemäss Art. 8 Abs. 2 EPDG ermöglichen würden (bedingt ev. Änderung auf Gesetzesstufe).	EPDG 1 IV EPDG 10 II EPDG 11 (b) EPDV 30 f.
2	Vermeiden der Verknüpfung der mHealth App mit elektronischer Identität des Patienten (Patientenidentifikationsnummer).	EPDV 10 III EPDV 12 IV
3	Ermöglichen einer automatisierten Datenbereitstellung durch mHealth Apps (*machine-to-machine*) nur unter entsprechend strengen Anforderungen an Datenschutz und Datensicherheit (bedingt Änderungen auf Verordnungsstufe).	EPDV 23 (b) EPDV 23 (c)
4	Sensibilisierung der Patienten und Gesundheitsfachpersonen über datenschutzspezifische Risiken von mHealth Apps; Ausarbeiten eines diesbezüglichen Merkblatts zur Verwendung durch die Stammgemeinschaften.	EPDV 15 II

Nr.	Massnahme	Gesetzl. Grundlage
5	Kriterienkatalog für die Anbindung von mHealth Apps mit datenschutzrechtlichen Mindestanforderungen, einschliesslich Pflicht zur Prüfung (Due Diligence) von mHealth Apps hinsichtlich der Einhaltung der Anforderungen.	
	Verantwortung für das Aufstellen des Kriterienkatalogs liegt beim EDI (BAG).	EDPG 12 I (b)
	Verantwortung für die Durchführung der Due Diligence sollte ebenfalls beim BAG (anstelle der Stammgemeinschaften) liegen (bedingt Änderungen auf Gesetzes- und Verordnungsstufe). Denkbar wäre auch eine Durchführung dieser Prüfung durch ein externes Zugangsportal (vgl. Massnahme 1).	EPDG 12 II EPDV 30 III
6	Aufstellen von Vorgaben für die vertragliche Anbindung von mHealth Apps.	EDPG 12 I (b) EPDV 12
	Erarbeiten einer (freiwilligen) Mustervorlage für einen Integrationsvertrag, der die Anbindung von mHealth Apps an die ePD-Schnittstelle auf der Grundlage schweizerischen Rechts datenschutzkonform regelt.	n/a

2. Ausgangslage

2.1. Struktur des elektronischen Patientendossiers (ePD) und rechtlicher Rahmen

26 Das elektronische Patientendossier (**ePD**) ist ein zentrales Element der von Bund und Kantonen gemeinsam erarbeiteten Strategie „eHealth Schweiz", welche der fortschreitenden Digitalisierung im Gesundheitswesen Rechnung trägt. Das ePD ist im Bundesgesetz vom 19. Juni 2015 über das elektronische Patientendossier (**EPDG**)[1] verankert.[2] Es legt die Massnahmen zur Einführung, Verbreitung und Weiterentwicklung des ePD fest (Art. 1 Abs. 2 EPDG) und regelt die Voraussetzungen für die Bearbeitung der Daten des ePD (Art. 1 Abs. 1 EPDG). Weiter bezweckt das Gesetz die Stärkung der Qualität und die Verbesserung der Prozesse der medizinischen Behandlung wie auch die Steigerung der Effizienz des Gesundheitssystems; gleichzeitig sollen aber auch die Patientensicherheit erhöht und die Gesundheitskompetenz der Patientinnen und Patienten[3] gefördert werden (Art. 1 Abs. 3 EPDG).[4]

27 Um das ePD begrifflich erfassen zu können, muss man dessen Architektur und Funktionsweise verstehen.[5] Das ePD ist ein sog. Sekundärsystem.[6] In diesem werden keine Krankengeschichten und andere Patientendossiers direkt erstellt, diese sind vielmehr in den Primärsystemen (Klinikinformations- und Praxissystemen) der Leistungserbringer abgelegt. Diejenigen Daten aus der Krankengeschichte, welche für die Weiterbehandlung eines Patienten relevant sind, sowie die vom Patienten selber erfassten Daten, werden in separierte dezentrale Ablagesysteme kopiert.[7] Das EPDG ermöglicht es, auf diese dezentral abgelegten Dokumente in einem konkreten Behandlungsfall zuzugreifen (Art. 2 lit. a EDPG).

---

1 SR 816.1.

2 Weiter sind die folgenden Verordnungen zu beachten:
- Verordnung vom 22. März 2017 über das elektronische Patientendossier (**EPDV**; SR 816.11);
- Verordnung vom 22. März 2017 des EDI über das elektronische Patientendossier (**EPDV-EDI**; SR 816.111);
- Verordnung vom 22. März 2017 über die Finanzhilfen für das elektronische Patientendossier (**EPDFV**; SR 816.12).

3 Für die verbesserte Lesbarkeit wird im Weiteren nur die männliche Form verwendet.

4 Eingehend zur Zielsetzung des ePD BAUR ISABEL/BLUM-SCHNEIDER BRIGITTE/EGGER MICHAEL, Das elektronische Patientendossier, *in:* Jusletter 28. August 2017, Rz. 5 ff.; vgl. auch Botschaft zum Bundesgesetz über das elektronische Patientendossier (EPDG) vom 29. Mai 2013, BBl 2013 5321, 5327 ff.

5 Eingehend hierzu WIDMER BARBARA, Das elektronische Patientendossier – ein Mammutprojekt wird Realität, *in:* AJP 2017, 765–779, 769 ff.

6 BAUR/BLUM-SCHNEIDER/EGGER (Fn. 4), Rz. 10.

7 Erläuterungen zur Verordnung über das elektronische Patientendossier (EPDV) und zur Verordnung des EDI über das elektronische Patientendossier (EPDV-EDI), Fassung vom 22. März 2017, 18. f.

Das ePD ist somit eine Linksammlung zu den Dokumenten, die in den dezentralen Ablagesystemen zu einem bestimmten Patienten gespeichert sind (virtuelles Dossier).[8]

28 Das ePD wird von sog. Stammgemeinschaften und Gemeinschaften betrieben (vgl. Art. 10 EPDG und Art. 9 ff. EPDV). Selbstredend nehmen der Datenschutz und die Datensicherheit bei der Wahrnehmung dieser Aufgabe einen hohen Stellenwert ein (vgl. Art. 12 EPDV). Den Stammgemeinschaften, welche für die Eröffnung und Schliessung eines ePD verantwortlich sind, obliegt zusätzlich die Patienteninformation und -beratung (vgl. Art. 15 EPDV).

2.2. Anknüpfungspunkt und Ziele der Anbindung von mHealth Apps an das EPD

29 Gemäss Art. 8 EDPG kann der Patient nicht nur auf seine Daten im ePD zugreifen (Abs. 1), sondern er kann auch selber eigene Daten erfassen (Abs. 2). Es ist vorgesehen, den Patienten diese Zugriffsmöglichkeiten grundsätzlich auch über mobile Applikationen im Gesundheitsbereich (sog. **mHealth Apps**) zu gewähren.[9]

30 Das Angebotsspektrum von mHealth Apps ist ausserordentlich vielfältig.[10] Im behandlungsrelevanten Kontext, der beim ePD im Zentrum steht, kommen z.B. mobile Applikationen zur Beobachtung chronisch kranker Patientin oder die Langzeitbetreuung älterer Menschen in Betracht.[11] Potenziell behandlungsrelevant können aber auch Vitalparameter sein, die mittels sog. *„Quantified Self"*-Applikationen (Bewegungs- und Biodaten) erfasst werden und als diagnostische Basis zur Erkennung von Gesundheitsstörungen dienen oder für medizinische, ernährungstechnische oder bewegungstherapeutische Empfehlungen herange-

8 WIDMER, AJP 2017 (Fn. 5), 770 f.

9 EHEALTH SUISSE, mobile Health (mHealth) Empfehlungen I, 16. März 2017, 8.

10 Internetportale, welche die ganze Breite des Angebots zeigen und laufend aktualisieren, sind bspw. https://www.imedicalapps.com/ und http://www.mobihealthnews.com (beide zuletzt besucht am 9. Oktober 2017); vgl. aus rechtlicher Sicht auch AEBISCHER GILLES, Les applications mobiles de santé, *in:* AJP 2017, 63–72; FUCHS PHILIPPE/GIOVANETTONI MARCO, Apps als Medizinprodukte – und die Folgen davon, *in:* Jusletter 27. Mai 2013; ISLER MICHAEL, Mobile Medical Apps: Patient Datenschutz, *in:* digma 2013, 110–115; DERS., Lifesyste- oder Medizinprodukt? *in:* digma 2016, 64–69; KELLER CLAUDIA, Fitness-Apps als Datensammler: Was sagt das Recht? *in:* Computerworld 5/27. März 2015, 20–22; KLETT BARBARA, Digitalisierte Gesundheit – Abgrenzungen und Regulierung, *in:* HAVE 2017, 104–113; KLETT BARBARA/VERDE MICHAEL, Medizinalprodukt- und haftpflichtrechtliche Aspekte bei Medizinal-Apps, *in:* Sicherheit & Recht 2016, 45–54.

11 Vgl. FHS ST. GALLEN, mHealth im Kontext des elektronischen Patientendossiers. Eine Studie im Auftrag von eHealth Suisse, 19. März 2015, 31 ff.

zogen werden können.[12] mHealth hat das Potential, die Qualität und die Effizienz der Behandlung zu steigern, indem bspw. Ärzte den Gesundheitszustand von Patienten ortsunabhängig beobachten und überwachen können oder indem Patienten ihre Compliance erhöhen, etwa dank der Verwendung von Erinnerungsfunktionen für die Arzneimitteleinnahme oder die Terminvereinbarung.[13]

31 Der Zugriff des Patienten auf das ePD erfolgt nach der gesetzlichen Regelung ausschliesslich[14] über das interne Zugangsportal seiner Stammgemeinschaft (Art. 10 Abs. 2 lit. b Ziff. 2 und 3 EPDG), welches vom Zugangsportal für Gesundheitsfachpersonen getrennt ist.[15] Die über mHealth Apps erhobenen Daten sollen über ein mobiles Gateway empfangen und eDP-konform als Dokumente aufbereitet werden können. Anschliessend kann der Patient diese Dokumente aktiv mittels Authentifizierung in das ePD überführen.[16] Die vom Patienten selbst erfassten Daten müssen in einer von der Stammgemeinschaft bereitgestellten dedizierten gemeinschaftsinternen Dokumentenablage gespeichert werden (EPDV-EDI, Anhang 2, Ziff. 10.1.1); Grund für diese logische oder physische Trennung der vom Patienten erfassten Daten von anderen ePD-Dokumenten sind Datensicherheitsüberlegungen.[17]

32 Sofern auch vorgesehen ist, dass der Patient Dokumente aus dem ePD abruft, um diese einer mHealth App zur Verfügung zu stellen, würden die Daten den umgekehrten Weg gehen, und das mobile Gateway müsste die Dokumente in ein standardisiertes Datenformat zurück konvertieren.[18]

---

12 ISLER, digma 2016 (Fn. 10), 64; EHEALTH SUISSE, Empfehlungen I (Fn. 9), 15; vgl. auch die weiteren Anwendungsszenarien in HINT AG, Patientenseitige Daten im elektronischen Patientendossier. Ein Konzept im Auftrag von eHealth Suisse, 1. Mai 2015, 17 ff.

13 Empfehlungen I (Fn. 9), 8.

14 Botschaft EPDG (Fn. 4), BBl 2013, 5336 und 5339.

15 WIDMER, AJP 2016 (Fn. 5), 774.

16 Vgl. die Beschreibung eines möglichen Lösungskonzepts in HINT AG (Fn. 12), 33 ff.; eine definitive Lösungsarchitektur existiert noch nicht. Neben dem Upload der mittels mHealth Apps erhobenen Daten über das ePD dürfte ebenso häufig eine Datenübermittlung an das Primärsystem des Leistungserbringers möglich sein. Die Bereitstellung der behandlungsrelevanten Daten im ePD würde in dieser Konstellation durch die Gesundheitsfachperson über ihr eigenes Zugangsportal erfolgen.

17 Erläuterungen EPDV-EDI (Fn. 7), 32.

18 Dieser Anwendungsfall, der Abruf von Dokumenten aus dem ePD zur weiteren Nutzung durch mHealth Apps, ist in den Empfehlungen I (Fn. 9) sowie den weiteren Studien und Konzepten bislang nicht vorgesehen. Er wird daher im Rahmen dieses Gutachtens auch nicht weiter vertieft. Grundsätzlich dürften aber aus Sicht des Datenschutzes für das „Download"-Szenario dieselben Überlegungen gelten wie für das „Upload"-Szenario.

33 Der Einbezug von mHealth Apps in das ePD bietet sich vor dem Hintergrund der Zwecksetzungen des EPDG[19] in zweifacher Hinsicht an:

– Zum einen wird mHealth ein enormes Effizienzsteigerungspotential im Behandlungsprozess zugeschrieben, da Prävention, Monitoring und Adhärenz verbessert werden können.[20]

– Zum anderen trägt der Patient mehr zum Behandlungsprozess bei, er übernimmt Eigenverantwortung und verbessert dadurch seine Gesundheitskompetenz.[21]

2.3. Gutachterliche Aufgabenstellung

34 Die Bedeutung von mHealth hat in den letzten Jahren im klinischen Alltag kontinuierlich zugenommen. Laut einer in Deutschland durchgeführten Studie bei Ärzten verwenden mehr als die Hälfte der befragten Ärzte täglich Apps im Rahmen ihrer Berufsausübung.[22] mHealth ist gegenwärtig stark anbieter- und konsumgetrieben, hingegen fehlt in der Schweiz bisher ein koordiniertes Vorgehen.[23]

35 Die Vorteile von mHealth lassen sich freilich nur dann ausschöpfen, wenn die Rahmenbedingungen und Voraussetzungen für einen vertrauensvollen und sicheren Umgang mit den mobilen Technologien geschaffen sind.[24] Ein wesentlicher Faktor neben der Datenqualität sind diesbezüglich der Datenschutz und die Datensicherheit. Es stellen sich Fragen zum anwendbaren Datenschutzrahmen, der Transparenz der Datenbearbeitung, den zulässigen Bearbeitungszwecken sowie den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit.[25] Aufgrund der Komplexität des App-Ökosystems mit seinen zahlreichen Datenübergabepunkten und im gesundheitlichen Be-

19 Vgl. vorstehend, Rz. 26.
20 FHS St. Gallen (Fn. 11), 15 f.; vgl. auch vorstehend, Rz. 30.
21 FHS St. Gallen (Fn. 11), 17 f.
22 Medinside, Die App gehört zum Berufsalltag, 24. August 2017, https://www.medinside.ch/de/post/die-app-gehoert-zum-aerztealltag (zuletzt besucht am 9. Oktober 2017). Zu berücksichtigen ist allerdings, dass sich die Befragung nur aus 252 Teilnehmern zusammensetzte, weshalb die Ergebnisse mit Vorsicht zu geniessen sind.
23 Vgl. Webseite von eHealth Suisse, https://www.e-health-suisse.ch/gemeinschaften-umsetzung/ehealth-aktivitaeten/mhealth.html (zuletzt besucht am 9. Oktober 2017).
24 Empfehlungen I (Fn. 9), 8.
25 Empfehlungen I (Fn. 9), 25 f.

reich oft unerfahrenen Marktakteuren ist die Anfälligkeit für Datenschutzverletzungen besonders gross.[26]

36 In starkem Kontrast zu dieser Bestandsaufnahme zeigen Untersuchungen, dass der Datenschutz bei einer Mehrheit der mHealth Apps im Argen liegt. Es fehlt nicht nur an Selbstverständlichkeiten wie Datenschutzerklärungen, sondern es wird vor allem auch die Datensicherheit stark vernachlässigt.[27]

37 Aufgrund der vorstehenden Erkenntnisse hat das Koordinationsorgan eHealth Suisse im Rahmen einer Handlungsempfehlung den folgenden Auftrag für ein juristisches Gutachten erteilt:

38 Der Handlungsbedarf im Bereich Datenschutz und Informationssicherheit soll mit Blick auf das Thema mHealth allgemein sowie im Weiteren unter speziellem Fokus auf die Interoperabilität mit dem ePD in einem juristischen Gutachten erörtert werden; zu berücksichtigen gilt es sowohl die Patientensicht als auch die Sicht der Gesundheitsfachpersonen.

39 Da der mHealth-Markt international ausgerichtet und in der Europäischen Union (**EU**) und den Vereinigten Staaten (**USA**) weiter fortgeschritten ist als in der Schweiz, soll die Rechtslage in den USA und der EU dem juristischen Gutachten als Ausgangspunkt dienen. Auf der Grundlage entsprechend gewonnener Erkenntnisse sollen ein möglicher Nachholbedarf für das schweizerische Recht identifiziert sowie zielführende Massnahmen zur Lückenschliessung aufgezeigt werden.

40 Gestützt auf diese Ausgangslage soll das juristische Gutachten folgende Fragen klären:

> *1. Wie gestaltet sich die Rechtslage in Sachen mHealth in den USA und der EU?*
>
> *2. Lässt sich gestützt auf die Erkenntnisse aus der ersten Frage für das schweizerische Recht Anpassungsbedarf*

---

26 ISLER, digma 2013 (Fn. 10), 110 f.; vgl. auch ARTIKEL 29-DATENSCHUTZGRUPPE, Opinion 02/2013 on apps on smart devices, 27. Februar 2013, 5; dieselbe Komplexität und entsprechende Risikoneigung stellt sich auch beim ePD, vgl. WIDMER, AJP 2017 (Fn. 5), 768; DIES., ePatientendossier und Datenschutz, *in:* digma 2017, 160–168, 160 („datenschutzrechtliches Worst-Case Szenario").

27 EPRIVACY GMBH, Datensicherheit und Datenschutz von Medical Apps, Whitepaper, November 2015; vgl. auch ISLER, digma 2013 (Fn. 10), 111.

identifizieren und wenn ja, welchen (erforderlich sind konkrete Vorschläge für Massnahmen)?

3. Wie lassen sich datenschutz- und informationssicherheitsrechtliche Vorgaben gegenüber den Entwicklern, Herstellern und Anbietern von mHealth-Lösungen (Apps und ähnlichem), die in der Regel sowohl im Verhältnis zueinander als auch im Verhältnis zu den Endnutzern unterschiedlichen Rechtsordnungen unterstehen, effektiv durchsetzen (erforderlich sind konkrete Vorschläge für Massnahmen)?

4. Wie gestaltet sich die Sach- und Rechtslage für die Endnutzer und -nutzerinnen von mHealth-Lösungen und wie können diese vor missbräuchlichen Bearbeitungen ihrer Gesundheitsdaten geschützt werden (erforderlich sind konkrete Vorschläge für Massnahmen)?

3. Rechtslage in Sachen mHealth in der EU und den USA

3.1. Rechtslage in der EU

3.1.1. Regulierung von mHealth auf EU-Ebene

3.1.1.1. Grünbuch über Mobile Health-Dienste

41 Eine spezifische Regulierung von mHealth auf EU-Ebene existiert nicht. Die Europäische Kommission (**EU Kommission**) hat allerdings im Jahr 2014 den Regulierungsrahmen in einem Grünbuch über Mobile Health-Dienste (**Grünbuch**) zusammengefasst.[28] Das Grünbuch initiiert eine öffentliche Konsultation zu Themen im Zusammenhang mit mHealth. Ziel des Grünbuchs ist es, Handlungsfelder für Massnahmen zu definieren, die es ermöglichen sollen, den beteiligten Akteuren eine Orientierungshilfe über den anwendbaren Rechtsrahmen auf EU-Ebene zu geben.[29]

28 EUROPÄISCHE KOMMISSION, Grünbuch über Mobile-Health-Dienste („mHealth"), 10. April 2014, COM(2014) 219 final.

29 Grünbuch (Fn. 28), 4.

42 Das Grünbuch wird sekundiert durch ein Arbeitsdokument der Kommissionsdienststellen zum Rechtsrahmen von *„Lifestyle"*- und *„Wellbeing"*-Apps, das sich den auf mHealth Apps anwendbaren Regularien des EU-Rechts widmet.[30] Konkret werden darin die Themen Produktsicherheits- und –leistungsanforderungen, Datenschutz sowie Konsumentenschutz beleuchtet.

43 Aus dem Grünbuch sind bislang drei konkrete Projekte hervorgegangen:

– Zum einen hat die EU-Kommission die Erarbeitung eines Datenschutzkodex für mHealth Apps (**EU Code of Conduct**) angestossen.[31] Der Entwurf des EU Code of Conduct ist gegenwärtig bei der Artikel 29-Arbeitsgruppe[32] in der Vernehmlassung und wird in einem gesonderten Kapitel dieses Gutachtens behandelt.[33]

– Weiter ist das Thema der Datenqualität und Zuverlässigkeit von mHealth Apps aufgegriffen worden. Die EU-Kommission rief im Februar 2016 eine Arbeitsgruppe ins Leben, welche den Auftrag hatte, einen Richtlinienkatalog für die Beurteilung der Qualität von mHealth Apps zu erarbeiten. In einem sehr breit abgestützten Prozess konnten sich die Beteiligten allerdings einzig darauf einigen, welche Kriterien für die Erarbeitung solcher Richtlinien relevant sein sollten, wobei das Verständnis über die Bedeutung dieser Kriterien bisweilen offenbar weit auseinanderdriftete: [34]

  (i) Datenschutz;

  (ii) Transparenz;

  (iii) Zuverlässigkeit;

  (iv) Validität;[35]

30 Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps, 10. April 2014, SWD(2014) 135 final.

