Mobile Health Apps

Datenschutzrechtliche Grundsatzfragen

Alles App – healthy, happy, haltbar? Chancen, Risiken und Nebenwirkungen von Mobile Health aus Sicht des Rechts

Law & Robots Workshop 2019
Juristische Fakultät der Universität Basel, 6. Juni 2019

Michael Isler

walderwyss rechtsanwälte

Hell or Heaven?

«For us to reap the benefits of artificial intelligence, we need to make data sharing simpler.»

Luke Miner, For a Longer, Healther Life, Share Your Data
New York Times, 22. Mai 2019

«Zu viel Ungerechtigkeit zeichnete unser bisheriges Gesundheitssystem aus. Die Kosten für die Behandlungen sogenannter unkooperativer Teile der Gesellschaft, die mutwillig Schuld an ihrem Gesundheitszustand tragen, verteilt auf die Schultern des kleinen Mannes.»

Thomes Vater, in: Sibylle Berg, GRM

Hell or Heaven?

«Versicherte sollen belohnt werden, welche nachweislich Massnahmen zur Erhaltung ihrer Gesundheit treffen (z. B. Schrittzähler, regelmässige Blutdruckmessung) und die Daten in ihr elektronisches Patientendossier (EPD) einstellen, sofern sie dies wollen und dies im Rahmen einer besonderen Versicherungsform wählen.»

Motion Humbel, Elektronisches Patientendossier nutzen für Anreize zu gesundheitsbewusstem Verhalten, 27. September 2018

Übersicht

- Mobile Health Apps – Elemente einer Datenschutzfolgenabschätzung
- Die wichtigsten Bearbeitungsgrundsätze im Kontext von Mobile Health
  - Transparenz und Einwilligung
  - Zweckbindung
  - Privacy by Design
- Einbindung von Mobile Health in das Gesundheitssystem
  - Obligatorische Krankenpflegeversicherung (BVGer A-3548/2018 – «Helsana+ App»)
  - Elektronisches Patientendossier (Automatisierte Datenbereitstellung)
- Vier Thesen für einen wirksameren Datenschutz im Bereich von Mobile Health

Mobile Health Apps – Elemente einer Datenschutzfolgenabschätzung

Leistungserbringer

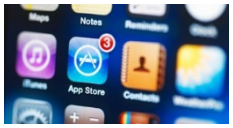
KIS

EPD
elektronisches
Patientendossier

Übermitt-
lungsnetz

App-Service
Plattform

App Store



Mobilgerät und
Betriebssystem

Patient

Mobile Health Apps – Elemente einer Datenschutzfolgenabschätzung

Hauptsächliche Risiken:

– **Diskriminierung** aufgrund medizinischer Prädisposition oder Lebensweise

– Verlust der **informationellen Selbstbestimmung** infolge subtiler Verhaltenssteuerung und Manipulation

– Selbstentblössung bei **Datenschutzverletzungen**

– **Kontrollverlust** wegen unerwünschter Weiter-bearbeitungen oder Verknüpfungen von Vitaldaten

Ursachen:

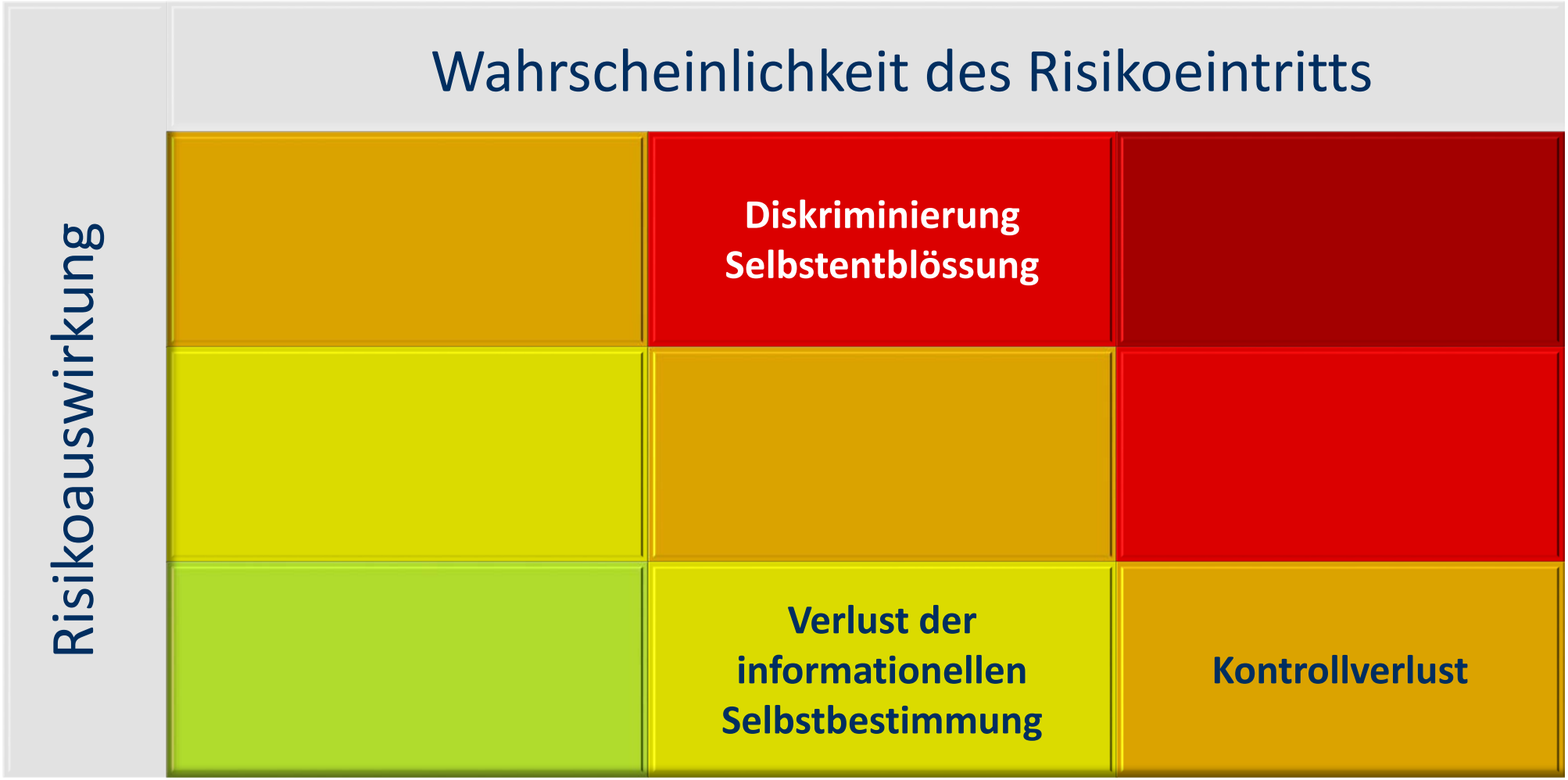
- Innerer Zwang zur **Selbst-vermessung** («Quantified Self»)

- Hoher ökonomischer und wissenschaftlicher **Wert der Daten**

- Komplexität des **App-Ökosystems** mit zahlreichen Daten-übergabepunkten

- **Gratiskultur** und amateurhafte Programmierung

Mobile Health Apps – Elemente einer Datenschutzfolgenabschätzung



Bearbeitungsgrundsätze
Transparenz und Einwilligung

*«Prior to or as soon as users install your app, you must obtain their **free**, **specific** and **informed** consent in order to process their data for the **purposes you have described** to them.»*

Draft Code of Conduct on privacy for mobile health applications

Bearbeitungsgrundsätze Transparenz und Einwilligung

- Einwilligung als Gold-Standard?
  - Für die Bearbeitung von Gesundheitsdaten ist nach Art. 9 Abs. 2 DSGVO kaum eine andere Berechtigungsgrundlage als die **ausdrückliche** Einwilligung «für einen oder mehrere **festgelegte Zwecke**» denkbar (lit. a).
  - Ausnahmen bei:
    - Bearbeitung zum Zweck der **Prävention, Diagnose oder Behandlung**, sofern gesetzliche Grundlage oder