31 Draft Code of Conduct on privacy for mobile health applications, 7. Juni 2016.

32 Die Artikel 29-Arbeitsgruppe ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes. Die Gruppe wurde durch Artikel 29 der Richtlinie 95/46/EG (**Datenschutz-RL**) vom 24. Oktober 1995 eingesetzt.

33 Vgl. nachstehend, Rz. 85 ff.

34 Vgl. Report of the Working Group on mHealth Assessment Guidelines, Februar 2016 – März 2017, 8.

35 Unter Validität versteht man die inhaltliche Übereinstimmung einer empirischen Messung mit einem logischen Messkonzept (Wikipedia).

(v) Interoperabilität.

– Schliesslich hat die EU-Kommission eine Arbeitsgruppe ins Leben gerufen, welche sich mit der Erarbeitung eines Qualitätsstandards für die Entwicklung von mHealth Apps beschäftigt. Ausgangspunkt bietet dabei ein einschlägiger, von der *British Standards Institution* erlassener *Code of Practice*.[36]

3.1.1.2. Neue Medizinprodukteverordnungen

44 Von einschneidender Bedeutung für mHealth in der EU werden überdies die neuen Medizinprodukteverordnungen[37] sein, welche die bestehenden Medizinprodukterichtlinien[38] per 26. Mai 2020[39] bzw. 2022[40] ablösen. Von dieser Entwicklung ist die Schweiz direkt betroffen. Die Regulierung der Medizinprodukte in der Schweiz ist nämlich mit der gemeineuropäischen Regulierung weitgehend harmonisiert. Die Anforderungen der gemeineuropäischen Medizinprodukterichtlinien sind in Art. 45 ff. des Heilmittelgesetzes[41] sowie der Medizinprodukteverordnung[42] umgesetzt. Grundlage für den Nachvollzug der europäischen Regulierung durch die Schweiz bildet das sektorielle Abkommen mit der europäischen Gemeinschaft über die gegenseitige Anerkennung von Konformitätsbewertungen[43]. Medizinprodukte, welche die grundlegenden Anforderungen nach dem Recht eines Mitgliedstaats der EU oder der Schweiz erfüllen, sind daher auf dem gesamten Gebiet der EU verkehrsfähig. Um diesen Status weiterhin aufrechterhalten zu können, wird die Schweiz das Heilmittel-

36 PAS 277:2015, Health and Wellness Apps – Quality Criteria Across the Lifecycle – Code of Practice.

37 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (**MDR**); Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (**IVDR**).

38 Richtlinie 93/42/EWG des Rates vom 14. Juni 19931 über Medizinprodukte; Richtlinie 98/79/EG des Europäischen Parlamentes und des Rates vom 27. Oktober 19982 über In-vitro-Diagnostika; Richtlinie 90/385/EWG des Rates vom 20. Juni 19903 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über aktive implantierbare medizinische Geräte.

39 Art. 123(2) MDR.

40 Art. 113(2) IVDR.

41 Bundesgesetz über Arzneimittel und Medizinprodukte (Heilmittelgesetz, **HMG**) vom 15. Dezember 2000 (SR 930.11).

42 Medizinprodukteverordnung (**MepV**) vom 17. Oktober 2001 (SR 012.213).

43 Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die gegenseitige Anerkennung von Konformitätsbewertungen (Mutual Recognition Agreement, **MRA**) vom 21. Juli 1999 (SR 0.946.526.81).

gesetz und die MepV revidieren müssen. Die MDR führt zu erhöhten Konformitätsanforderungen für zahlreiche Software-Produkte und damit auch mHealth Apps, soweit diese als Medizinprodukte zu qualifizieren sind. Namentlich werden ab Mai 2020 mHealth Apps, die dazu bestimmt sind, Informationen zu liefern, die zu Entscheidungen für diagnostische oder therapeutische Zwecke herangezogen werden, oder für die Kontrolle von physiologischen Prozessen bestimmt sind, neu mindestens in Risikoklasse IIa (anstelle wie bisher in Risikoklasse I) eingeordnet.[44] Diese bedeutet u.a., dass die Konformität solcher mHealth Apps mit den grundlegenden Anforderungen für Medizinprodukte inskünftig durch eine externe Konformitätsbewertungsstelle bescheinigt werden muss,[45] während bislang eine Selbstdeklaration genügte. Dies dürfte zu einem merklichen Qualitätsschub führen, aber auf längere Sicht auch die Zahl der auf dem Markt erhältlichen mHealth Apps reduzieren sowie die Technologie weniger erschwinglich machen.

3.1.1.3. mHealth-Initiativen in den Mitgliedstaaten

45 Kaum mehr zu überblicken sind schliesslich die mHealth-Initiativen auf einzelstaatlicher Ebene. Eine diesbezügliche Übersicht liefert ein Bericht der mHealth Untergruppe des gemeineuropäischen eHealth-Aktionsplans 2012–2020.[46] Dort stechen mehrere nationale Projekte hervor, die sich mit der Anbindung von mHealth Apps an elektronische Patientendossiers befassen.[47] In datenschutzrechtlicher Hinsicht herrscht in den EU-Mitgliedstaaten die Auffassung vor, dass der bestehende Regulierungsrahmen genüge und eine spezifische mHealth-Regulierung nicht erforderlich sei.[48]

46 Von den nationalen Projekten sticht eine Initiative des *National Health Service* (**NHS**) in Grossbritannien besonders hervor.[49] Diese hält eine Auswahl von mHealth Apps vor, die den Ansprüchen eines umfassenden Kriterienkatalogs genügen. Anbieter können ihre Produkte anmelden und müssen eine ausführliche Selbsteinschätzung abgeben. Diese bezieht sich nicht nur auf datenschutz- und datensicherheitsrechtliche Aspekte, sondern behandelt auch die Wirksamkeit, Zweckmässigkeit und klinische Qualität der mHealth Apps. Sind die Kriterien nach der Selbsteinschätzung erfüllt, erfolgt eine vertiefte Prüfung durch

44 MDR, Anhang VIII, Regel 11.
45 Vgl. MDR, Anhang X.
46 mHealth sub-group Report on national mHealth strategies, 25. Oktober 2016.
47 Vgl. mHealth sub-group Report (Fn. 46), 11.
48 Vgl. mHealth sub-group Report (Fn. 46), 19 f.
49 Vgl. https://apps.beta.nhs.uk/#! (zuletzt besucht am 1. Dezember 2017).

Experten des NHS. mHealth Apps, welche den Test bestanden haben, erhalten das Gütesiegel „NHS Approved“. Ende 2017 hatte eine mHealth App den Test bestanden, drei weitere befanden sich in der Evaluation.

47 Eine weiterführende Auseinandersetzung mit den diversen, nur kurz gestreiften Regulierungsinitiativen würde den Rahmen dieses Gutachtens sprengen; dessen Schwerpunkt liegt auf dem Gebiet des Datenschutzes.

3.1.2. Datenschutzrechtlicher Rahmen

3.1.2.1. Geltendes Recht

48 Auf internationaler Ebene gilt für sämtliche Mitgliedsstaaten der EU zunächst das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen STE 108) vom 28. Januar 1981 (**ERK 108**), das auch für die Schweiz am 1. Februar 1998 in Kraft getreten ist.[50] Das Ziel der ERK 108 besteht vor allem darin, im privaten und öffentlichen Sektor ein Minimum an Persönlichkeitsschutz bei der Bearbeitung von Personendaten sicherzustellen und eine gewisse Harmonisierung des Schutzsystems zu erreichen. Sie sieht dazu u.a. folgende Grundsätze für die Bearbeitung von Personendaten vor, die auch im europäischen und im schweizerischen Recht zu beachten sind:[51]

– Treu und Glauben;

– Rechtmässigkeit;

– Zweckbindung;

– Verhältnismässigkeit und Speicherbegrenzung;

– Richtigkeit;

– Datensicherheit;

50 SR 0.235.1.

51 Ähnliche Grundsätze finden sich in den OECD-Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten (www.oecd.org/internet/ieconomy/15589558.pdf, zuletzt besucht am 9. Oktober 2017). Praktisch relevant sind diese Grundsätze allerdings kaum, weshalb sie hier nicht näher dargestellt werden.

– Betroffenenrechte, zum Beispiel das Recht auf Auskunft, Berichtigung und Löschung;

– Rechtsschutz betroffener Personen.

49 Innerhalb der EU gilt sodann die Richtlinie 95/46/EG[52] (**Datenschutz-RL**), die noch bis zum 24. Mai 2018 den wesentlichen Rechtsrahmen der EU bildet. Sie ist am 13. Dezember 1995 in Kraft getreten und war, als Richtlinie, von den Mitgliedstaaten im innerstaatlichen Recht umzusetzen.[53] Mit der Datenschutz-RL wurde u.a. die erwähnte ERK 108 umgesetzt. Die Datenschutz-RL gilt nur für Daten natürlicher Personen und beruht nach Art. 7 auf dem Grundsatz des „Verbots mit Erlaubnisvorbehalt". Die Bearbeitung von Personendaten ist danach verboten, sofern sie sich nicht auf einen Rechtfertigungsgrund wie beispielsweise eine Einwilligung oder die Erfüllung einer gesetzlichen Pflicht stützen lässt, was in der Praxis dazu führt, dass jeweils zunächst eine Bearbeitungsgrundlage zu identifizieren ist. Im schweizerischen Recht gilt im Privatsektor dagegen der Grundsatz der Erlaubnis mit Verbotsvorbehalt. Datenbearbeitungen sind danach erlaubt, solange die Grundsätze des DSG nicht verletzt werden (Art. 12 Abs. 1 DSG).[54]

50 Im Telekommunikationsbereich wird die Datenschutz-RL sodann durch die Richtlinie 2002/58/EG (**ePrivacy-RL**) ergänzt.[55] Die ePrivacy-RL ist am 31. Juli 2002 in Kraft getreten und verpflichtet die Mitgliedstaaten, spezifische Regelungen zum Datenschutz in der Telekommunikation zu erlassen, z.B. über das Mithören von Telefongesprächen und das Abfangen von E-Mails. Sie war bis am 31. Oktober 2003 in innerstaatliches Recht umzusetzen.[56] 2009 wurde die ePrivacy-RL sodann durch die Richtlinie 2009/136/EG[57] ergänzt (**Cookie-Richtlinie**),

52 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.

53 Deutschland etwa hat die Datenschutz-RL durch eine Änderung insb. des Bundesdatenschutzgesetzes umgesetzt. Die Änderung ist am 23. Mai 2001 in Kraft getreten.

54 Vgl. auch nachstehend, Rz. 122 ff.

55 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.

56 In Deutschland wurde sie allerdings erst verspätet und nach einem Vertragsverletzungsverfahren durch eine im Jahr 2004 in Kraft getretene Änderung des Telekommunikationsgesetzes (TKG) umgesetzt.

57 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

die für das Setzen von Cookies[58] eine ausdrückliche Einwilligung verlangt. Die Cookie-Richtlinie wurde in der EU nur uneinheitlich umgesetzt.[59]

51 Die Artikel-29-Arbeitsgruppe[60] hat sich verschiedentlich zur Bedeutung des Europäischen Datenschutzrechts im Bereich eHealth und mHealth geäussert.[61]

3.1.2.2. Revisionen

52 Sämtliche der im vorangehenden Abschnitt erwähnten Bestimmungen befinden sich zurzeit in Revision. Von Bedeutung ist insbesondere die Datenschutz-Grundverordnung (**DSGVO**)[62], die auf den 25. Mai 2018 die Datenschutz-RL ablöst. Gleichzeitig wird auch die ERK 108 revidiert. Da sich die ERK 108 nicht an Private, sondern an die Signatarstaaten richtet und in der EU durch die DSGVO umgesetzt wird, ist ihre Revision allerdings nicht von direkter praktischer Bedeutung, weshalb wir im Folgenden nicht weiter auf sie eingehen.

53 Die DSGVO ist eine Verordnung, nicht eine Richtlinie, und gilt als solche unmittelbar in allen Mitgliedstaaten der EU. Damit soll eine grössere Einheitlichkeit des europäischen Datenschutzes erreicht und der freie Datenverkehr erleichtert werden. Um dennoch auf die Bedürfnisse einzelner Mitgliedstaaten einzugehen, erlaubt die DSGVO allerdings durch sog. „Öffnungsklauseln" zahlreiche Konkretisierungen und Abweichungen durch das nationale Recht, so dass sie bereits als „Richtlinie im Gewand einer Verordnung" bezeichnet wurde. Bei der Anwendung der DSGVO ist deshalb stets auch das entsprechende nationale Recht im Auge zu behalten. Zahlreiche Umsetzungsgesetze wurden bereits verabschiedet oder vorgeschlagen, so etwa in Deutschland[63]. In Island, Liechtenstein und Norwegen wird die DSGVO gestützt auf das EWR-Abkommen[64] gel-

58 Ein Cookie ist eine Textdatei auf einem Computer. Sie enthält typischerweise Daten über besuchte Webseiten, die der Webbrowser beim Surfen im Internet speichert (Wikipedia).

59 In Deutschland unterblieb eine Umsetzung, weil das (in Fn. 56 erwähnte) TKG als ausreichend angesehen wurde.

60 Vgl. Fn. 32.

61 ARTIKEL-29-ARBEITSGRUPPE, Arbeitspapier über die Verarbeitung von Gesundheitsdaten in elektronischen Patientenakten vom 15. Februar 2007 (Working Document Nr. 131 on the processing of personal data relating to health in electronic health records (EHR)); ARTIKEL-29-ARBEITSGRUPPE, Stellungnahme zu Apps auf Smart Devices vom 27. Februar 2013 (Opinion 02/2013 on apps on smart devices).

62 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

63 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (DSAnpUG-EU).

64 Abkommen über den Europäischen Wirtschaftsraum (EWR).

ten. Heute ist allerdings noch nicht bekannt, auf welches Datum die Übernahme erfolgt.[65]

54 Die DSGVO erweitert u.a. bestehende Betroffenenrechte und sieht neue Rechte vor, z.B. das Recht auf Datenportabilität (Art. 20 DSGVO). Dramatisch verschärft wurde der Sanktionsrahmen: Je nach Art des Verstosses sind Bussen bis zu EUR 20 Mio. oder 4% des weltweiten Konzernumsatzes möglich, wobei der höhere Betrag gilt (Art. 83 DSGVO). Die DSGVO ist unter bestimmten Bedingungen auch auf Unternehmen ohne eine Niederlassung in der EU anwendbar.[66]

55 Die ePrivacy-Richtlinie soll sodann durch eine Verordnung (**ePrivacy-Verordnung**) abgelöst werden. Zurzeit liegen ein entsprechender Vorschlag der Europäischen Kommission[67] sowie Änderungs- und Ergänzungsvorschläge des Rats[68] vor, den auch das EU-Parlament mit zusätzlichen Verschärfungen bereits verabschiedet hat. Nach dem Willen der Kommission soll die ePrivacy-Verordnung gleichzeitig mit der DSGVO am 25. Mai 2018 in Kraft treten. Die e-Privacy-Verordnung gilt für elektronische Kommunikationsdienste (bspw. bei der Verarbeitung elektronischer Kommunikationsdaten), allerdings nur für öffentliche Dienste, und regelt u.a. das Fernmeldegeheimnis, die elektronische Kommunikation zwischen Menschen, Unternehmen und Maschinen (M2M[69]; beides unabhängig davon, ob dabei Personendaten bearbeitet werden), die Verwendung von Cookies und anderen Tracking-Technologien, die Werbung per Telefon oder per E-Mail und weitere Punkte. Sie ist damit für digitale Dienste wie mHealth Apps von hoher Relevanz. Mit Bezug auf elektronische, personenbezogene Kommunikationsdaten wäre sie *lex specialis* zur DSGVO. Die DSGVO bliebe ausserhalb der spezifischen Regelungen der ePrivacy-Verordnung anwendbar.

65 Zurzeit werden Stellungnahmen der EWR-Länder eingeholt (der aktuelle Stand ist hier abrufbar: www.efta.int/eea-lex/32016R0679). Der nächste Verfahrensschritt ist der Entwurf eines Übernahmebeschlusses durch den „Gemischten Ausschuss". Nach Inkrafttreten des Übernahmebeschlusses wird dieser in das EWR-Abkommen aufgenommen, und die DSGVO wird in Liechtenstein unmittelbare Anwendung finden.

66 Vgl. für Einzelheiten nachstehend, Rz. 59 f.

67 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation).

68 Dokument 2017/0003 (COD) vom 8. September 2017.

69 Machine-to-machine.

56 Ebenfalls revidiert wird zurzeit die Schengen-Richtlinie.[70] Sie richtet sich an die Verarbeitung von Personendaten durch Behörden im weiteren Zusammenhang mit der Strafvollstreckung. Auf sie wird vorliegend nicht weiter eingegangen.

3.1.2.3. Die DSGVO insbesondere

57 Die DSGVO will den Schutz natürlicher Personen verbessern. Dazu dient die Ausgestaltung als Verordnung, nicht als Richtlinie, vor allem aber die Stärkung der Betroffenenrechte, die erhöhte Transparenz, die höheren Sanktionsdrohungen und generell die Stärkung der Governance und Compliance. So werden Datenverarbeiter[71] dazu verpflichtet, Grundsätze wie *„Privacy by Design"* (Datenschutz durch Technik) und *„Privacy by Default"* (datenschutzfreundliche Voreinstellungen) einzuhalten und bei hohen Datenschutzrisiken eine Datenschutz-Folgenabschätzung durchzuführen. Bei Verletzungen der Datensicherheit ist zudem eine Meldung an die zuständige Aufsichtsbehörde und gegebenenfalls auch an die betroffenen Personen vorgesehen.

58 Ebenfalls der Compliance dient der *„Accountability"*-Grundsatz. Danach liegt es am Datenverarbeiter, die Einhaltung der DSGVO nachzuweisen (Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO). Im Ergebnis erfolgt dadurch eine Beweislastumkehr. Demselben Ziel dient die Pflicht, Datenverarbeitungen zu dokumentieren (Art. 30 DSGVO).

59 Die DSGVO ist primär auf Datenverarbeiter mit einer Niederlassung in der EU anwendbar (Art. 3 Abs. 1 DSGVO). Sie findet jedoch auch auf Datenverarbeiter ausserhalb der EU Anwendung, z.B. auf Unternehmen mit Sitz in der Schweiz, sofern und soweit diese Personendaten bearbeiten im Zusammenhang

- mit gezielten Vertragsangeboten an Personen in der EU (Art. 3 Abs. 2 lit. a DSGVO); oder
- der Beobachtung des Verhaltens von Personen in der EU, insbesondere durch Online-Tracking (Art. 3 Abs. 2 lit b DSGVO).

---

70 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

71 Die DSGVO spricht von der „Verarbeitung" von Personendaten, das schweizerische Recht von der „Bearbeitung". Beide Begriffe werden hier synonym verwendet; in der Sache meinen sie jeweils jeden Umgang mit Personendaten.

Anbieter von mHealth Apps, deren Produkte in den EU-Mitgliedstaaten über die einschlägigen App Stores vertrieben werden, haben daher die DSGVO zu beachten.[72]

60 Im Zusammenhang mit mHealth sind die folgenden Bestimmungen der DSGVO besonders hervorzuheben:

(a) „Personenbezogenen Daten" i.S.v. Art. 4 Nr. 1 DSGVO (vgl. dazu Erwägungsgrund 35):

61 Als Personendaten gelten weiterhin Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Dazu gehören im Bereich mHealth auch etwa Sensordaten bspw. aus einer App oder einem Fitness-Messgerät, soweit diese Daten einer einzelnen Person zugeordnet werden können. Über eine mHealth App übermittelte Fotografien zu Diagnosezwecken oder in Fällen der Telekonsultation über Videochat ist auch eine direkte Bestimmung der Identität der betroffenen Person denkbar. Gerade letzteres Szenario ist aber für das ePD nicht relevant.

62 Eine gewisse Unsicherheit besteht bei der Frage, ob zumindest im Online-Bereich auch Angaben als personenbezogen gelten, die sich auf eine von allen anderen Personen unterscheidbare, aber nicht namentlich bekannte Person beziehen („Singularisierung" statt „Identifizierung").[73] Die Legaldefinition in Art. 4 Nr. 1 DSGVO scheint darauf hinzudeuten. Nach unserer Auffassung ist die Singularisierung indessen nur ein Indiz für den Personenbezug, ersetzt diesen aber nicht.[74] Infolgedessen sollten Angaben wie MAC-Adressen (Gerätekennnummern), die Advertising ID oder IP-Adressen nicht als personenbezogen gelten, soweit der Personenbezug nicht durch Verknüpfung mit weiteren Angaben hergestellt werden kann.

(b) „Gesundheitsdaten" i.S.v. Art. 4 Nr. 15 DSGVO (vgl. dazu Erwägungsgrund 35 der DSGVO):

63 Gesundheitsdaten sind vereinfacht gesagt personenbezogene Daten, die Informationen über den Gesundheitszustand einer Person enthalten. Dazu gehören beispielsweise Angaben über physische oder psychische Krankheiten, aber auch

72 Vgl. BÜHLMANN LUKAS/REINLE MICHAEL, Extraterritoriale Wirkung der DSGVO, *in:* digma 2017, 8–12, 9.
73 Vgl. hierzu ROSENTHAL DAVID, Personendaten ohne Identifizierbarkeit? *in:* digma 2017, 198–203.
74 Ebenso ROSENTHAL, digma 2017 (Fn. 73), 202.

über deren Abwesenheit, Behandlung und Heilung. Erfasst sind ferner Angaben, die mittelbar Aufschlüsse über den Gesundheits- bzw. Krankheitszustand einer Person zulassen, beispielsweise Herzfrequenzmessungen. Keine Gesundheitsdaten sind dagegen sog. „Lifestyle"-Daten wie z.B. die Anzahl täglich zurückgelegter Schritte, sofern sie nicht etwa zu diagnostischen Zwecken verwendet werden.

64 Gesundheitsdaten gelten als sensible Daten (Art. 9 Abs. 1 DSGVO). Solche Daten dürfen nur verarbeitet werden, wenn die strengen Anforderungen von Art. 9 Abs. 2 DSGVO erfüllt sind. Das betrifft insbesondere (aber nicht ausschliesslich) folgende Fälle:

– die betroffene Person hat in die Bearbeitung ausdrücklich eingewilligt (Art. 9 Abs. 2 lit. a DSGVO). Die Einwilligung ist dabei nur wirksam, wenn sie den Anforderungen von Art. 4 Nr. 11, Art. 7 und Art. 9 Abs. 2 lit. a DSGVO genügt, d.h. freiwillig, für den bestimmten Fall, nach angemessener Information (u.a. über den besonderen Schutzbedarf der Daten[75]) und unmissverständlich abgegeben wird, in ausdrücklicher (d.h. nicht konkludenter) Weise erfolgt und nicht widerrufen wurde (Art. 7 Abs. 3 DSGVO). Schriftliche Einwilligungserklärungen müssen überdies in klarer und einfacher Sprache gehalten sein und dürfen nicht mit anderen vertraglichen Bestimmungen wie z.B. AGB vermischt werden (Art. 7 Abs. 2 DSGVO);

– die Verarbeitung ist erforderlich, um das Arbeits- oder Sozialversicherungsrecht der EU bzw. eines Mitgliedstaats (nicht aber der Schweiz; vgl. Art. 6 Abs. 3 DSGVO) einhalten zu können (lit. b);

– die Bearbeitung ist zum Schutz lebenswichtiger Interessen erforderlich und eine Einwilligung kann nicht eingeholt werden (lit. c);

– die Verarbeitung ist zur Durchsetzung oder Abwehr von Rechtsansprüchen erforderlich (lit. f);

– die Verarbeitung ist erforderlich u.a. für die Prävention, die Diagnose und die Behandlung (lit. h), wobei strittig ist, ob dieser Erlaubnistatbestand aufgrund von Art. 9 Abs. 3 DSGVO nur die Bearbeitung durch Be-

75 WEICHERT THILO, *in:* KÜHLING/BUCHNER (Hrsg.), Datenschutz-Grundverordnung, München 2017, Art. 9 N 47.

rufsgeheimnisträger erlaubt.[76] Sollte dies zu bejahen sein, stellt sich die weitere – offene – Frage, ob auch ein im aussereuropäischen Recht begründetes Berufsgeheimnis wie etwa das Geheimnis nach Art. 321 StGB genügt;

– die Verarbeitung ist auf der Grundlage des EU-Rechts oder des Rechts eines Mitgliedstaats (nicht aber der Schweiz) erforderlich für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (lit. j).

(c) Privacy by Design (Art. 25 Abs. 1 DSGVO):

65 Der Grundsatz von *„Privacy by Design"* oder „Datenschutz durch Technikgestaltung" verpflichtet den für die Verarbeitung Verantwortlichen (aber nicht den blossen Auftragsverarbeiter), nicht erst bei der konkreten Datenverarbeitung, sondern bereits bei der Planung (der „Festlegung der Mittel", wie sich Art. 25 Abs. 1 DSGVO ausdrückt) die erforderlichen Massnahmen vorzusehen, um die Datenschutzgrundsätze einzuhalten.

66 Dieser Grundsatz nimmt andere Grundsätze auf wie insb. jenen der Datensicherheit (Art. 24 und 32 DSGVO)[77] oder Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO). Er verlangt keine anderen oder zusätzlichen Massnahmen, sondern präzisiert nur, dass diese Massnahmen (wie etwa eine Pseudonymisierung, wenn die Kenntnis der betroffenen Person für die Verarbeitung nicht erforderlich ist) rechtzeitig und nicht erst bei Aufnahme der Verarbeitung zu treffen sind. Art. 25 Abs. 1 DSGVO enthält eine Reihe von Kriterien für die Bestimmung der zu treffenden Massnahmen. Sie entsprechen den in Art. 32 DSGVO (Sicherheit der Verarbeitung) genannten Kriterien.

67 Hersteller von Systemen (beispielsweise Softwarehersteller von Apps) fallen nicht unter diese Bestimmung, sofern sie nicht gleichzeitig Datenverarbeiter sind. Das ist insofern konsequent, als der sachliche Anwendungsbereich der DSGVO auf Datenverarbeitungen beschränkt ist. Die DSGVO kann somit Personen, die keine Personendaten verarbeiten, nicht in die Pflicht nehmen. Diese Beschränkung führt dazu, dass der Schutz der DSGVO auf Datenverarbeiter beschränkt ist, auch wenn sie *diese* Personen durchaus im Vorfeld eigentlicher Da-

76 Dagegen (d.h. Bearbeitung auch ohne Berufsgeheimnis erlaubt): Kühling/Buchner-WEICHERT (Fn. 75), Art. 9 N 138; mit Hinweisen auf andere Ansichten; dafür (d.h. Bearbeitung ohne Berufsgeheimnis verboten) SCHULZ SEBASTIAN, *in:* GOLA (Hrsg.), Datenschutz-Grundverordnung, München 2017, Art. 9 N 30.

77 Nachstehend, Rz. 74.

tenverarbeitungen in die Pflicht nimmt (nicht nur durch die Grundsätze von *Privacy by Design* und *Privacy by Default*, sondern auch durch die Pflicht, unter Umständen eine Datenschutz-Folgenabschätzung durchzuführen[78]). Hersteller werden in Erwägungsgrund 78 aber (unverbindlich) aufgerufen, ihre Produkte datenschutzfreundlich auszugestalten. Die Zertifizierung von Produkten nach Art. 40 ff. DSGVO bietet dazu immerhin ein – wenn auch kaum genutztes – Mittel.

(d) Privacy by Default (Art. 25 Abs. 2 DSGVO):

68 Der *„Privacy by Default"*-Grundsatz ist mit dem *Privacy by Design*-Grundsatz verwandt und sieht im Wesentlichen vor, dass ein Produkt oder Dienst bereits beim ersten Aufruf durch den Nutzer die datenschutzfreundlichsten Einstellungen aufzuweisen hat. Das betrifft beispielsweise Adressbücher oder andere Datenquellen, auf die ein Social Media-Dienst nicht ohne aktive Handlung des Nutzers zugreifen darf. Darüber hinaus sollten durch den Nutzer konfigurierbare Einstellungen die datenschutzfreundlichste Voreinstellung als Standard anbieten, um sog „Nudging", d.h. das subtile Lenken der betroffenen Person auf die vom Anbieter gewünschte Einstellung, zu vermeiden.[79]

69 Auch dieser Grundsatz gilt nicht für Hersteller von Apps oder anderen Systemen; Hersteller wie etwa Softwarehersteller werden aber wie erwähnt (oben zu *„Privacy by Design"*) ermuntert, entsprechende Vorkehrungen zu treffen.

(e) Datenschutz-Folgenabschätzung (Art. 35 f. DSGVO):

70 Die Datenschutz-Folgenabschätzung ist ein aus schweizerischer Sicht neues Instrument der datenschutzrechtlichen Risikoprävention. Nach Art. 35 Abs. 1 DSGVO ist der Verantwortliche verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen, wenn eine bestimmte Datenverarbeitung voraussichtlich zu hohen Risiken für die betroffenen Personen führt.

71 Aus Art. 35 Abs. 1 DSGVO und Erwägungsgrund 91 ergibt sich, dass das „hohe Risiko" nach Art, Umfang, Umständen und Zweck der Verarbeitung zu bestimmen ist und insbesondere in folgenden Fällen vorliegen kann:[80]

78 Dazu nachstehend, Rz. 70 ff.

79 Zum sog. "Nudging" im Kontext des ePD ausführlich WIDMER, digma 2017 (Fn. 26), 164 m.w.H.

80 Weitere Hinweise ergeben sich aus dem Entwurf des Arbeitspapiers Nr. 248 der Art. 29-Datenschutzgruppe, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679, 4. April 2017.

– Entscheidungen auf Basis eines Profilings[81] oder einer Verarbeitung sensibler Daten;

– systematische Verarbeitung von Personendaten in grossem Umfang, wobei die Verarbeitung Patientendaten nicht in diesem Sinne als „umfangreich“ gilt, wenn sie durch einen einzelnen Arzt erfolgt.

72 Art. 35 Abs. 2 und 7 DSGVO enthalten Vorgaben für Durchführung und den Inhalt der Datenschutz-Folgenabschätzung. Im Kern geht es um eine systematische Risikobewertung unter Berücksichtigung risikomindernder Massnahmen.

73 Ergibt die Datenschutz-Folgenabschätzung, dass trotz der geplanten Massnahmen ein hohes Restrisiko verbleibt, ist die Aufsichtsbehörde nach Art. 36 DSGVO zu konsultieren. Die Mitgliedstaaten können im öffentlichen Bereich weitere Konsultationspflichten vorsehen, beispielsweise im Gesundheitsbereich (Art. 36 Abs. 5 DSGVO).

(f) Datensicherheit (Art. 32 DSGVO)

74 Art. 32 Abs. 1 DSGVO hält fest, dass Verarbeiter dazu verpflichtet sind, mit technischen und organisatorischen Massnahmen ein dem Risiko angemessenes Schutzniveau sicherzustellen. Beispielhaft werden die folgenden Massnahmen genannt:

– Pseudonymisierung und Verschlüsselung personenbezogener Daten;

– Befähigung zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Datenverarbeitungssysteme und –dienste;

– Rasche Widerherstellung der Datenverfügbarkeit bei einem technischen Zwischenfall;

– Verfahren zur regelmässigen Wirksamkeitsüberprüfung.

75 Die Zweckmässigkeit der Datensicherheitsmassnahmen ist stets an den Risiken zu messen, die mit einer spezifischen Datenverarbeitung verbunden sind. Welche Gefahren dabei zu beachten sind, ergibt sich insb. aus Erwägungsgrund 85 (bspw. die Gefahr eines physischen, materiellen oder immateriellen Schadens,

81 Vgl. dazu nachstehend, Rz. 84.

die unbefugte Verarbeitung von Daten, die Einschränkung von Betroffenenrechten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, Rufschädigung, etc.). Es gibt somit keinen allgemeingültigen Sicherheitsstandard, die Regulierung ist vielmehr prinzipienbasiert. Die getroffenen Massnahmen sind nach dem bereits erwähnten „*Accountability*"-Grundsatz sodann zu dokumentieren.[82]

76 Wie bei den Grundsätzen von *Privacy by Default*[83] und *Privacy by Design*[84] setzt die DSGVO nicht bei der Programmierung von Systemen wie bspw. mHealth Apps an, sondern erst bei der Verarbeitung der personenbezogenen Daten.

(g) Meldepflichten bei Datenschutzverletzungen (Art. 33 f. DSGVO):

77 Im Fall einer Verletzung des Datenschutzes im Sinne von Art. 4 Nr. 12 DSGVO (z.B. ein unbefugter Zugriff auf Nutzerkonten) ist der Verantwortliche verpflichtet, die Verletzung der zuständigen Aufsichtsbehörde zu melden, sofern sich Risiken für die betroffenen Personen nicht ausschliessen lassen. Die Meldung muss unverzüglich erfolgen; erfolgt sie später als 72 Stunden nach Bekanntwerden der Verletzung, ist der Verantwortliche dafür begründungspflichtig. Art. 33 Abs. 3-4 DSGVO enthalten Vorgaben über den Inhalt und die Art und Weise der Meldung. Nach Abs. 5 müssen Datenschutzverletzungen sodann dokumentiert werden.

78 Nach Art. 34 DSGVO ist der Verantwortliche zusätzlich verpflichtet, die betroffenen Personen zu benachrichtigen, wenn die Datenschutzverletzung voraussichtlich zu einem hohen Risiko führt oder wenn die Aufsichtsbehörde eine Benachrichtigung anordnet. Die Benachrichtigung kann unterbleiben, wenn das Risiko durch Sicherheitsvorkehrungen ausreichend reduziert wurde oder wenn die Meldung mit einem unverhältnismässigen Aufwand verbunden wäre; im letzteren Fall muss der Verantwortliche allerdings Ersatzmassnahmen treffen, beispielsweise eine öffentliche Bekanntmachung.

(h) Verhaltensregeln und Zertifizierung (Art. 40 ff. DSGVO):

79 Die DSGVO sieht in Art. 40 vor, dass Verbände und andere Vereinigungen Verhaltensregeln ausarbeiten und genehmigen lassen können, um bestimmte Re-

82 Vorstehend, Rz. 58.
83 Vorstehend, Rz. 68.
84 Vorstehend, Rn. 66.

geln der DSGVO zu konkretisieren, etwa die Anforderungen an die Transparenz, die Verarbeitung zu berechtigten Interessen, die Art und Weise der Erhebung personenbezogener Daten, die Pseudonymisierung oder Datensicherheitsmassnahmen (Art. 40 Abs. 2 DSGVO). Art. 41 DSGVO enthält Bestimmungen über die Überwachung der genehmigten Verhaltensregeln.

80 Art. 42 DSGVO sieht sodann vor, dass Verantwortliche und Auftragsverarbeiter Datenverarbeitungen zertifizieren lassen können, sofern eine Zertifizierungsstelle nach Art. 43 DSGVO oder die zuständige Aufsichtsbehörde die Zertifizierung genehmigt haben. Die Zertifizierung kann sich bspw. auf Produkte oder Dienstleistungen beziehen, auch etwa auf eine mHealth App und die damit zusammenhängende Datenverarbeitung, und erleichtert den Nachweis, dass datenschutzrechtliche Pflichten (etwa im Bereich Privacy by Design, Privacy by Default oder Datensicherheit) eingehalten werden.

81 Die freiwillige Einhaltung von Verhaltensregeln oder Zertifizierungen durch Verantwortliche oder Auftragsverarbeiter in einem Drittstaat kann ferner die Datenübermittlung erleichtern (Art. 40 Abs. 3 und 42 Abs. 3 DSGVO).

(i) Grenzüberschreitende Datenbekanntgabe (Art. 45 ff. DSGVO)

82 Die Übermittlung von personenbezogenen Daten an ein Drittland ist nur zulässig, wenn eine der folgenden Bedingungen erfüllt ist:

– Das Drittland verfügt selbst über ein angemessenes Datenschutzniveau, was auf alle oder nur auf bestimmte Datenempfänger des betreffenden Staats zutreffen kann (letzteres bei besonderen Regelungen wie etwa des „*EU-US Privacy Shield*“, der nur für zertifizierte Unternehmen wirksam ist[85]). Diese Feststellung hat durch einen Angemessenheitsbeschluss der Kommission zu erfolgen (Art. 45 DSGVO);

– der Datenschutz ist durch wirksame und durchsetzbare vertragliche Garantien sichergestellt (Art. 46 DSGVO);

– es liegen von der zuständigen Aufsichtsbehörde genehmigte verbindliche Datenschutzvorschriften innerhalb einer Unternehmensgruppe vor (Art. 47 DSGVO);

85 Dazu näher nachstehend, Rz. 133.

– ein Ausnahmetatbestand von Art. 49 DSGVO ist erfüllt. Unter diesem Titel darf die Übermittlung bspw. auf Grundlage einer wirksamen Einwilligung erfolgen, für den Abschluss oder die Erfüllung von Verträgen in bestimmten Konstellationen, zum Schutz eines öffentlichen Interesses (wobei nur Interessen in Frage kommen, die auf dem Recht der EU oder eines Mitgliedstaats beruhen) oder lebenswichtiger Interessen einer natürlichen Person, oder zur Durchsetzung oder Abwehr von Rechtsansprüchen.

83 Gerade im Umfeld von mHealth Apps sind grenzüberschreitende Datenflüsse gang und gäbe, denn die Verarbeitung der Daten erfolgt in der Regel nicht lokal auf dem mobilen Endgerät, sondern in externen Rechenzentren, die häufig auch in den USA liegen.[86]

(j) Weitere Bestimmungen (Auswahl):

84 Eine Reihe weiterer Bestimmungen sind mit Blick auf den Gesundheitsbereich relevant, bspw. die folgenden:

– Ein Recht auf Löschung (Art. 17 DSGVO) besteht ausnahmsweise nicht, sofern die Verarbeitung von Personendaten aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich ist (Art. 22 Abs. 3 lit. c DSGVO);

– "Profiling" i.S.v. Art. 4 Nr. 4 DSGVO ist eine automatische Bewertung persönlicher Aspekte zur Analyse oder Prognose, etwa mit Bezug auf die Gesundheit einer Person. An die Durchführung eines Profiling allein knüpft die DSGVO allerdings keine direkten Folgen. Erst wenn das Profiling dazu dient, automatisierte Einzelentscheidungen i.S.v. Art. 22 DSGVO zu treffen, entstehen entsprechende Pflichten, bspw. die Informationspflicht nach Art. 14 Abs. 2 DSGVO, die Auskunftspflicht nach Art. 15 DSGVO und die Rechte nach Art. 22 DSGVO.

– Bei automatisierten Einzelfallentscheidungen durch ein Profiling hat der Verantwortliche darauf zu achten, das Risiko einer Diskriminierung beispielsweise aufgrund genetischer Anlagen oder des Gesundheitszustands durch geeignete mathematische oder statistische Verfahren zu verhindern (Erwägungsgrund 71).

86 Vgl. ISLER, digma 2013 (Fn. 10), 110.

3.1.3. "Code of Conduct on Mobile Health Applications"

85 Im April 2015 hat das „Global Digital Health Network"[87] im Auftrag der europäischen Kommission mit der Ausarbeitung eines Verhaltenskodizes für Gesundheits-Apps begonnen („Code of Conduct on Mobile Health Applications" – **EU Code of Conduct**).[88] Die Kommission will den Entwicklern von mHealth Apps damit eine Anleitung zur Einhaltung des europäischen Datenschutzrechts in die Hand geben und das Vertrauen der Konsumenten in solche Apps stärken. Der EU Code of Conduct besteht im Kern aus Fragen (z.B. „Wie ist die Einwilligung der Nutzer einzuholen?", „Welche Grundsätze habe ich vor allem einzuhalten?", „Welche Informationen muss ich den Nutzern zur Verfügung stellen?" etc.) und entsprechenden Erläuterungen.

86 Am 7. Juni 2016 legte die Kommission den Entwurf des EU Code of Conduct der Artikel-29-Arbeitsgruppe zur Stellungnahme vor. Findet der Code die Zustimmung dieses Gremiums, soll er danach zur Anwendung gelangen.

87 Der EU Code of Conduct soll unter Geltung der Datenschutz Grundverordnung die Bedeutung genehmigter Verhaltensregeln (Art. 40 f. DSGVO)[89] haben. Die Einhaltung des Codes soll dementsprechend freiwillig sein. Entwickler, die sich zur Einhaltung verpflichten, können aber in einem öffentlichen Register verzeichnet werden, sofern sie neben der Selbstverpflichtung auf den Code eine Datenschutz-Folgenabschätzung durchgeführt haben. Die Verwaltung des Codes einschliesslich der Prüfung der Datenschutz-Folgenabschätzung obliegt dabei einem Aufsichtsorgan (dem *„Monitoring Body"*), das nach Art. 40 und 41 DSGVO zur Überwachung des Codes akkreditiert werden soll. Das Aufsichtsorgan wird durch das sogenannte *„Governance Board"* bestimmt, das seinerseits aus der Generalversammlung (*„General Assembly"*) der Stakeholder – etwa Konsumentenschutzorganisationen, Vertretern der Zivilgesellschaft, Patientenorganisationen, IT-Organisationen etc. – gewählt wird. Es ist also vorgesehen, zur Überprüfung der Einhaltung des Kodex einen eindrücklichen Apparat einzurichten.

87 „mHealth Working Group"

88 Der Europäische Datenschutzbeauftragte (EDSB) hat in seinem Jahresbericht 2016 zudem – ohne Bezug auf den Code of Conduct – angekündigt, im Lauf des Jahres 2017 eine Auszeichnung für datenschutzfreundliche mobile Gesundheits-Apps auszuloben, um Entwickler zum Schutz der Privatsphäre zu ermutigen.

89 Siehe dazu vorstehend, Rz. 79 ff.

3.2. Rechtslage in den USA

3.2.1. Regulierung von mHealth in den USA

88 In den USA wird die Entwicklung und Integration von mHealth sowohl von der Wissenschaft als auch von verschiedenen staatlichen Behörden, u.a. die Food and Drug Administration (**FDA**), gefördert.[90] So erkennt die FDA die Vorteile von mHealth sowohl für den einzelnen Patienten als auch zum Wohle des Kollektivs, d.h. im Sinne eines Public Health-Ansatzes: Die Reduktion der Gesundheitskosten, die Erleichterung des Zugangs zur Medizin, die Reduktion von Ineffizienzen im Gesundheitswesen, die Qualitätssteigerung im Gesundheitswesen und die bessere Ausrichtung der Medizin auf die Besonderheiten des einzelnen Patienten (sog. personalisierte Medizin).[91]

89 Im Gegensatz zur Schweiz setzt sich die USA schon seit geraumer Zeit mit den rechtlichen Aspekten von mHealth und deren Regulierung auseinander. Diese sollen im Nachfolgenden dargelegt werden. Schwerpunkt der nachfolgenden Ausführungen bildet die Regulierung in Bezug auf den Datenschutz. Ausgeklammert bleiben namentlich medizinprodukterechtliche Fragen.[92]

90 Datenschutz wird in den USA diametral anders verstanden als in Europa. Im Vordergrund steht nicht der Schutz der Persönlichkeit der Datensubjekte, sondern die freie Verwertbarkeit der Daten als Wirtschaftsgut. Dennoch ist Datenschutz in den USA nicht inexistent, im Gegenteil: Verstösse gegen Datenschutzerklärungen von Privaten (*Privacy Policies*) oder grobe Verletzungen der Datensicherheit werden in den USA rigoroser durchgesetzt als in Europa.[93] Kompetent ist diesbezüglich die *Federal Trade Commission* **(FTC)**[94], welche unter Federführung des *US Department of Commerce* auch die Zertifizierungen

---

90 Vgl. z.B. CORTEZ NG/COHEN IG/KESSELHEIM AS, FDA regulation of mobile health technologies, *in:* N Engl J Med 2014, 24;371(4):372-379; NASLUND JA./MARSCH LA./MCHUGO GJ/BARTELS SJ, Emerging mHealth and eHealth interventions for serious mental illness: a review of the literature, *in:* J Ment Health 2015;24(5):321-332.

91 Webseite der FDA, https://www.fda.gov/medicaldevices/digitalhealth/ (zuletzt besucht am 9. Oktober 2017).

92 Vgl. diesbezüglich FDA, Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff, 9. Februar 2015.

93 Vgl. DETERMANN LOTHAR, *in:* PASSADELIS/ROSENTHAL/THÜR Datenschutzrecht, Basel 2015, Rn. 33.6.; vgl. in Bezug auf mobile Applikationen FEDERAL TRADE COMMISSION, Mobile Privacy Disclosures Report, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf (zuletzt besucht am 9. Oktober 2017).

94 Die FTC ist kraft FTC Act, 15 U.S.C. § 45(a) und (n) mit der Kompetenz ausgerüstet, unlauteres Geschäftsgebaren zu ahnden, wenn dadurch Konsumenten erheblich und unverhältnismässig geschädigt werden. Datenschutz- und Datensicherheitsverletzungen können derartiges unlauteres Geschäftsgebaren darstellen; vgl. BEARDWOOD JOHN/BOWMAN MARK, Cybersecurity Evolves? Understanding What Constitutes Reasonable and Appropriate Privacy Safeguards Post-Ashly Madison, *in:* CRi 2016, 166172, 167.

von US-amerikanischen Unternehmen unter dem *Privacy Shield* zum sicheren Datenverkehr zwischen der EU bzw. der Schweiz und den USA überwacht.[95] Nach der Praxis der FTC müssen Datensicherheitsmassnahmen *„reasonable and appropriate"* sein, wobei als Gradmesser für die erforderlichen Sicherheitsmassnahmen die Menge und die Art der Daten, die Grösse und Komplexität des Geschäfts sowie die Kosten von Verbesserungen der Datensicherheit dienen.[96]

91 Sodann gibt es eine Fülle sektor- oder ereignisspezifischer Datenschutzvorschriften auf Bundes- wie auch auf einzelstaatlicher Ebene.[97] Spezifische Vorschriften in Bezug auf den Datenschutz und die Informationssicherheit im Gesundheitswesen finden sich auf Bundesebene primär in der Health Insurance Portability and Accountability Act (**HIPAA**)[98] sowie der Health Information Technology for Economic and Clinical Health Act (**HITECH**)[99]:[100]

– HIPAA wurde 1996 erlassen und verpflichtet Gesundheitsorganisationen im Rahmen der *„Privacy Rule"*, *„Security Rule"* und *„Breach Notification Rule"* sicherzustellen, dass Produkte sicher und sensible Patienten- bzw. Gesundheitsdaten genügend geschützt sind.[101] HIPAA war mit einem der Hauptziele in Kraft gesetzt worden, die Abhängigkeit der Spitäler von Systemlieferanten durch proprietäre Datenformate zu lindern. Die dadurch bewirkte Datenmobilität machte einen flankierenden Datenschutz notwendig, der sich inzwischen zu einem der Hauptaspekte des Gesetzes gemausert hat.[102]

– Die HITECH Act, die im Jahre 2009 erlassen wurde, ergänzt die HIPAA und hat zum Ziel, eine effektivere und effizientere Gesundheitsversor-

95 Vgl. EDÖB, Swiss-US Privacy Shield: neuer Rahmen für Datenübermittlungen in die USA, 11. Januar 2017, https://www.edoeb.admin.ch/datenschutz/00626/00753/01405/01406/index.html?lang=de (zuletzt besucht am 9. Oktober 2017).

96 *LabMD, Inc. v. Federal Trade Commission,* 11th Circuit, 29. September 2016, 10-11.

97 Vgl. DETERMANN (Fn. 93), Rn. 33.1.

98 42 U.S.C. § 300gg, 29 U.S.C § 1181 ff.

99 42 U.S.C. § 1320d ff.

100 Vgl. DETERMANN (Fn. 93), Rn. 33.12 ff.

101 Webseite des U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; THE OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY (HEALTHIT.GOV), Guide to Privacy and Security of Electronic Health Information, April 2015, 10 ff., https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf (zuletzt besucht am 9. Oktober 2017); DILIP CHATULINGATH, Regulations and Compliance for Enterprise Mobile Health Applications, Juli 2012, 2, http://www.rapidvaluesolutions.com/whitepapers/regulations-and-compliance-for-enterprise-mobile-health-apps.html (zuletzt besucht am 9. Oktober 2017).

102 ISLER, digma 2013 (Fn. 10), 115.

gung durch den vermehrten Einsatz von Technologie, z.B. durch die Implementierung eines elektronischen Gesundheitsdatensystems, und den damit einhergehenden sinkenden Gesundheitskosten zu ermöglichen. Auch die HITECH beinhaltet Vorschriften zur *„Privacy“*, *„Security“* und *„Breach Notification“*.[103]

92 Daneben hat auch die FDA zusammen mit dem *Office of the National Coordinator for Health IT* (**ONC**) und der *Federal Communication Commission* (**FCC**) basierend auf der Food and Drug Administration Safety Innovation Act (**FDASIA**) Empfehlungen zur Sicherstellung einer sichereren und innovativen Health IT erlassen.[104]

93 Die Vorschriften von HIPAA waren ursprünglich ausschliesslich von sog. *„Covered Entities“* zu berücksichtigen. Diese Gruppe umfasst Gesundheitsdienstleister (z.B. Ärzte, Spitäler, Alters- und Pflegeheime, Apotheken, Krankenversicherungen oder Abrechnungsstellen für medizinische Leistungen).[105] Die Zudiener, welche die für die Datenverarbeitung notwendige Technologie zur Verfügung stellen, waren HIPAA ursprünglich nicht unterstellt. Die Lücke wurde mit HITECH geschlossen, indem das Gesetz die Kategorie der *„Business Associates“* einführte.[106] Von den Business Associates umfasst sind nicht-medizinische natürliche und juristische Personen, die Dienstleistungen erbringen für die Covered Entities *und* dabei Zugang zu Gesundheitsdaten erhalten. Hierzu gehören etwa IT-Fachkräfte (unter der Voraussetzung, dass diese Zugang zur PHI haben), jedoch beispielsweise nicht Reinigungskräfte, denen der Zugang zu solchen Daten fehlt.[107]

94 Anbieter von mHealth Apps können als Business Associates qualifiziert werden, wenn das Personal von Covered Entities auf die Betriebsumgebung der App zugreift, um Patientendaten zu bearbeiten, oder die App dazu benützt wird, um Gesundheitsinformationen aus einer Covered Entity dem Patienten mitzuteilen. Auf der anderen Seite fällt eine mHealth App dann nicht unter HIPAA und HITECH, wenn die von der App generierten Daten einer Covered Entity übermit-

103 CHATULINGATH (Fn. 101), 2.

104 FDASIA Health IT Report, Proposed Strategy and Recommendations for a Risk-Based Framework, April 2014, https://www.fda.gov/downloads/aboutfda/centersoffices/officeofmedicalproductsandtobacco/cdrh/cdrhreports/ucm391521.pdf (zuletzt besucht am 9. Oktober 2017).

105 Webseite der FDA, https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html, mit weiteren Ausführungen (zuletzt besucht am 9. Oktober 2017); DETERMANN (Fn. 93), Rn. 33.12.

106 ISLER, digma 2013 (Fn. 10), 115.

107 THE OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY, Guide to Privacy and Security of Electronic Health Information, April 2015, S. 11 f.

telt und dort auf einer abgegrenzten Betriebsumgebung weiterbearbeitet werden.[108] In einem solchen Anwendungsszenario gelten die im Rahmen der mHealth App bearbeiteten Daten nicht als *„protected health information"*[109] im Sinne der HIPAA-Gesetzgebung. Auf den Kontext des ePD bezogen, wären also nur diejenigen Apps reguliert, die Dokumente aus dem ePD abrufen könnten, nicht aber diejenigen, welche lediglich dazu dienen, über eine Schnittstelle zum ePD Daten dort abzulegen.

95 Die FTC betont allerdings in ihrer Aufsichtstätigkeit, dass zumindest die Informationssicherheitspflichten von HIPAA und HITECH auch in Bezug auf andere Sektoren als das Gesundheitswesen als sinnvoller Massstab für sachgerechte Sicherheitsmassnahmen analog herangezogen werden können.[110]

3.2.2. Informationssicherheitspflichten

3.2.2.1. Informationssicherheitspflichten unter HIPAA

96 Von Bedeutung für die vorliegende Fragestellung ist Titel II der HIPAA[111]. In diesem Abschnitt wird u.a. geregelt, wie nicht-anonymisierte Gesundheitsdaten (sog. *„protected health information"*, **PHI**) geschützt und wie Zuwiderhandlungen sanktioniert werden sollen. Von der PHI sind Informationen umfasst, die im Zusammenhang stehen mit

- dem früheren, gegenwärtigen und zukünftigen Gesundheitszustand des Individuums;
- der medizinischen Behandlung des Individuums;
- der vergangenen, gegenwärtigen und zukünftigen Leistungsdeckungen bzw. Kostenübernahme für die medizinischen Behandlungen.[112]

Demgegenüber sind anonymisierte Gesundheitsdaten (sog. *„de-identified health information"*) von der Privacy Rule ausgeschlossen.[113]

---

108 GREENE ADAM H., When HIPAA Applies to Mobile Applications, *in:* mobihealthnews, 16. Juni 2011, http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications/ (zuletzt besucht am 9. Oktober 2017).

109 Vgl. zur Legaldefinition der *"protected health information"* nachstehend, Rz. 96.

110 *LabMD, Inc. v. Federal Trade Commission* (Fn. 96), 12-14.

111 *"Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Form".*

112 HEALTHIT.GOV (Fn. 107), 11.

97 Die ***HIPAA Privacy Rule*** schreibt die Minimalvorschriften vor in Bezug auf den Datenschutz, die Nutzung sowie die Offenlegung von PHI auf Bundesebene. Sie beinhaltet Pflichten der Covered Entity sowie Rechte des einzelnen Patienten. Demnach darf eine Covered Entity u.a. keine PHI (auch nicht, wenn dies der Beschleunigung einer Therapie dienen würde) ohne die ausdrückliche schriftliche Einwilligung des Patienten offenlegen.[114] Bei der Offenlegung hat die Covered Entity beispielsweise stets darauf zu achten, dass sie nur so viele Daten weitergibt, wie dies zur Erfüllung des Zwecks notwendig ist (*„minimum necessary standard"*).[115] Ebenso darf die Covered Entity die PHI nur verkaufen, wenn sie hierfür die explizite Einwilligung des Patienten hat. Hingegen ist es der Covered Entity erlaubt, die PHI für ihre eigenen medizinischen Dienstleistungen ohne Einwilligung des Patienten zu benutzen.[116] Des Weiteren gibt die Privacy Rule dem einzelnen Patienten das Recht, falsche Angaben der PHI gegenüber der Covered Entity geltend zu machen und Letztere dazu zu verpflichten, entsprechende Korrekturen vorzunehmen.[117] Zudem müssen Covered Entities die Patienten über den Zugriff und die Benutzung ihrer PHIs informieren und dies dokumentieren.[118]

98 Die ***HIPAA Security Rule*** ergänzt die Privacy Rule. Während die Privacy Rule sowohl die physische als auch die elektronische PHI umfasst, regelt die Security Rule spezifisch die elektronischen Gesundheitsdaten (*„Electronic Protected Health Information*", **ePHI**).[119] Als prominentes Beispiel hierfür dient das elektronische Patientendossier („*Electronic Health Records*"). Auf vier Ebenen soll die Sicherheit bzw. der Datenschutz gewährleistet werden, um beispielsweise Cyber-Attacken oder den Datenverlust zu vermeiden:

– Administrative Schutzmassnahmen („*Administrative Safeguards*"): Mit diesen Massnahmen sollen Datenschutzverletzungen vermieden bzw. frühzeitig entdeckt werden. So müssen die Covered Entities zum Beispiel eine verantwortliche Person bestimmen, welche für die Durchführung einer Risikoanalyse und die Entwicklung sowie Implementierung aller in der Security Rule verankerten Sicherheitsvorschriften verantwortlich ist.

---

113 HEALTHIT.GOV (Fn. 107), 20; vgl. für mehr Informationen zur Privacy Rule etwa die Webseite des HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (zuletzt besucht am 9. Oktober 2017).
114 45 CFR 164.524(a)(1)(ii).
115 45 CFR 164.502(b).
116 HEALTHIT.GOV (Fn. 107), 15.
117 45 CFR 164.526.
118 45 CFR 164.528.
119 HEALTHIT.GOV (Fn. 107), 26.

Des Weiteren dürfen ePHI nur solchen Arbeitnehmern zugänglich gemacht werden, welche diese Daten für die Ausübung ihres Berufs benötigen. Covered Entities müssen auch gewährleisten, dass ihre Arbeitnehmer regelmässige Schulungen besuchen, um die Funktionen der Schutzmassnahmen zu erlernen.[120]

– Physische Schutzmassnahmen („*Physical Safeguards*"): Mit diesen Vorschriften soll der unbefugte Zugang zu sensiblen Gesundheitsdaten verhindert werden. Angesetzt wird bereits bei Vorschriften zu den Räumlichkeiten, der Beschilderung und der Begleitung von Besuchern bzw. Unbefugten. Des Weiteren sollen Bildschirme nicht im Blickfeld von Unbefugten liegen.[121]

– Schutzmassnahmen betreffend die Organisation („*Organizational Standards*"): Die Covered Entities sind verpflichtet, Vereinbarungen mit den Business Associates zu treffen, damit auch diese im Einklang mit den Vorschriften für den Schutz der ePHI handeln.[122]

– Richtlinien und Ablauf („*Policies and Procedures*"): Damit soll sichergestellt werden, dass die Covered Entities angemessene Richtlinien erarbeiten, um intern die Privacy Rule einhalten zu können. So muss eine Covered Entity z.B. regelmässig ihre Dokumentation und eigenen Organisationsrichtlinien überprüfen und anpassen.[123]

99 Das ONC umschreibt in seinem Leitfaden[124] am Beispiel des elektronischen Patientendossiers exemplarisch, wie die Security Rule in Bezug auf die ePHI erfüllt werden kann. Diese Ausführungen können auch im mHealth-Kontext angewendet werden. Zusammengefasst weist es auf folgende Sicherheitsmassnahmen hin (nicht abschliessend):

– Die meisten Softwareprodukte für das elektronische Patientendossier verfügen bereits über integrierte Sicherheitsmassnahmen, jedoch ist es notwendig, dass die Covered Entities stets die Upgrades vollziehen, um die aktuell besten Sicherheitsmassnahmen zu erfüllen;

120 HealthIT.gov (Fn. 107), 27 m.w.H.
121 HealthIT.gov (Fn. 107), 27 m.w.H.
122 HealthIT.gov (Fn. 107), 27 m.w.H.
123 HealthIT.gov (Fn. 107), 27 m.w.H. Vgl. für mehr Informationen zur Security Rule etwa die Webseite des HHS, https://www.hhs.gov/hipaa/for-professionals/security/index.html (zuletzt besucht am 9. Oktober 2017).
124 Vgl. vorstehend, Rz. 92.

– Verschlüsselung des ursprünglichen medizinischen Textes zu einem codierten Text;

– Erstellung unverwechselbarer Benutzer-IDs und sicherer Passwörter sowie regelmässige Änderung der letzteren;

– Auto time-out;

– Verschlüsselung von E-Mails;

– Installation von Firewalls;

– Benutzung eines Anti-Viren-Programms.[125]

100 Das ONC konkretisiert diese allgemeinen Hinweise anhand eines beispielhaften, sieben Schritte umfassenden Vorgehens für die Implementierung eines sicheren Management Prozesses („*Sample Seven-Step Approach for Implementing a Security Management Process*“).[126]

101 Einen in der Praxis wichtigen, aber unverbindlichen Sicherheitsstandard gibt sodann das National Institute of Standards and Technology (**NIST**) heraus.[127] Die FTC schreibt diesem Standard, ähnlich wie der HIPAA Security Rule,[128] generell Vorbildcharakter zu.[129] So hat sich auch ausserhalb des Anwendungsbereichs HIPAA ein relativ konkreter Standard dazu entwickelt, welche Art von Sicherheitsmassnahmen bei der Bearbeitung von sensitiven Personendaten erforderlich sind:

– Ein Datensicherheitskonzept, welches eine Dokumentation der Sicherheitsvorschriften und -massnahmen, einen Risikomanagement-Prozess und eine angemessene Ausbildung des Personals umfasst;

– Zugriffsschutz durch Zwei-Faktoren-Authentifizierung und strenge Passwortregeln;

125 Vgl. zum Ganzen HEALTHIT.GOV (Fn. 107), 27 ff.
126 HEALTHIT.GOV (Fn. 107), 35 ff.
127 NIST, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Oktober 2008, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf (zuletzt besucht am 9. Oktober 2017).
128 Vgl. vorstehend, Rz. 95.
129 *LabMD, Inc. v. Federal Trade Commission* (Fn. 96), 12-14.

– umfangreiches Monitoring der Netzwerksicherheit sowie des Verhaltens der Nutzer;

– Limitierung der administrativen Zugriffsrechte.[130]

102 Die ***Breach Notification Rule*** schliesslich verpflichtet Covered Entities, die betroffenen Patienten sowie das Aufsichtsorgan *US Health and Human Services* über allfällige Verletzungen der Sicherheitspflichten von PHI aufzuklären. Dies hat unmittelbar und spätestens bis 60 Tage nach Entdeckung der Verletzung zu erfolgen. Eine Ausnahme bezüglich der Frist gilt, wenn weniger als 500 Patienten betroffen sind. In diesen Fällen reicht es, die US Health and Human Services einmal jährlich über den Vorfall zu unterrichten.[131]

3.2.2.2. Informationssicherheitspflichten unter HITECH

103 Die HITECH Act ist Teil der American Recovery and Reinvestment Act von 2009 und beinhaltet Regelungen in Bezug auf die „*health care information technology*" im Allgemeinen sowie wichtige Grundsätze in Bezug auf den Einsatz des elektronischen Patientendossiers. Das Regelwerk hat zum Ziel, das gesamte Potential des elektronischen Patientendossiers auszuschöpfen, um von seinen Vorteilen umfassend profitieren zu können.[132]

104 Von vorliegendem Interesse sind die in der HITECH Act verankerten Voraussetzungen in Bezug auf die Sicherheits- („*Privacy Provisions*") und Datenschutzmassnahmen („*Security Provisions*") für die PHI und ePHI (z.B. das elektronische Patientendossier oder mHealth Apps). Unter Subtitle D Part 1 der HITECH Act werden die Privacy und Security Rules sowie die Breach Notification Rule der HIPAA verschärft und auf Business Associates von Covered Entities erweitert.[133] So sind beispielsweise die Bussen bei Zuwiderhandlungen gegen die Sicherheits- und Datenschutzmassnahmen höher als in der HIPAA. Entsprechend wird

130 BEARDWOOD/BOWMAN (Fn. 94), 172.

131 Vgl. zum Ganzen 45 CFR 164.400-414; CENTER FOR MEDICARE & MEDICAID (CMS), HIPAA Basics for Providers, Privacy, Security and Breach Notification Rules, August 2016, https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf (zuletzt besucht am 9. Oktober 2017). Für mehr Informationen siehe Webseite des HHS, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (zuletzt besucht am 9. Oktober 2017).

132 BLUMENTHAL D., Launching HITECH, *in:* N Engl J Med 2010;362:382-385.

133 ED JONES, ARRA's HITECH Privacy Provisions Apply HIPAA Security Rule to Business Associates, 20. Februar 2009, https://www.hipaa.com/arras-hitech-privacy-provisions-apply-hipaa-security-rule-to-business-associates/ (zuletzt besucht am 9. Oktober 2017).

die HITECH Act in den USA auch „*HIPAA on Steroids*“ oder „*HIPAA II*“ genannt.[134]

3.2.2.3. FDASIA Health IT Report

105 Die FDA hat zusammen mit dem ONC sowie der FCC Strategien und Empfehlungen entwickelt, welche die Health IT fördern und gleichzeitig auch vor Missbrauch schützen sollen („*Proposed Strategy and Recommendations for a Risk-Based Framework*“). Diese sollen die involvierten Akteure bei der Umsetzung der dargelegten gesetzlichen Vorschriften unterstützen.

106 Die Strategien und Empfehlungen setzen auf vier Ebenen an:

- Förderung des Gebrauchs von Qualitätsmanagementprinzipien;
- Identifizierung, Entwicklung and Adaptierung von Standards und Best Practices;
- Einsatz von Konformitätsbewertungsinstrumenten;
- Entwicklung einer kontinuierlichen Lern- und Verbesserungsumgebung.[135]

3.3. Gesamtwürdigung

107 Auf EU-Ebene ist mHealth stark in den Blickpunkt geraten. (Zu) viele Initiativen auf gemeineuropäischer und mitgliedstaatlicher Ebene nehmen sich dem Thema an. Der datenschutzrechtliche Rahmen wird durch die DSGVO vorgegeben, ein detailreiches Regelwerk, welches den Akteuren gerade auch im Gesundheitsbereich nur noch wenig Spielraum lässt. Es wird sich zeigen, ob und wie die strengen Datenschutzstandards der DSGVO im globalen Kontext effektiv durchgesetzt werden können. Gerade im Bereich mHealth ist zu erwarten, dass die Anbieter dem Datenschutz inskünftig mehr Beachtung schenken werden. Datenschutz-Compliance dürfte zum Wettbewerbsvorteil werden, gerade auch, wenn der EU Code of Conduct zu einem Instrument wird, an dem für seriöse

134 https://www.healthcareinfosecurity.com/essential-guide-to-hitech-act-a-2053 (zuletzt besucht am 9. Oktober 2017).

135 Vgl. zum Ganzen und für weitere Ausführungen FDASIA Health IT Report (Fn. 104).

Anbieter kein Weg mehr vorbeiführt. Schliesslich wird auch die neu aufgelegte Medizinprodukteregulierung dafür sorgen, dass zumindest diejenigen mHealth Apps, welche für medizinische Zwecke eingesetzt werden, die Qualitätsstandards verbessern. Diejenigen Anbieter, welche die damit zusammenhängenden hohen Kosten auf sich nehmen, werden ein erhebliches Interesse daran haben, dass die schwarzen Schafe mit der Zeit aus dem Markt verdrängt werden. Diese Entwicklung dürfte aber auch das Angebot verteuern.

108 In den USA setzen sich die staatlichen Behörden seit über 20 Jahren mit der konkreten Regelung von mHealth auseinander. Die Vorschriften für den Datenschutz und die Informationssicherheit der mHealth-Daten bzw. PHI werden auf Bundesebene nicht in einem allgemeinen Gesetz, sondern von Spezialgesetzen spezifisch geregelt, nämlich von der HIPAA und der HITECH Act. Die Vorschriften sind zahlreich und beinhalten nicht nur allgemeine Grundsätze, sondern auch sehr konkrete (Vorgehens-)Pflichten für Covered Entities und Business Associates. Daneben umschreiben Erläuterungsberichte sowie Strategien und Empfehlungen der erlassenden Behörden konkreter die gesetzlichen Rahmenbedingungen und dienen als Hilfestellung für die Umsetzung der Vorschriften im Einzelfall. Diese erinnern bisweilen stark an die im europäischen Raum geläufigen TOM („technische und organisatorische Massnahmen"), weisen aber eine geringere Abstraktionshöhe auf. Damit folgen die USA im Gesundheitsbereich über weite Strecken einem regelbasierten Regulierungsansatz, der die Sicherstellung der Compliance durch konkrete Handlungsvorgaben und mittels Abarbeitung von Checklisten ermöglicht. „*HIPAA Compliance*" ist daher für mHealth Apps ein starkes Gütesiegel.

109 Man muss allerdings auch sehen, dass nur ein kleiner Teil der auf dem Markt erhältlichen mHealth Apps von HIPAA und HITECH direkt betroffen ist. Dies bedeutet jedoch nicht, dass sich diese Produkte in einem datenschutzrechtlichen Vakuum bewegen. Die Vorgaben der FTC, welche Datensicherheitsvorkehrungen bei der Bearbeitung von sensitiven Personendaten als *„reasonable and appropriate"* zu betrachten sind, haben inzwischen sehr konkrete Formen angenommen.

4. Anpassungsbedarf für das schweizerische Recht

4.1. Schweizerischer Datenschutzrahmen für mHealth Apps

4.1.1. Anwendbares Recht

110 Die bisherigen Vorarbeiten an der Schnittstelle zwischen mHealth und ePD gehen davon aus, dass Anbieter von mHealth Apps (**Anbieter**) in der Regel jenem Datenschutzrecht unterstehen, das an ihrem jeweiligen Firmensitz gilt, so dass es bei der Anbindung von mHealth Apps an das ePD zu Divergenzen bei den Datenschutzstandards kommen könne.[136] Diese Grundannahme ist bei näherem Hinsehen jedoch zu relativieren.

111 Die Anbieter sind im privatrechtlichen Bereich tätig. Die auf sie anwendbaren datenschutzrechtlichen Normen bestimmen sich deshalb primär nach dem Bundesgesetz über das Internationale Privatrecht (IPRG)[137], sofern die Zuständigkeit eines schweizerischen Gerichts gegeben ist.

112 Eine internationale Zuständigkeit in der Schweiz dürfte regelmässig gegeben sein, wenn eine betroffene Person mit Wohnsitz oder gewöhnlichem Aufenthalt in der Schweiz gegenüber einem Anbieter, der sich nicht an die datenschutzrechtlichen Vorgaben hält, eine Persönlichkeitsverletzung geltend macht. Persönlichkeitsverletzungen sind im Hinblick auf die Prüfung der gerichtlichen Zuständigkeit als unerlaubte Handlung zu qualifizieren. Die schädigende Handlung des mHealth Anbieters wirkt sich in der Schweiz aus, so dass an die gerichtliche Zuständigkeit am sog. Erfolgsort gemäss Art. 129 IPRG bzw. Art. 5 Nr. 3 LugÜ[138] angeknüpft werden kann.[139] Daran ändert auch die Vereinbarung einer fremden Zuständigkeit in den allgemeinen Geschäftsbedingungen (AGB) des Anbieters nichts, da im Verhältnis zu Konsumenten eine solche Gerichtsstandsklausel unwirksam sein dürfte (vgl. Art. 114 IPRG bzw. 17 LugÜ).[140]

136 Empfehlungen I (Fn. 9), 25 f.
137 SR 291.
138 Übereinkommen über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung vom Entscheidungen in Zivil- und Handelssachen (Lugano Übereinkommen, **LugÜ**), SR 0.275.12.
139 BÜHLMANN/REINLE (Fn. 72), 12 Fn. 19; PASSADELIS NICOLAS, *in:* PASSADELIS/ROSENTHAL/THÜR (Hrsg.), Datenschutzrecht, Basel 2015, Rn. 6.23.
140 Vgl. im Kontext von Social Media-Plattformen, STAFFELBACH OLIVER, *in:* STAFFELBACH/KELLER (Hrsg.), Social Media Recht für Unternehmen, Zürich 2015, Rn. 1.80. Dieser Schutz kann aber mittels Vereinbarung einer Schiedsklausel ausgehebelt werden, vgl. nachstehend, Rz. 188.

113 Liegt eine internationale Zuständigkeit in der Schweiz vor, kann die betroffene Person zwischen mehreren Rechtsordnungen wählen (Art. 139 Abs. 1 i.V.m. Art. 139 Abs. 3 IPRG):[141] Sie kann sich u.a. auf das Recht an ihrem eigenen Wohnsitz bzw. gewöhnlichen Aufenthaltsort wie auch am Erfolgsort berufen, sofern der Schädiger mit dem Erfolgseintritt in einem dieser Staaten rechnen musste. Anbieter, die ihre Produkte über die gängigen App Stores an Nutzer in der Schweiz vertreiben, müssen damit rechnen, dass ein Nutzer in der Schweiz in seiner Persönlichkeit verletzt werden kann.[142]

114 Damit gelten im Verhältnis zu den Anbietern zumindest die zivilrechtlichen Normen des schweizerischen Datenschutzrechts, auch wenn die Datenbearbeitung im Ausland stattfindet. Die Anwendung der öffentlich-rechtlichen Normen des Datenschutzgesetzes, allen voran die Prüfungszuständigkeit des EDÖB gemäss Art. 29 DSG, beurteilt sich demgegenüber nach dem Territorialitätsprinzip,[143] wobei die Erhebung von Personendaten oder der Eintritt einer Persönlichkeitsverletzung in der Schweiz als Anknüpfungspunkt auch dann genügen, wenn die Daten ins Ausland übermittelt und überwiegend dort bearbeitet werden.[144]

115 Der extraterritoriale Geltungsanspruch von Datenschutzvorschriften ist nichts Aussergewöhnliches. Die DSGVO will in bestimmten Fällen ebenfalls extraterritorial angewendet sein.[145] Somit müssen sich Anbieter mit Sitz ausserhalb der EU darauf einstellen, dass für sie die DSGVO gilt. Gleiches gilt für Anbieter, die den schweizerischen mHealth-Markt bearbeiten wollen.

4.1.2. Einbezug der DSG-Revision

116 Das schweizerische Datenschutzgesetz wird derzeit umfassend revidiert, um es in Einklang mit den Vorgaben der DSGVO zu bringen.[146] Auf eine ausführliche Darstellung des Entwurfs (**E-DSG**) wird hier verzichtet. Stattdessen wird bei den

---

141 Eine akzessorische Anknüpfung an das auf den Vertrag zwischen den beteiligten Parteien anwendbare Recht (Art 133 Abs. 3 IPRG) wird abgelehnt: ROSENTHAL DAVID, *in:* ROSENTHAL/JÖHRI, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 139 IPRG N 16 m.w.H. Der Vertrag zwischen dem Anbieter und dem Nutzer würde ohnehin in der Regel zwingend schweizerischem Recht unterstehen (Art. 120 IPRG).

142 ISLER, digma 2013 (Fn. 10), 112; PASSADELIS (Fn. 139), Rn. 6.77.

143 BÜHLMANN/REINLE (Fn. 72), 12.

144 BGE 138 II 346, E. 3.2 m.w.H. – *Google Street View*.

145 Vgl. vorstehend, Rz. 59.

146 Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Entwurf), BBl 2017 7193 ff.; Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941 ff.

weiteren Ausführungen an den relevanten Stellen die voraussichtliche revidierte Regelung behandelt.

4.1.3. Anwendbarkeit des Datenschutzgesetzes

4.1.3.1. Persönlicher Anwendungsbereich

117 Das Datenschutzgesetz gilt für das Bearbeiten von Personendaten durch private Personen und Bundesorgane (Art. 2 Abs. 1 DSG). Die Anbieter von mHealth Apps sind durchwegs im privatrechtlichen Rahmen tätig und nehmen keine staatlichen Aufgaben wahr. Die Bearbeitung von Personendaten im Zuge des Betriebs und der Nutzung von mHealth Apps unterliegt somit den Regeln des Datenschutzgesetzes. Dies gilt auch dann, wenn über mHealth Apps generierte Daten in das ePD eingestellt werden; die mHealth Apps werden dadurch nicht zum Bestandteil des ePD, sondern sind diesem vorgelagert. Ausnahmen können sich für Gesundheitsfachpersonen und weitere Leistungserbringer im Gesundheitswesen ergeben, die mHealth Apps im Rahmen ihrer dienstlichen Tätigkeit einsetzen. Je nach Rechtsgrundlage der ausgeübten Tätigkeit ist für sie der Datenschutz unter Umständen auch kantonal geregelt (z.B. bei öffentlichen Spitälern und ihrem Personal).[147]

4.1.3.2. Personenbezug

118 Das Datenschutzgesetz greift, wenn Personendaten bearbeitet werden (Art. 2 DSG). Personendaten sind gemäss Art. 3 lit. a DSG alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Im Fokus steht regelmässig die Frage, ob sich die bearbeiteten Daten auf eine *bestimmbare* Person beziehen. Bestimmbar ist eine Person dann, wenn aufgrund zusätzlicher Informationen auf deren Identität geschlossen werden kann. Für die Bestimmbarkeit genügt jedoch nicht jede theoretische Möglichkeit der Identifizierung. Vielmehr ist der Aufwand zu berücksichtigen, der eine Identifizierung einer Person aus dem vorhandenen Datenschatz mit sich bringt. Ist der Aufwand dafür derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet werden muss, dass ein Interessent diesen auf sich nehmen wird, liegt keine Bestimmbarkeit vor.[148] Die Bestimmbarkeit einer Person hängt m.a.W. von den konkreten Umständen ab, wobei die Möglichkeiten und Interessen sämtlicher

147 ISLER, digma 2013 (Fn. 10), 113 f.

148 Botschaft zum Bundesgesetz über den Datenschutz (DSG), BBl 1988 II 444 f., Ziff. 221.1.; vgl. auch Botschaft E-DSG (Fn. 146), BBl 2017, 7019.

Bearbeiter im Datenerhebungs- und Verarbeitungsprozess zu berücksichtigen sind.[149] Stellt für einen bestimmten Datenbearbeiter in der Verarbeitungskette eine Information ein Personendatum dar, gilt diese Qualifikation grundsätzlich auch für die ihm vorgelagerten Datenbearbeiter.[150]

119 Sofern eine mHealth App die Registrierung des Nutzers vorsieht, ist eine Verknüpfung der Daten mit der Identität des Nutzers ab diesem Zeitpunkt gegeben. Geschieht die Nutzung der mHealth App ohne Login oder aufgrund einer pseudonymen Verknüpfung, weisen die Daten im Kontext des ePD spätestens dann, wenn sie in das Repository des Nutzers gelangen, einen Personenbezug auf. Sämtliche über mHealth Apps erhobene Daten eines Patienten sind somit im vorliegenden Zusammenhang als Personendaten zu qualifizieren.

120 Das Kriterium der Bestimmbarkeit wird für das schweizerische Recht nach ähnlichen Massstäben beurteilt wie unter EU-Recht.[151] Es besteht somit Übereinstimmung mit dem europäischen Rechtsrahmen; ein Anpassungsbedarf ist nicht gegeben.

4.1.4. Bearbeitungsgrundsätze

121 Die über mHealth Apps generierten Personendaten sind im Kontext des ePD in aller Regel als Gesundheitsdaten zu qualifizieren. Dabei handelt es sich gemäss Art. 3 lit. c Ziff. 2 DSG um besonders schützenswerte Personendaten, an deren Bearbeitung qualifizierte Anforderungen gestellt werden. Höhere Anforderungen gelten auch, wenn sich die Gesamtheit der Datenpunkte zu einem Persönlichkeitsprofil gemäss Art. 3 lit. d DSG verdichten.[152]

122 Das schweizerische Recht kennt allerdings – im Gegensatz zum europäischen Recht[153] – selbst für Gesundheitsdaten kein Bearbeitungsverbot mit Erlaubnisvorbehalt, solange die Bearbeitung rechtmässig und in Übereinstimmung mit den Datenbearbeitungsgrundsätzen von Art. 4, 5 und 7 DSG erfolgt (vgl. Art. 12 Abs. 2 lit. a DSG). Es sind dies:

---

149 BGE 136 II 508, E. 3.2 – *Logistep;* ähnlich der Europäische Gerichtshof (EuGH), 19. Oktober 2016, Rs. C-582/14 – *Patrick Breyer ./. Bundesrepublik Deutschland*, E. 45 ff.

150 BGE 136 II 508, E. 3.5 – *Logistep*.

151 Vgl. vorstehend, Rz. 61 f.

152 Art. 4 E-DSG verzichtet auf die Legaldefinition des Persönlichkeitsprofils und führt stattdessen im Einklang mit der DSGVO den Begriff des „Profiling“ ein.

153 Vgl. vorstehend, Rz. 64.

- *Grundsatz der Transparenz:* Die Beschaffung der Personendaten und insbesondere der Zweck ihrer Bearbeitung muss für die betroffene Person erkennbar sein (Art. 4 Abs. 4 DSG);

- *Grundsatz der Zweckbindung:* Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG);

- *Grundsatz der Verhältnismässigkeit:* Die Bearbeitung der Personendaten muss verhältnismässig sein, d.h. darf nicht weiter gehen, als es der Zweck der Bearbeitung erforderlich macht (Art. 4 Abs. 2 DSG);

- *Grundsatz der Datenintegrität:* Der Bearbeiter hat sich über die Richtigkeit der Personendaten zu vergewissern und unvollständige oder unrichtige Personendaten zu vernichten (Art. 5 Abs. 1 DSG);

- *Grundsatz der Datensicherheit:* Personendaten sind durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen (Art. 7 Abs. 1 DSG).

123 Folglich ist nach schweizerischem Recht eine Einwilligung der betroffenen Person oder ein anderer Rechtfertigungsgrund für die Rechtmässigkeit der Bearbeitung von Gesundheitsdaten nicht erforderlich. Es genügt, wenn die betroffene Person über den Zweck der Bearbeitung informiert ist und der Bearbeiter sich an den Zweckbindungsgrundsatz sowie die weiteren Bearbeitungsgrundsätze hält. Davon ausgenommen ist die Bekanntgabe besonders schützenswerter Daten (u.a. Gesundheitsdaten) an Dritte; sie bedarf stets einer Rechtfertigung (Art. 12 Abs. 2 lit. c DSG). Liegt der Rechtfertigungsgrund in der Einwilligung der betroffenen Person (Art. 13 Abs. 1 DSG), so muss diese nach angemessener Information freiwillig und überdies ausdrücklich erfolgen (Art. 4 Abs. 5 DSG). Die betroffene Person hat sodann stets die Möglichkeit, einer Bearbeitung zu widersprechen (Art. 12 Abs. 2 lit. b DSG). Der E-DSG ändert an dieser Grundkonzeption nichts (vgl. Art. 5 Abs. 6 E-DSG, Art. 26 E-DSG).

124 Der im Vergleich zum EU-Recht liberale schweizerische Ansatz ist im Kontext der mHealth Apps sachgerecht. Geht die Datenbearbeitung über den primären Zweck der Bearbeitung gesundheitsbezogener Informationen im Rahmen der mHealth App-Funktionalität hinaus, ist sie entweder nicht mehr verhältnismässig oder – im Falle einer Bekanntgabe von Gesundheitsdaten an Dritte – ohnehin untersagt, weshalb für exorbitante Bearbeitungszwecke auch nach schweizerischem Recht stets eine Einwilligung der betroffenen Person oder ein

anderer Rechtfertigungsgrund erforderlich ist. Es besteht daher keine Veranlassung, die strengen Vorgaben von Art. 9 DSGVO[154] integral zu übernehmen.

4.1.5. Privacy by Design und Privacy by Default

125 Die Grundsätze von „*Privacy by Design*“ und „*Privacy by Default*“ sind im schweizerischen Datenschutzgesetz nicht positivrechtlich verankert und können höchstens aus dem allgemeinen Datenbearbeitungsgrundsatz der Verhältnismässigkeit (Art. 4 Abs. 2 DSG) abgeleitet werden. Das revidierte Datenschutzgesetz wird jedoch diese Lücke voraussichtlich schliessen (vgl. Art. 6 E-DSG).

4.1.6. Datensicherheit

126 Die Datensicherheit ist einer der wichtigsten, in der (juristischen) Praxis aber oft stiefmütterlich behandelten datenschutzrechtlichen Aspekte der mHealth Apps.

127 Datensicherheit ist ein relativer Begriff: Die organisatorischen und technischen Massnahmen zur Gewährleistung der Datensicherheit müssen den Risikofaktoren angemessen ausgestaltet sein, was dem Verantwortlichen weiten Ermessensspielraum lässt (Art. 7 Abs. 1 DSG). Art. 8 Abs. 1 VDSG konkretisiert den Bedeutungsgehalt der Datensicherheit dahingehend, dass sowohl die Vertraulichkeit, die Verfügbarkeit als auch die Integrität der Daten darunter zu subsumieren sind.[155] Der Bearbeiter ist insbesondere verpflichtet, die Systeme gegen folgende Risiken zu schützen:

- Unbefugte oder zufällige Vernichtung;
- zufälligen Verlust;
- technische Fehler;
- Fälschung, Diebstahl oder widerrechtliche Verwendung;
- unbefugtes Ändern, Kopieren, Zugreifung oder andere unbefugte Bearbeitungen.

[154] Vgl. vorstehend, Rz. 64.

[155] Weitere – aber nicht rechtsverbindliche – Konkretisierungen lassen sich etwa dem „Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes“ des EDÖB entnehmen.

128 Der Umfang der Datensicherheit geht also über den reinen Zugriffsschutz hinaus und umfasst auch Aspekte des Grundsatzes der Datenrichtigkeit (Art. 5 Abs. 1 DSG). Bei mHealth Apps kommt dem Grundsatz der Datenrichtigkeit, namentlich der Messgenauigkeit und Manipulationsresistenz, entscheidende Bedeutung zu, weil bei mangelnder Datenqualität auch die körperliche Integrität bedroht sein kann. Die Datensicherheit nimmt somit diesbezüglich auch eine flankierende Qualitätssicherungsfunktion wahr.

129 Das breite Anwendungsspektrum der Datensicherheit ist sachgerecht, überfordert aber in der praktischen Umsetzung nicht nur die Juristen, sondern auch Entwickler und Anbieter von mHealth Apps. Diese Überforderung hat drei Hauptursachen:[156]

– Es fehlt an analytischen Werkzeugen, um das Risikopotential der Datenbearbeitungen abzuschätzen und gestützt darauf die risikogerechten Datensicherheitsanforderungen zu konkretisieren. Das Instrument der Datenschutz-Folgenabschätzung (Art. 20 E-DSG) wird in Zukunft diesen Missstand hoffentlich beseitigen.

– Es gibt kaum verbindliche Standards, welche die Datensicherheitsanforderungen an Produkte und Systeme auf technischer und organisatorischer Ebene konkretisieren. Die einschlägigen Standards (namentlich die ISO/IEC 27000-Normenfamilie) beschlagen betriebliche Datensicherheitsanforderungen, nicht aber produkt- oder systembezogene Aspekte. International anerkannte Standards zu sicherheitsrelevanten Themen von im Gesundheitsbereich eingesetzter Software existieren zwar[157], doch bleiben auch dort die Vorgaben jeweils vage. Im Vordergrund stehen auch in diesen Normenwerken die Analyse der Risiken und die Dokumentation, wie mit diesen Risiken umzugehen ist.[158]

– Datensicherheit hat ihren Preis. Die Gratiskultur der App-Ökonomie nährt die Versuchung, Nutzerdaten im Gegenzug für die kostenlose Software-Überlassung als „Währung“ zu betrachten und Datensicherheitsaspekte im Zuge der App-Programmierung bewusst oder unbewusst zu vernachlässigen.[159]

156 Vgl. dazu auch BEARDWOOD/BOWMAN (Fn. 94), 166 und 172.
157 Vgl. IEC 82304-1 Health Software – Part 1: General requirements for product safety, Oktober 2016.
158 Vgl. Ziff. 4.2 und 7.2.3.1 IEC 82304-1 (Fn. 157).
159 ISLER, digma 2013 (Fn. 10), 111.

130 Die Regulierung der Datensicherheit ist nach dem Gesagten prinzipienbasiert ausgestaltet. Dies ist auch unter dem Regime der DSGVO sowie unter dem E-DSG nicht anders. Obwohl der US-amerikanische regelbasierte Ansatz mehr praktische Hilfestellungen bietet, ist aus unserer Sicht dennoch am europäischen Konzept festzuhalten. Die intellektuellen Anforderungen an die Marktteilnehmer sind zwar hoch und erfordern ein hohes Mass an Eigenverantwortung, doch kann die Datensicherheit jeweils einzelfallbezogen beurteilt und umgesetzt werden.

4.1.7. Meldepflichten bei Verletzungen der Datensicherheit

131 Meldepflichten bei Verletzungen der Datensicherheit haben sich dies- und jenseits des Atlantiks als Standardinstrumente des Datenschutzes etabliert. Das revidierte Datenschutzgesetz will deshalb auch für die Schweiz nachziehen (Art. 22 E-DSG). Dabei geht es nicht nur um Datenlecks, sondern um Ereignisse, die dazu führen, dass Personendaten verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden (vgl. Art. 4 lit. g E-DSG).

132 Das geltende Recht sieht eine Meldepflicht nicht explizit vor. Eine Meldepflicht bei Datenschutzverstössen kann aber unter den Grundsatz von Treu und Glauben nach Art. 4 Abs. 2 DSG, den Grundsatz der Zweckbindung nach Art. 4 Abs. 3 DSG oder den Grundsatz der Datensicherheit Art. 7 DSG subsumiert werden.[160] Eine Meldung ist daher geboten, wenn die betroffene Person die berechtigte Erwartung hat, über einen Vorfall informiert zu werden, z.B. weil sie dadurch die erforderlichen Sicherheitsmassnahmen auf ihrer Seite vornehmen kann, wie Kreditkartensperren oder Änderungen von Passwörtern etc. Bei einem unbefugten Zugriff auf Gesundheitsdaten, aber auch bei deren Manipulation oder Vernichtung, können die Risiken für die betroffene Person beträchtlich sein, gerade auch wenn der Verdacht besteht, dass allenfalls die Richtigkeit von gesundheitsbezogenen Daten nicht mehr gewährleistet ist. Die Einführung einer expliziten Meldepflicht bei Datenschutzverletzungen ist daher zu begrüssen.

160 FASNACHT TOBIAS, *in:* PASSADELIS/ROSENTHAL/THÜR (Hrsg.), Datenschutzrecht, Basel 2015, Rn. 31.19; EBNETER MATTHIAS, Informationspflichten im Zusammenhang mit Data Security Breaches, *in:* Jusletter 7. Juni 2010, Rz. 11; ROSENTHAL (Fn. 141), Art. 4 DSG N 16.

4.1.8. Bekanntgabe von Personendaten ins Ausland

133 Die Bekanntgabe von Personendaten ins Ausland ist ohne Einwilligung der betroffenen Person oder andere Rechtfertigungsgründe auch nach schweizerischem Recht u.a. nur erlaubt, wenn im Importstaat ein angemessenes Datenschutzniveau besteht oder vertragliche Garantien die Einhaltung des Datenschutzes sicherstellen (Art. 6 DSG). Wichtig ist in diesem Kontext vor allem, dass die Schweiz im Verhältnis zur EU nach Wirksamwerden der DSGVO ihren Status als sicheres Drittland beibehalten kann, damit der grenzüberschreitende Datenverkehr nicht gehemmt wird. Im Verhältnis zur USA hat auch die Schweiz den Privacy Shield adaptiert[161], so dass der Datenverkehr mit zertifizierten US-amerikanischen Unternehmen ohne den Abschluss vertraglicher Garantien gewährleistet bleibt.

134 Der Privacy Shield ist allerdings weiterhin Kritik ausgesetzt. Diese ist jedoch überzogen. Der Formalismus der Datentransferverträge, die häufig unreflektiert abgeschlossen werden, erhöht das Schutzniveau nicht. Insofern kann die Privacy Shield-Zertifizierung eines US-amerikanischen Anbieters durchaus ein Kriterium darstellen, wenn es darum geht, ob eine mHealth App als datenschutzkonform zu beurteilen ist.

4.1.9. Zertifizierungsverfahren

135 Die Zertifizierung von Datenverarbeitungssystemen oder -programmen gemäss Art. 11 Abs. 1 DSG ist in der Schweiz toter Buchstabe geblieben,[162] hat aber dennoch den Sprung in das Revisionsvorhaben geschafft (vgl. Art. 12 E-DSG).

136 Produktzertifizierungen von mHealth Apps haben auch in der EU einen schweren Stand. Das freiwillige europäische Datenschutzgütesiegel „EuroPriSe“ (European Privacy Seal) wurde erst an wenige mHealth Apps verliehen.[163] Die ePrivacy GmbH mit Sitz in Hamburg bietet ein freiwilliges Datenschutz-Gütesiegel für mHealth Apps an, doch wurden bislang lediglich eine Handvoll Produkte zertifiziert.[164] Zu erwähnen ist auch die in Grossbritannien eingeführte mHealth App-Zertifizierung durch den NHS („*NHS Approved*“), die nebst klinischen Krite-

161 Botschaft E-DSG (Fn. 146), BBl 2017, 6999; vgl. vorstehend, Rz. 90.
162 GLOOR SCHEIDEGGER CAROLINE, *in:* PASSADELIS/ROSENTHAL/THÜR, Datenschutzrecht, Basel 2015, Rn. 23.73.
163 Beispiel: Haemoassist, https://www.european-privacy-seal.eu/eps-en/statconsult-haemoassist (zuletzt besucht am 9. Oktober 2017).
164 Vgl. die Webseite der ePrivacy GmbH: https://www.eprivacy.eu/guetesiegel/eprivacyapp/ (zuletzt besucht am 9. Oktober 2017).

rien auch den Datenschutz erfasst.[165] Es bleibt abzuwarten, ob der EU Code of Conduct[166] zu einem Zertifizierungsschub führen wird.

4.2. Vorgaben des EPDG

4.2.1. Anbindung von mHealth Apps

137 Wie bereits erwähnt, ist das ePD ein Sekundärsystem, welches durch die in den Primärsystemen abgelegten Patientendossiers befüllt wird. Der Regelungsbereich des EPDG (sog. „Vertrauensraum“) erfasst die Primärsysteme grundsätzlich nicht, regelt aber deren ePD-seitige Anbindung über die Zugangsportale der Gemeinschaften und Stammgemeinschaften. Die patientenseitigen internen Zugangsportale der Stammgemeinschaften, welche für das Einstellen von Dokumenten durch Patienten dienen, werden ebenfalls vom Regelungsbereich des EDPG erfasst (Art. 10 Abs. 2 lit. b Ziff. 3).

138 Die Stammgemeinschaften, welche die internen Zugangsportale für die Patienten betreiben, unterliegen einer Zertifizierungspflicht (Art. 11 lit. a EPDG). Die von den Stammgemeinschaften als Voraussetzung für die Zertifizierung einzuhaltenden Datenschutz- und Datensicherheitsanforderungen sind in der EDPV festgelegt (Art. 12 Abs. 1 EPDG). Art. 12 EPDV bestimmt, dass die Gemeinschaften und Stammgemeinschaften ein risikogerechtes Datenschutz- und Datensicherheitsmanagementsystem betreiben müssen. Dieses muss insbesondere folgende Elemente umfassen:

- Ein System zur Erkennung von und zum Umgang mit Sicherheitsvorfällen;
- ein Inventar der Informatikmittel und Datensammlungen;
- die Datenschutz- und Datensicherheitsanforderungen an die angeschlossenen Gesundheitseinrichtungen und Dritte.

Diese Elemente sind in der EPDV-EDI, Anhang 2 weiter konkretisiert.

[165] Vgl. vorstehend, Rz. 46.
[166] Vgl. vorstehend, Rz. 85 ff.

139 Das EPDG sieht eher beiläufig (Art. 1 Abs. 4 EPDG) auch sog. externe, d.h. von den Gemeinschaften und Stammgemeinschaften unabhängige Zugangsportale vor. Diese unterliegen ebenfalls einer Zertifizierungspflicht (Art. 11 lit. b EPDG). Die Funktionalität der externen Zugangsportale bleibt nach dem Willen des Gesetzgebers allerdings auf die Dateneinsicht durch den Patienten beschränkt, während eine Datenbereitstellung durch den Patienten oder Gesundheitsfachpersonen ausgeschlossen ist.[167] Im aktuellen Ausführungsrecht sind die externen Zugangsportale sodann gar nicht vorgesehen, da der Bundesrat es unterlassen hat, die entsprechenden Zertifizierungsvoraussetzungen gemäss Art. 12 EPDG zu regeln.[168]

140 Während die Gemeinschaften verpflichtet sind, ein Inventar der Primärsysteme zu führen, mit denen auf das ePD zugegriffen werden kann (EPDV-EDI, Anhang 2, Ziff. 4.6.2 lit. j), ist eine Inventarisierung der Applikationen, mit denen Daten auf Initiative der Patienten in das ePD gestellt werden können, derzeit nicht vorgesehen.

141 Gemeinschaften müssen weiter eine Liste mit allen Lieferanten und Dienstleistungserbringern („Dritte“) führen, die unter Umständen auf Daten des ePD zugreifen, sie verarbeiten, speichern, weitergeben oder Informatikinfrastrukturkomponenten dafür bereitstellen (EPDV-EDI, Anhang 2, Ziff. 4.9.1). Auch diese Vorgabe greift nicht auf mHealth Apps aus. Eine Gleichbehandlung von mHealth Apps mit Primärsystemen, deren Grad der Einbindung an das ePD vielfach wesentlich tiefer ist, wäre wohl auch nicht in jedem Fall sachgerecht. Vorläufig ist zudem angedacht, dass die über mHealth Apps bereitgestellten Daten erst dann als Dokumente in den Vertrauensraum des ePD gelangen können, wenn der Patient sich auf dem Zugangsportal seiner Stammgemeinschaft im Einzelfall authentifiziert und in den Datentransport eingewilligt hat.[169] Die Zwischenablagen, in denen die durch mHealth Apps generierten Daten auf ihre Aufbereitung Überführung in das ePD „warten“, befinden sich ausserhalb des Vertrauensraums.[170] Vor dem Hintergrund dieser Systemarchitektur ist es nicht zwingend geboten, den Anbietern von mHealth Apps weitreichende Datenschutzpflichten aufzuerlegen; immerhin ist aber im Sinne einer Minimalanforderung darauf zu achten, dass keine Daten aus dem Vertrauensraum (insbesondere auch nicht die Patientenidentifikationsnummer) ohne Zustimmung des Patienten mit den mHealth Apps verknüpft werden.

167 Botschaft EPDG (Fn. 4), BBl 2013, 5336 und 5339.
168 Vgl. Art. 30 f. EPDV.
169 Vgl. zu diesem Lösungsansatz vorstehend, Rz. 31.
170 Vgl. sogleich nachstehend, Rz. 142.

142 Sollte jedoch zur Verbesserung der Nutzerfreundlichkeit ein automatischer Transport der Daten einer mHealth App über das patientenseitige Zugangsportal direkt in das ePD (d.h. *machine-to-machine*) vorgesehen sein, müssten sowohl die Kriterien für die Authentifizierung des Patienten wie auch die weiteren Anforderungen an die Datensicherheit und den Datenschutz für mHealth Apps – ähnlich wie bei den Primärsystemen – zwingend auf einem hohen Schutzniveau festgelegt werden.

143 Nach der geltenden Rechtslage liesse sich eine solche automatische Datenbereitstellung in das ePD indes gar nicht umsetzen. Gemäss Art. 7 Abs. 1 lit. a EPDG müssen Patienten, die auf das ePD zugreifen, über eine sichere elektronische Identität verfügen. In Zwischenablagen ausserhalb des Vertrauensraums gespeicherte Daten dürfen nur dann in das ePD überführt werden, wenn der Patient hierfür seine Einwilligung erteilt hat (EPDV-EDI, Anhang 2, Ziff. 9.4.3 lit. a). Hierzu bedarf es stets eines starken Authentifizierungsverfahren mit mindestens zwei Authentifizierungsfaktoren (vgl. Art. 23 lit. c EPDV sowie EPDV-EDI, Anhang 2, Ziff. 8.3 sowie Anhang 8).[171] Art. 23 lit. b EPDV konkretisiert die Anforderungen an die Identifikationsmittel für Gesundheitsfachpersonen und Patienten sodann u.a. dahingehend, dass sie so aufgebaut sein müssen, dass sie nur von den berechtigten Personen verwendet werden können. Es darf z.B. nicht möglich sein, das geschützte Schlüsselmaterial des Identifikationsmittels auf ein anderes System oder Medium zu übertragen, z.B. durch Abfangen von im Klartext übermittelten Passwörtern.[172] Derartige „Schaber" existieren bspw. für mobile Applikationen, welche Kontoinformationen von Kunden bei verschiedenen Banken abfragen und in einer aggregierten Übersicht zusammenstellen. Im Kontext des ePD will man die Weitergabe der Zugangsdaten an Dritte jedoch explizit unterbinden. Damit wäre es nach geltendem Ausführungsrecht gar nicht möglich, die Ablage von über mHealth Apps generierten Patientendaten im ePD zu automatisieren.[173]

171 Erläuterungen EPDV (Fn. 7), 30.
172 Erläuterungen EPDV (Fn. 7), 35.
173 Vgl. auch Erläuterungen EPDV (Fn. 7), 32, in Bezug auf den „umgekehrten" Fall, d.h. den automatischen Export von Daten aus dem ePD, der ohne explizite Einwilligung des Patienten nicht möglich sein darf. Hingegen ist es denkbar, dass die Zugangsportale der Stammgemeinschaften Ablagefunktionen ausserhalb des Vertrauensraums bereitstellen, die Daten aus Datenspeichern von mHealth Apps automatisch abrufen, wobei dem Patienten immer auch die Möglichkeit gegeben werden muss, Daten direkt, d.h. ohne Verwendung intermediärer Speicher, im ePD zu erfassen (vgl. EPDV-EDI, Anhang 2, Ziff. 9.4.3).

4.2.2. Aufklärungspflichten

144 Im Bereich von mHealth kommt den Stammgemeinschaften eine Informationspflicht über Datenschutz- und Datensicherheitsmassnahmen zu (vgl. Art. 15 Abs. 2 EPDV). Hierbei geht es in erster Linie um Hinweise zum sicheren Umgang mit Identifikationsmitteln und geheimen Authentifizierungsinformationen, aber auch um Aufklärung zu Betrugsmustern und sichererer Verwendung von Endgeräten.[174] Die Aufklärung über Datenschutzrisiken bei der Verwendung von mHealth Apps gehört nicht explizit zum Pflichtenheft, kann aber unter diese Bestimmung subsumiert werden, wenn das Zugangsportal für die Patienten eine Anbindung an mHealth Apps vorsieht.

4.3. Anpassungsbedarf und Massnahmenkatalog

145 Der Streifzug durch die für mHealth Apps relevante Normenlandschaft in der EU, den USA und der Schweiz hat gezeigt, dass die wichtigsten Vorgaben zu Datenschutz und Informationssicherheit im Bereich der Gesundheitsinformationstechnologie in der EU, den USA und der Schweiz weitgehend deckungsgleich sind. Unterschiede ergeben sich aber in den Regulierungsansätzen: Während in der Schweiz und der EU die allgemeinen Datenschutzvorschriften gelten, haben die USA eine sektorspezifische Regulierung erlassen. Diese enthält für die unter HIPAA / HITECH fallenden Dienste ein engmaschiges Netz an einzuhaltenden Standards, führt aber auch dazu, dass der Datenschutz im Sinne des europäischen Rechtsverständnisses bei Produkten und Diensten, die nicht von der Regulierung erfasst sind, lückenhaft ist. Dies gilt insbesondere für mHealth Apps, die nicht der Datenerfassung oder -bearbeitung durch Gesundheitsfachpersonen dienen, sondern als reine Datenzulieferer in das Gesundheitssystem fungieren.[175]

146 Nach dem Gesagten lassen sich für die meisten Anwendungsfälle von mHealth aus der fortgeschrittenen Regulierung in den USA für die Anbindung von mHealth Apps an das ePD keine direkten Schlussfolgerungen ableiten. Hingegen sind die weit fortgeschrittenen und detaillierten Datensicherheitsstandards in den USA auch für die Entwicklung und den Einsatz von mHealth Apps in Europa eine wertvolle Orientierungshilfe. Das Anwendungsspektrum der mHealth-Initiativen in der EU, allen voran der EU Code of Conduct, ist jedoch wesentlich

[174] Erläuterungen EPDV (Fn. 7), 29.
[175] Vgl. vorstehend, Rz. 94.

breiter und damit als Richtschnur für die mHealth-Regulierung in der Schweiz besser geeignet.

147 Anbieter von global agierenden mHealth Apps einer Sonderregulierung zu unterstellen, wäre daher nicht zielführend. Der Fokus ist vielmehr auf folgende Ansätze zu legen:

– Überdenken der dezentralen Bereitstellung der Zugangsportale für Patienten durch die Stammgemeinschaften (**Massnahme 1**);

– Vermeiden der Verknüpfung von mHealth Apps mit elektronischer Identität des Patienten (**Massnahme 2**);

– Ermöglichen einer automatisierten Datenbereitstellung durch mHealth Apps (**Massnahme 3**);

– Information und Sensibilisierung der Bevölkerung (**Massnahme 4**).

4.3.1. Massnahme 1: Überdenken der dezentralen Bereitstellung der Zugangsportale für Patienten durch die Stammgemeinschaften

148 Die Zugangsportale für die Patienten werden durch die Stammgemeinschaften betrieben (Art. 10 Abs. 2 lit. b und c EPDG). Die Stammgemeinschaften sind daher in erster Linie verantwortlich für die Anbindung von mHealth Apps an das ePD. Diese dezentrale Struktur kann dazu führen, dass je nach Stammgemeinschaft die Integration von mHealth Apps unterschiedlich gefördert und der ohnehin kleine schweizerische mHealth-Markt weiter zersplittert wird. Es stellt sich sodann generell die Frage, ob die Stammgemeinschaften die erforderlichen Ressourcen und Kompetenzen aufbringen können, um mHealth Apps auf ihre Datenschutzkonformität und klinische Qualität zu prüfen und die Einhaltung der Vorgaben sicherzustellen. Dieselbe Problematik stellt sich an sich auch bei der Anbindung von Primärsystemen, doch ist dort das Produkteangebot möglicherweise weniger fragmentiert als im mHealth-Bereich. Darüber hinaus haben die Leistungserbringer als Träger der Stammgemeinschaften einen Anreiz, die von ihnen genutzten Primärsysteme an das ePD anzubinden; bei mHealth Apps ist dies nicht unbedingt der Fall.

149 Eine gewisse Zentralisierung könnte möglicherweise durch die Zulassung externer Zugangsportale mit Schreibrecht für die Patienten gemäss Art. 8 Abs. 2 EPDG erreicht werden, sofern für eine derartige Lösung überhaupt ein Markt vorhanden ist. Die externen Zugangsportale sind im EPDG nur rudimentär gere-

gelt. Sie werden in Art. 1 Abs. 4 EPDG beiläufig als „Portale für den Zugang der Patientinnen und Patienten zu ihren Daten“ definiert und in Art. 11 lit. b EPDG der Zertifizierungspflicht unterstellt. Laut Botschaft zum EDPG soll sich die Funktionalität der externen Zugangsportale ausschliesslich auf ein Leserecht für die Patienten beschränken, während die Datenbereitstellung durch den Patienten nur über das Zugangsportal der Stammgemeinschaft möglich sein soll.[176] Im Gesetzestext selbst findet diese Einschränkung allerdings keinen zwingenden Niederschlag, so dass nach unserer Auffassung der Verordnungsgeber externe Zugangsportale in eigener Kompetenz auch mit einem Schreibrecht ausstatten könnte.

150 Sollte die Einführung externer Zugangsportale mit Schreibrechten für die Patienten in Erwägung gezogen werden, wäre vertieft zu prüfen, ob hierfür entgegen den Ausführungen in der Botschaft im EPDG bereits eine gesetzliche Grundlage besteht. Darüber hinaus müsste das Ausführungsrecht die Zertifizierung dieser Zugangsportale regeln, was es bis anhin nicht tut (vgl. Art. 30 f. EPDV).

151 Als Alternative zur Einführung externer Zugangsportale für Patienten mit erhöhter Funktionalität könnte auch eine stärkere Rolle des Bundesamts für Gesundheit (**BAG**) bei der Prüfung von mHealth Apps auf deren Konformität mit den datenschutzrechtlichen Anforderungen ins Auge gefasst werden.[177]

4.3.2. Massnahme 2: Vermeiden der Verknüpfung der mHealth App mit elektronischer Identität des Patienten

152 Bei der Anbindung von mHealth Apps an das ePD dürfte in der Regel die Implementierung einer Schnittstelle zwischen dem mobilen Gateway des ePD und der mHealth App erforderlich sein. Hierbei ist die Verknüpfung des Datenflusses von der mHealth App in das ePD mit der elektronischen Identität des Patienten erforderlich, damit bei der individuellen Zuordnung der Daten keine Fehler passieren. Diese Verknüpfung hat im Idealfall so zu erfolgen, dass eine Identifizierung des Nutzers der mHealth App durch den Anbieter nicht möglich ist. Die Identifizierung des Patienten sollte sodann seitens der mHealth App nicht über die Patientenidentifikationsnummer gemäss Art. 4 EPDG erfolgen. Die Verwendung der Patientenidentifikation ist zwar im Anwendungsbereich

[176] Vgl. vorstehend, Rz. 139.
[177] Vgl. hierzu Massnahme 5 (nachstehend, Rz. 176 ff.).

des EPDG gestattet (Art. 6 EPDG), doch ist deren Verknüpfung mit Drittsystemen zu vermeiden.[178]

153 Die empfohlene Vorgabe wäre auf Stufe EPDV-EDI umzusetzen. Die entsprechenden Delegationsnormen finden sich in Art. 10 Abs. 3 sowie Art. 12 Abs. 4 EPDV und brauchen nicht angepasst zu werden.

4.3.3. Massnahme 3: Ermöglichen einer automatisierten Datenbereitstellung durch mHealth Apps

154 Es ist angedacht, dass der Patient die über den mobilen Gateway generierten Dokumente jeweils situativ in das ePD einstellt und dementsprechend jede Session erneut authentifizieren muss.[179] Es fragt sich, ob diese Schwelle den angestrebten Einbezug von mHealth in das ePD nicht übermässig behindert. Die fehlende Durchgängigkeit der Daten in das ePD weist zweifelsfrei datenschutzrechtliche Vorteile auf, senkt aber die Nutzerfreundlichkeit von mHealth Apps im Kontext des ePD. Die Vorteile von mHealth liegen gerade darin, dass Gesundheitsdaten im Kontinuum verfügbar sind und der behandelnde Arzt unabhängig von physischen Konsultationen stets ein aktuelles Datenprofil einsehen kann.[180] Selbst wenn der Patient im wöchentlichen Rhythmus bestimmte Werte in das ePD einstellen sollte, kann nicht von ihm erwartet werden, dass er sich regelmässig im richtigen Zeitpunkt frisch über das Zugangsportal seiner Stammgemeinschaft anmeldet und in den Upload der Dokumente einwilligt (vgl. EPDV-EDI, Anhang 2, Ziff. 9.4.3 lit. a). Ein erheblicher Teil des Zusatznutzens von mHealth Apps geht durch dieses Einwilligungserfordernis verloren.

155 Die Zulassung einer automatisierten Bereitstellung von Daten von mHealth Apps in das ePD könnte demgegenüber zu einer stärkeren Einbindung der Anbieter entsprechender mHealth Apps führen, da die Authentifizierung der Patienten nach der ersten Authentifizierung des Patienten und der Erteilung einer Globaleinwilligung für den kontinuierlichen Upload der generierten Dokumente in das ePD jeweils automatisiert über einen Authentifizierungs-Token (*machine-to-machine*) erfolgen müsste. Damit müssten an diese mHealth Apps ähnlich hohe Anforderungen gestellt werden wie an die Anbieter von Primärsystemen,

---

178 Dies gilt ebenso bei der Anbindung von Primärsystemen an das ePD, vgl. eHEALTH SUISSE, Einführung in das ePatientendossier: Anbinden von Primärsystemen, 13. September 2016, 20.

179 Vgl. vorstehend, Rz. 31 und 141 f.

180 ISLER MICHAEL, Healthcare Meets Smart Wireless – and the Law? 2013, 4, https://www.walderwyss.com/publications/1460.pdf (zuletzt besucht am 9. Oktober 2017).

und die Zugangsportale der Stammgemeinschaften müssten die Einhaltung der Datenschutz- und Datensicherheitsvorschriften zwingend sicherstellen (vgl. EPDV-EDI, Anhang 2, Ziff. 4.9).

156 Sollte eine automatisierte Datenbereitstellung in das ePD im beschriebenen Sinne angestrebt werden, müssten Art. 23 lit. b und c EPDV angepasst werden.[181] Die Vorgaben der Zwei-Faktor-Authentifizierung und des Aufbaus des Identifikationsmittels in der Weise, dass es nur von der berechtigten Person verwendet werden kann, müssten durch einen Passus ergänzt werden, wonach das EDI hiervon Ausnahmen vorsehen könnte, um das automatische Erfassen von Daten im elektronischen Patientendossier durch vom Patienten genutzte technische Hilfsmittel zu ermöglichen. Die konkrete Ausführung wäre auf Stufe EDPV-EDI, Anhang 2 zu regeln.

4.3.4. Massnahme 4: Sensibilisierung der Patienten und Gesundheitsfachpersonen

157 Die Stammgemeinschaften müssen den Patienten Datenschutz- und Datensicherheitsmassnahmen empfehlen (Art. 15 Abs. 2 EPDV). Diese Informations- und Aufklärungspflicht greift auch auf den Umgang der Patienten mit mHealth Apps aus, wenn diese in die ePD-Umgebung eingebunden werden. Um die Aufgabe der Stammgemeinschaften zu erleichtern und eine einheitliche Sprachregelung zu verwenden, wäre die Ausarbeitung eines Merkblatts, das sich zu datenschutzspezifischen Risiken, Vorsichtsmassnahmen und Handlungsempfehlungen äussert, sinnvoll.

5. Durchsetzungsmechanismen

5.1. Rolle der Beteiligten (Anbieter, Entwickler, Gesundheitsfachpersonen, Gemeinschaften und Patienten)

158 Wie bereits dargelegt,[182] zeichnet sich das App-Ökosystem durch zahlreiche Beteiligte aus, deren Funktionen ineinander verwoben sind:

– Der **Anbieter** der mHealth App betreibt die App. Häufig hängt der Betrieb der App von einer externen Cloud-Plattform ab, auf der die pro-

[181] Vgl. vorstehend, Rz. 142.
[182] Vgl. vorstehend, Rz. 35.

grammierten Funktionen ablaufen und die Daten gespeichert werden. Diese Plattformen unterliegen ebenfalls der Verantwortung des Anbieters. Der Anbieter ist aus datenschutzrechtlicher Sicht Inhaber der Datensammlung („Verantwortlicher“ unter dem E-DSG sowie der DSGVO) und daher für die Einhaltung des Datenschutzes und der Datensicherheit primär verantwortlich.

– Der **Entwickler** der mHealth App kann mit dem Anbieter identisch sein, aber auch in dessen Auftrag oder als unabhängiger Dritter das Programm entwickelt haben. Entwickler werden durch das Datenschutzrecht nur am Rande tangiert. Da sie nicht selbst Personendaten bearbeiten, fallen sie nicht in den Anwendungsbereich des Datenschutzgesetzes. Die technischen Datenschutzvorgaben wie Privacy by Design, Privacy by Default und Datensicherheit beginnen erst auf der Ebene der Datenbearbeitung zu greifen.[183] Es liegt also am Anbieter, die technische Datenschutzkonformität der mHealth App sicherzustellen. Der einzige datenschutzrechtliche Ansatzpunkt, welcher bereits auf der Entwicklungsstufe greift, ist die Zertifizierung von Produkten.[184]

– Der **Patient** ist die Person, über die in der mHealth App Daten bearbeitet werden. Er ist somit die betroffene Person im Sinne der Datenschutzgesetzgebung. Er ist Adressat der vom Anbieter abgegeben Datenschutzerklärungen und muss unter Umständen seine ausdrückliche Einwilligung zu bestimmten Bearbeitungsvorgängen erteilen.

– Die **Stammgemeinschaften** betreiben das Zugangsportal für die Patienten. Sie sorgen dafür, dass es den Patienten ermöglicht wird, über mHealth Apps generierte Daten als Dokumente in das ePD zu stellen und dort datenschutzkonform zu speichern. Nach der Übergabe der Daten in das ePD sind diese von den mHealth Apps entkoppelt und gelangen in den Verantwortungsbereich der Stammgemeinschaft. Ab dem Eintreffen der Daten im mobilen Gateway des ePD übernehmen die Stammgemeinschaften somit die Aufgaben eines Inhabers der Datensammlung bzw. eines Verantwortlichen.

– Die **Gesundheitsfachpersonen** schliesslich haben über das ePD keine direkte Schnittstelle zu den mHealth Apps. Sie sind daher in den Bearbei-

[183] Vgl. vorstehend, Rz. 67, 69, 76.
[184] Vgl. vorstehend, Rz. 79 ff., 134 f.

tungsvorgang nicht eingebunden. Es kann aber sein, dass sie über andere Kanäle auf die Daten des Patienten zugreifen können, entweder indem der Anbieter die Daten in einem Speichermedium vorhält, auf das die Gesundheitsfachperson zugreifen kann, oder indem eine Schnittstelle der mHealth App zum Primärsystem der Gesundheitsfachperson eingerichtet wird. Solche alternativen technischen Lösungen sind jedoch vom ePD unabhängig und daher vorliegend nicht weiter von Belang.

159 Im Zentrum der Handhabung der zu erörternden Durchsetzungsinstrumente stehen nach dem Gesagten Anbieter, die Stammgemeinschaften und die Patienten:

– Die Anbieter sind die Adressaten der Durchsetzungsinstrumente. Deren Tauglichkeit ist daran zu messen, ob sich präventive Schutzmassnahmen wirksam umsetzen und Verstösse sanktionieren lassen.

– Die Stammgemeinschaften sind nach der gegenwärtigen gesetzlichen Regelung dafür verantwortlich, dass die Anbindung von mHealth Apps an das ePD funktioniert und die Datensicherheit auf der Ebene des ePD gewährleistet bleibt. Sie haben damit eine Gatekeeper-Funktion und können entscheiden, welche mHealth Apps für eine Anbindung an das ePD und Frage kommen und welche nicht.

– Die Patienten sind die Personen, deren Daten zu schützen sind. Sie haben selbst auch Durchsetzungsinstrumente in der Hand, deren Wirksamkeit in einem separaten Kapitel untersucht wird.[185]

160 Am Rande, nämlich auf der Stufe der Produktzertifizierungen, sind auch die Entwickler auf freiwilliger Basis involviert.

5.2. Durchsetzungsinstrumente

5.2.1. Verwaltungsrechtliche Instrumente

161 Der griffigste Durchsetzungsmechanismus ist die präventive Kontrolle. Die Stammgemeinschaften nehmen diesbezüglich als Gatekeeper im Rahmen der Anbindung von mHealth Apps an das ePD eine zentrale Funktion wahr. Um eine

[185] Vgl. nachstehend, Rz. 182 ff.

einheitliche Praxis unter dem Stammgemeinschaften sowie eine hohe Durchdringung von mHealth im Kontext des ePD zu forcieren, wäre es allerdings sinnvoll, diese Aufgaben zumindest teilweise zu zentralisieren, entweder indem

– ein externes Zugangsportal die Anbindung von mHealth Apps übernimmt (vgl. Massnahme 1);[186] oder

– das BAG einen Teil der Gatekeeper-Funktion für sämtliche Stammgemeinschaften übernimmt (Massnahme 5).[187]

162 Im Vordergrund steht ein Kriterienkatalog für mHealth Apps. Kriterienkataloge schaffen zweifachen Nutzen: Zum einen bieten sie Herstellern von mHealth Apps eine Hilfestellung bei der Entwicklung von datenschutzfreundlichen Programmen und Diensten, zum anderen können Apps, welche die Kriterien erfüllen, mit einem Gütesiegel ausgezeichnet werden und dadurch die Auswahl der Patienten aus der Fülle der Angebote erleichtern.

163 Die Ausgestaltung der Kriterien für die Anbindung von Dritten an die Zugangsportale der Patienten steht dem Verordnungsgeber frei. Namentlich obliegt es dem Bundesrat, die Anforderungen an die Zertifizierung der Stammgemeinschaften und ihrer Zugangsportale im Hinblick auf die Gewährleistung des Datenschutzes und der Datensicherheit festzulegen (Art. 12 Abs. 1 lit. b EPDG i.V.m. Art. 11 EPDG). Diese Anforderungen können auch Kriterien mit einschliessen, welche die an das ePD angebundenen Drittsysteme erfüllen müssen.

164 Keine gesetzliche Grundlage im EPDG hätte jedoch eine Zertifizierungspflicht für mHealth Apps selbst.

165 Bei der Ausgestaltung des Kriterienkatalogs sind folgende Abstufungen denkbar:

– **Stufe 1**: Die Anbindung von mHealth Apps an das ePD ist auf mHealth Apps beschränkt, welche mit einem bestimmten Datenschutzgütesiegel ausgezeichnet sind. Apps, welche diese Voraussetzungen nicht erfüllen, könnten nicht an das ePD angebunden werden.

[186] Vgl. vorstehend, Rz. 148 ff.
[187] Vgl. nachstehend, Rz. 176 ff.

– **Stufe 2**: Die Datenschutzkonformität von mHealth Apps ist vor der Anbindung einer Prüfung (*Due Diligence*) durch die Stammgemeinschaft anhand eines definierten Kriterienkatalogs zu unterziehen. Apps, welche diese Prüfung nicht bestehen, könnten nicht an das ePD angebunden werden.

– **Stufe 3**: Die Anbindung von mHealth Apps an das ePD ist frei, sofern entsprechende Schnittstellen vorhanden sind. Es liegt an der Gesundheitsfachperson, welche die mHealth Apps empfiehlt, und in der Eigenverantwortung des Patienten, ein vertrauenswürdiges Produkt zu wählen. Die Stammgemeinschaften nehmen flankierend ihre Aufklärungspflicht wahr.

166 Stufe 1 ist untauglich, da entsprechend ausgezeichnete Produkte nicht in genügender Zahl vorliegen. Darüber hinaus ist es in der Schweiz vorläufig gar nicht möglich, ein Produkt zertifizieren zu lassen. Auch von privater Seite ausgegebene Datenschutzzertifikate sind eine Rarität. Eine Neubeurteilung könnte sich ergeben, wenn der EU Code of Conduct in Kraft gesetzt wird und sich eine ansehnliche Anzahl von Anbietern dem Kodex unterwirft.

167 Stufe 2 kommt nahe an das Zertifizierungserfordernis heran, verschiebt aber die Verantwortung von den Entwicklern der mHealth Apps auf die Stammgemeinschaften bzw. ein externes Zugangsportal und/oder das BAG, sofern die entsprechenden Massnahmen umgesetzt werden.[188] Während ein Zertifikat als Gütesiegel den Vertrauensnachweis unmittelbar erbringt, muss bei der individuellen Prüfung von mHealth Apps anhand eines Kriterienkatalogs das Vertrauen mittels einer Due Diligence erarbeitet werden. Um wirklich in die Tiefe der Datenschutzkonformität zu gehen und die Güte der Datensicherheitsmassnahmen beurteilen zu können, müssten ein Dialog mit den Anbietern sowie technische Audits stattfinden. Ein solches Unterfangen würde überproportional Ressourcen beanspruchen und im Ergebnis einer Zertifizierung gleichkommen. Aus diesem Grund sollte sich die Prüfung auf Minimalkriterien beschränken.

168 Stufe 3, ein offenes System, betont die Eigenverantwortung der Patienten wie auch die Aufklärungspflicht der Gesundheitsfachpersonen und Stammgemeinschaften, enthält aber keine wirksamen präventiven Kontrollmechanismen.

[188] Vgl. hierzu Massnahme 1 (vorstehend, Rz. 148 ff.) und Massnahme 5 (nachstehend, Rz. 176 ff.).

169 Das System der Prüfung anhand eines Kriterienkatalogs (Stufe 2) erscheint am sinnvollsten. Da der Durchsetzung der datenschutzrechtlichen Vorgaben gegenüber Anbietern von mHealth Apps grosses Gewicht beigemessen wird und die präventive Kontrolle der effektivste Durchsetzungsmechanismus ist, kommt ein offenes System (Stufe 1) kaum in Frage. Darüber hinaus entfällt bei einem offenen System eine wichtige Sanktionsmöglichkeit, nämlich die Entfernung einer mHealth App vom ePD bei Datenschutzverstössen. Es ist zumindest eine niederschwellige Kontrolle vorzusehen. Allein der Prüfungspunkt, ob überhaupt eine Datenschutzerklärung vorliegt und die grundlegendsten Datenschutzvorgaben eingehalten werden (Stufe 2), wird einen Grossteil der mHealth Apps von der Anbindung an das ePD ausschliessen. Das Abstellen auf eine Zertifizierung (Stufe 3) würde demgegenüber die Messlatte derart hoch setzen, dass – zumindest im gegenwärtigen Zeitpunkt – aufgrund der geringen Zahl von Zertifizierungen praktisch keine mHealth App-Anbindungen möglich wären.

5.2.2. Vertragliche Instrumente

170 Es ist wahrscheinlich, dass die Stammgemeinschaften oder Zugangsportale mit den Anbietern Integrationsvereinbarungen schliessen werden, da für die Anbindung der mHealth Apps an die Schnittstelle des mobilen Gateways eine Zusammenarbeit erforderlich ist.

171 Eine Integrationsvereinbarung wäre ein weiteres probates Mittel, um die Datenschutz-Compliance der Anbieter, insbesondere der in einem Kriterienkatalog definierten Anforderungen, sicherzustellen. Durch die Vereinbarung eines Gerichtsstandes in der Schweiz könnte der effektive Rechtsschutz im Falle von Vertragsverletzungen gesteigert werden.

172 Es wäre daher sachgerecht, analog zu den bereits bestehenden Vorgaben bezüglich der Anbindung von Primärsystemen (vgl. EPDV-EDI, Anhang 2, Ziff. 4.9.4) die vertraglichen Mindestanforderungen an die Integrationsverträge mit Anbietern von mHealth Apps in den Zertifizierungsvoraussetzungen festzulegen und zusätzlich einen marktfähigen Integrationsmustervertrag zu entwickeln, welcher dem Datenschutz und der Datensicherheit breiten Raum einräumt.

5.2.3. Organisatorische und technische Instrumente

173 Die bisher vorgeschlagenen Massnahmen zielen darauf ab, die Datenschutzkonformität im Zeitpunkt der Erstanbindung der mHealth App an das ePD sicherzu-

stellen. Organisatorische und technische Massnahmen sollen sicherstellen, dass den gestellten Anforderungen auf Dauer nachgelebt wird.

174 Solche Massnahmen könnten periodisch durchgeführte Datensicherheits-Audits oder Datenfluss-Analysen beinhalten, um sicherzustellen, dass dem Zweckbindungsgrundsatz nachgelebt wird. Es ist allerdings weder Aufgabe der Stammgemeinschaften noch des EDI, die Datenschutz-Konformität von mHealth Apps laufend zu untersuchen. Eine entsprechende Untersuchungskompetenz kommt dem EDÖB zu (Art. 29 DSG).

175 Eine sinnvolle organisatorische Massnahme wäre jedenfalls ein Monitoring der mHealth-Landschaft, um auf Entwicklungen reagieren und bei bekannt gewordenen Datenschutzverstössen die erforderlichen Massnahmen treffen zu können. Es ist anzunehmen, dass dies innerhalb der Arbeitsgruppe mHealth bereits sichergestellt ist, weshalb zu diesem Punkt keine spezifische Massnahme vorgeschlagen wird.

5.3. Massnahmenkatalog

5.3.1. Massnahme 5: Kriterienkatalog für die Anbindung von mHealth Apps

176 Es wird empfohlen, bei der Anbindung von mHealth Apps eine datenschutzrechtliche Due Diligence anhand eines Kriterienkatalogs durchzuführen. Dieser müsste etwa die folgenden Prüfpunkte abdecken:

- Hat die App in öffentlich zugänglichen datenschutzspezifischen Tests positiv oder negativ abgeschnitten? Ist sie allenfalls zertifiziert?
- Liegt eine für die angesprochene Patientengruppe verständliche und leicht zugängliche Datenschutzerklärung vor?
- Wird in der Datenschutzerklärung der Anbieter identifiziert?
- Muss der Nutzer vor Inbetriebnahme der App in die Datenbearbeitung einwilligen? Sind die Eckpunkte dieser Einwilligung verständlich dargelegt?
- Sind die Bearbeitungszwecke in der Datenschutzerklärung auf den für die Funktion der mHealth App erforderlichen Umfang beschränkt? Kann

der Nutzer einer weitergehenden Bearbeitung zumindest widersprechen?

– Muss sich der Nutzer vor Inbetriebnahme der App identifizieren? Ist eine Identifizierung für die Funktionalität der App erforderlich?

– Kann über das Mobilgerät auf historische Gesundheitsdaten zugegriffen werden? Wenn ja, ist dieser Zugriff an eine sichere Authentifizierung (z.B. Fingerprint oder Passwort) gebunden?

– Erfolgt die Datenspeicherung und -übermittlung verschlüsselt?

177 Die Verantwortung für das Aufstellen des Kriterienkatalogs ist eine Aufgabe des Verordnungsgebers und kommt daher letztlich dem EDI (BAG) zu (Art. 12 Abs. 4 EPDV). Um Divergenzen und Doppelspurigkeiten zwischen den Stammgemeinschaften zu vermeiden, sollte die Durchführung der Prüfung (Due Diligence) der mHealth Apps ebenfalls zentralisiert erfolgen. Sofern diese Aufgabe nicht in der Verantwortung eines externen Zugangsportals zu liegen kommt,[189] wäre das BAG ebenfalls prädestiniert, diese Rolle auszufüllen, müsste aber die eigentliche Durchführung der Prüfungen an einen Dritten delegieren können. mHealth Apps, welche die Prüfung bestanden haben, würden auf einer Liste geführt, die allen Stammgemeinschaften (wie auch der Öffentlichkeit) zur Einsicht offensteht.

178 Die Prüfungstiefe wäre für mHealth Apps, die für eine automatisierte Datenbereitstellung in das ePD in Frage kommen, wesentlich umfassender als für diejenigen mHealth Apps, deren Daten bis zur individuellen Freigabe durch den Patienten ausserhalb des Vertrauensraums verbleiben.[190]

179 Die vorgeschlagene Massnahme bedingt Anpassungen auf verschiedenen Ebenen. Grundsätzlich obliegt dem Bund die Festlegung der Zertifizierungsvoraussetzungen im Hinblick auf die Gewährleistung des Datenschutzes und der Datensicherheit (Art. 12 Abs. 1 lit. b EPDG), während für die Umsetzung der Vorgaben die Stammgemeinschaften verantwortlich sind. Damit besteht für das Aufstellen eines Kriterienkatalogs für mHealth Apps eine gesetzliche Grundlage, sofern und soweit dieser Teil der Zertifizierungsanforderungen ist. Demgegen-

189 Vgl. hierzu Massnahme 1 (vorstehend, Rz. 148 ff.).

190 Zur Erinnerung ist darauf hinzuweisen, dass die Zulassung einer automatisierten Datenbereitstellung in das ePD eine Änderung von Art. 23 lit. b und c EPDV erforderlich machen würde; vgl. vorstehend, Rz. 156.

über ist die Durchführung von Prüfungen, ob bestimmte Drittdienste wie mHealth Apps im Einklang mit den Zertifizierungsanforderungen stehen, keine Bundesaufgabe. Sie obliegt den Stammgemeinschaften, während die Zertifizierungsstellen jährlich zu überprüfen haben, ob die Zertifizierungsvoraussetzungen eingehalten sind (Art. 34 Abs. 1 EPDV). Die Prüfung von mHealth Apps kann auch nicht nach Art. 13 Abs. 2 EPDG in ein „Zertifizierungsverfahren für einzelne Elemente der Informatikinfrastruktur" überführt werden, denn dies würde auf eine im Gesetz nicht vorgesehene Zertifizierung für mHealth Apps hinauslaufen. Sollte das BAG die vorgeschlagene Rolle übernehmen, wäre daher eine Delegationsnorm in das EDPG aufzunehmen, wonach der Bundesrat das BAG ermächtigen dürfte, die Stammgemeinschaften und Zugangsportale bei der Einhaltung der Zertifizierungsanforderungen zu unterstützen (Ergänzung von Art. 12 Abs. 2 EPDG und entsprechende Subdelegation in Art. 30 Abs. 3 EPDV). Die Rolle des BAG wäre anschliessend auf Stufe EDPV-EDI zu definieren.

5.3.2. Massnahme 6: Vorgaben für die vertragliche Anbindung von mHealth Apps und Erarbeitung einer Vorlage für einen Integrationsvertrag

180 Die Stammgemeinschaften sollen die Anbieter von mHealth Apps vertraglich verpflichten müssen, die Einhaltung der Vorgaben an den Datenschutz und die Datensicherheit sicherzustellen; dies bedarf einer Ergänzung der EPDV-EDI (analog EPDV-EDI, Anhang 2, Ziff. 4.9.4, in Bezug auf die Primärsysteme). Die Mindestvorgaben an den Inhalt dieser Verträge sind Bestandteil der Zertifizierungsvoraussetzungen (vgl. Art. 12 Abs. 1 lit b EPDG).

181 Um die Anbindung von mHealth Apps auf eine tragfähige vertragliche Grundlage stellen zu können, ist ein marktfähiger Integrationsmustervertrag zu entwerfen, der von den Stammgemeinschaften für die Anbindung von mHealth Apps an die ePD-Umgebung auf freiwilliger Basis verwendet werden kann. Dieser Vertrag sollte etwa den folgenden datenschutzrelevanten Mindestinhalt aufweisen:[191]

- Verpflichtung des Anbieters, die Anforderungen des schweizerischen Datenschutzgesetzes und/oder der DSGVO einzuhalten;
- Festlegung des Standards für die Datenübermittlung an das ePD, inkl. Verschlüsselung;

[191] Vgl. auch den Anforderungskatalog für Lieferanten und Leistungserbringer gemäss EDPV-EDI, Anhang 2, Ziff. 4.9.4.

– Meldepflichten bei Verletzungen der Datensicherheit;

– App-Nutzer als Drittbegünstigte der Datenschutzversprechen des Anbieters (Vertrag zu Gunsten Dritter);

– Haftung und ggf. auch Konventionalstrafen bei Datenschutzverletzungen;

– Ausserordentliches Kündigungsrecht im Falle von Verstössen gegen den Datenschutz;

– Anwendung schweizerischen Rechts; Gerichtsstand Schweiz.

182 Mit diesem Instrument lässt sich somit auch absichern, dass schweizerisches Recht zur Anwendung kommt und im Streitfall ein schweizerisches Gericht zuständig ist. Bei Verstössen gegen die datenschutzrechtlichen Vorgaben steht als Sanktion ein Ausschluss der mHealth App vom ePD zur Verfügung. Eine spezifische gesetzliche Grundlage für die Umsetzung dieser Massnahme ist nicht erforderlich.

5.4. Schutz der Endnutzer vor missbräuchlicher Datenbearbeitung

5.4.1. Präventiver Charakter der vorgeschlagenen Massnahmen

183 Der Datenschutz baut in erster Linie darauf, dass sich die Rechtsunterworfenen an die rechtlichen Vorgaben halten. Die abschreckende Wirkung von Sanktionen sowie die öffentliche Prangerwirkung von Datenschutzverstössen tragen zur Compliance bei.

184 Im vorliegenden Kontext wird der Schutz vor Missbrauch denn auch in erster Linie durch präventive Massnahmen erreicht. Anbieter, welche die grundlegendsten Prinzipien des Datenschutzes nicht beachten, sollen gar nicht erst in den Genuss kommen, dass ihre mHealth Apps im Kontext des ePD genutzt werden. Die Sensibilisierung der Bevölkerung für den Datenschutz im mHealth-Bereich ist ebenfalls eine präventive Massnahme.

185 Den Endnutzern stehen zwar durchaus auch Rechtsbehelfe zur Verfügung, mit denen sie ihre persönlichen Schutzinteressen durchsetzen können, doch ist vor allem der zivilrechtliche Klageweg für den einzelnen teuer und aufgrund der über weite Strecken beim Kläger liegenden Beweislast auch mit Risiken verbun-

den. Dennoch werden die reaktiven Rechtsbehelfe der Nutzer nachstehend dargelegt.

5.4.2. Reaktive Interventionsmöglichkeiten

5.4.2.1. Zivilrechtliche Klagebefugnisse

186 Datenschutz im Privatbereich ist Persönlichkeitsrecht. Den betroffenen Personen stehen zunächst verschiedene Rechtsbehelfe aus dem Datenschutzgesetz zu:

- Das Recht auf **Auskunft** über die bearbeiteten Daten, einschliesslich Angaben über die Herkunft der Daten, den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, der an der Datensammlung Beteiligten und der Datenempfänger (Art. 8 Abs. 1 und 2 DSG);

- Das Recht auf **Berichtigung** unrichtiger Daten (Art. 5 Abs. 2 DSG);

- Das Recht auf **Löschung** widerrechtlich bearbeiteter Daten (Art. 15 Abs. 1 DSG). Ein Recht auf Löschung für in der Vergangenheit rechtmässig erhobene Daten gewährt das Datenschutzgesetz zwar nicht, doch kann eine betroffene Person gestützt auf das Widerspruchsrecht (Art. 12 Abs. 2 lit. b DSG) dennoch jederzeit die Löschung ihrer Personendaten verlangen[192], wobei bei Persönlichkeitsverletzungen in der Regel ein materieller Schaden schwer darzulegen ist.

187 Weitere Ansprüche ergeben sich aus dem Zivilgesetzbuch (**ZGB**), namentlich das Recht, eine drohende Verletzung zu verbieten (Sperrung der Datenbearbeitung, Verbot der Datenbekanntgabe an Dritte) oder die Widerrechtlichkeit einer Verletzung gerichtlich feststellen zu lassen, wenn sich diese weiterhin störend auswirkt (Art. 15 Abs. 1 DSG i.V.m. Art. 28a Abs. 1 ZGB). Schliesslich stehen dem Verletzten auch reparatorische Ansprüche (Schadenersatz, Genugtuung, Herausgabe des Verletzergewinns) zu (Art. 28a Abs. 3 ZGB).

188 Eine in der Datenschutzpraxis bislang soweit ersichtlich nicht genutzte Klagemöglichkeit ist das Verbandsklagerecht nach Art. 89 der Zivilprozessordnung

192 ROSENTHAL (Fn. 141), Art. 12 DSG N 32.

(**ZPO**).[193] Vereine und andere Organisationen von gesamtschweizerischer oder regionaler Bedeutung, die nach ihren Statuten zur Wahrung der Interessen bestimmter Personengruppen befugt sind, können in eigenem Namen auf Verletzung der Persönlichkeit der Angehörigen dieser Personengruppen klagen. Somit könnten bspw. Patientenschutzorganisation von diesem Kollektivklagerecht Gebrauch machen.

189 Die internationale Zuständigkeit in der Schweiz ist in der Regel gegeben; entgegenstehende Gerichtsstandsvereinbarungen sind im Verhältnis zu Konsumenten unwirksam.[194]

5.4.2.2. Strafantrag

190 Das Strafrecht führt im Datenschutzgesetz ein Schattendasein. Im revidierten Datenschutzgesetzt ist der Strafkatalog stark ausgebaut und enthält bspw. auch eine Strafsanktion bei Verletzung der Datensicherheit oder der Verletzung der Pflichten zu Privacy by Design oder Privacy by Default (Art. 51 Abs. 1 lit. c und e E-DSG). Darüber hinaus können auch Straftatbestände ausserhalb des Datenschutzgesetzes relevant sein.[195]

191 Die in Frage kommenden Straftatbestände sind meistens als Antragsdelikte ausgestaltet, weshalb die betroffene Person einen Strafantrag stellen muss, damit die Tat verfolgt wird. Hierbei sind die Antragsfristen zu beachten: Das Antragsrecht erlischt gemäss Art. 31 StGB[196] nach Ablauf von drei Monaten. Die Frist beginnt mit dem Tag, an welchem der antragsberechtigten Person der Täter bekannt wird.

192 Eine Strafsanktion richtet sich in der Regel gegen die natürliche Person, welche die Tat begangen hat. Dies ist denn auch die grosse Schwäche des Strafrechts als Sanktionsinstrument für Datenschutzverletzungen, sowohl aus Sicht des Täters wie auch aus Sicht des Opfers. In der Regel steht eine Organisation als Verantwortliche hinter einer Datenschutzverletzung, und diese sollte dementsprechend auch sanktioniert werden.

193 Im internationalen Kontext ist ein Strafanspruch auch dann gegeben, wenn der Erfolg einer im Ausland verübten Straftat in der Schweiz eintritt; die Tat gilt

193 Vgl. dazu eingehend ROSENTHAL DAVID, *in:* PASSADELIS/ROSENTHAL/THÜR, Datenschutzrecht, Basel 2015, Rn. 7.14 f.
194 Vgl. vorstehend, Rz. 110 ff.
195 Übersicht bei ROSENTHAL (Fn. 193), Rn. 7.43 ff.
196 Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0.

dann in der Schweiz als begangen (Art. 3 Abs. 1 i.V.m. Art. 8 Abs. 1 StGB).[197] Eine Vollstreckung der Busse im Ausland dürfte allerdings in der Regel scheitern, wenn es an einer Strafbarkeit der Tat am Aufenthaltsort des Täters fehlt (Grundsatz der beidseitigen Strafbarkeit).[198]

5.4.3. Anzeige an die Datenschutzaufsicht

194 Schliesslich kann die betroffene Person Datenschutzverletzungen auch der zuständigen Behörde melden. Dies kann der EDÖB, aber auch eine Datenschutzaufsichtsbehörde im Ausland sein, wenn eine solche am Sitz des Anbieters existiert.

195 Gemäss Art. 29 Abs. 1 DSG klärt der EDÖB den Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler). Solche Abklärungen können zunächst in eine Empfehlung münden (Art. 29 Abs. 3 DSG). Wird die Empfehlung vom Datenbearbeiter nicht befolgt, kann der EDÖB Klage beim Bundesverwaltungsgericht einreichen (Art. 29 Abs. 4 DSG).

196 Die Sachverhaltsabklärung des EDÖB ist die schärfste reaktive Waffe des Datenschutzgesetzes. Sie zeigt auch gegenüber multinationalen Unternehmen Wirkung, wie bspw. das „*Google Street View*"-Verfahren gezeigt hat.[199] Eine Kompetenz für Sachverhaltsabklärungen des EDÖB in der Schweiz ist auch dann gegeben, wenn die Datenbearbeitungen hauptsächlich im Ausland stattfinden, sofern ein genügender Bezug zur Schweiz erstellt ist.[200]

197 Die Anbieterlandschaft im mHealth-Bereich ist sehr zersplittert. Die Unternehmen weisen daher nicht die kritische Grösse und eine entsprechende Marktstellung in der Schweiz auf, welche genügen würde, damit eine Sachverhaltsabklärung des EDÖB ihre abschreckende Wirkung entfalten könnte. Es ist denkbar, dass sich Anbieter um eine solche Sachverhaltsabklärung foutieren und ihr Angebot nötigenfalls vom schweizerischen App Store-Portal entfernen würden.

---

197 Vgl. BURGA SABRINA, La télémédecine et le droit suisse Analyse au regard du droit contractuel, de la Loi fédérale sur la protection des données, de la responsabilité civile et des assurances sociales, Diss. Neuchâtel, Basel 2012, Rn. 721; im DSG finden sich keine Bestimmungen zum räumlichen Anwendungsbereich der Strafnormen, weshalb nach Art. 333 StGB die Bestimmungen des StGB Anwendung finden.

198 Vgl. hierzu für die Schweiz Art. 94 I lit. b IRSG (Bundesgesetz über internationale Rechtshilfe in Strafsachen, SR 351.1); andere Staaten kennen diesen Grundsatz auch.

199 BGE 138 II 346 – *Google Street View*.

200 BGE 138 II 346, E. 3.3 – *Google Street View*.

198 Mit Inkrafttreten des revidierten Datenschutzgesetzes wird die Untersuchungskompetenz des EDÖB konzeptionell beibehalten. Inskünftig wird er aber nicht nur bei Systemfehlern, sondern bei jeden Verdacht auf gesetzeswidrige Datenbearbeitung aktiv werden dürfen (Art. 41 Abs. 1 E-DSG). Gleichwohl ist absehbar, dass der Umfang solcher Untersuchungen aufgrund der begrenzten Ressourcen des EDÖB nicht merklich zunehmen wird.

199 Die Untersuchungskompetenz des EDÖB ist ein wirksames Instrument gegenüber global tätigen Grossunternehmen, die auf ihre Reputation achten und für welche die Schweiz ein wichtiger Markt ist. Dies ist bei zahlreichen Anbietern im mHealth-Bereich vorläufig nicht der Fall, könnte sich aber ändern. Aufgrund der strengeren Datenschutz- und Medizinprodukteregulierung in der EU dürfte auf diesem Markt voraussichtlich in näherer Zukunft ohnehin eine Flurbereinigung stattfinden. Die Bestrebungen der Anbieter, mit den Anforderungen der DSGVO kompatibel zu sein, werden auch auf die Schweiz durchschlagen.

5.4.4. Auswirkungen auf den Massnahmenkatalog

200 Die Darstellung der Schutzmechanismen für die Endnutzer unterstreicht die Bedeutung der präventiven Massnahmen. Eine Stärkung der Rechte der betroffenen Personen im Sinne einer Beweislastumkehr bei Datenschutzverletzungen oder einem Ausbau der Kompetenzen des EDÖB dürfte politisch chancenlos sein.[201] Trotz der hohen Hürden für den individuellen Rechtsschutz ist die Durchsetzung des Datenschutzes gegen global tätige Unternehmen aber nicht illusorisch.[202] In der Schweiz hat dies das *Google Street View*-Verfahren gezeigt, in der EU hat ein einzelner Datenschutzaktivist das Safe Harbour-Framework zwischen der EU und den USA zu Fall gebracht.[203]

Stand Gesetzgebung, Literatur und Rechtsprechung: 30. November 2017

[201] Vgl. Botschaft E-DSG (Fn. 146), 6984 f.

[202] Vgl. Stellungnahme des Bundesrates vom 16. August 2017 auf die Interpellation Schwab: Lassen sich die Internetgiganten mit den heutigen rechtlichen Sanktionen bändigen?, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173277 (zuletzt besucht am 9. Oktober 2017).

[203] EuGH, 6. Oktober 2015, Rs. C‑362/14 – *Maximilian Schrems ./. Data Protection Commissioner*.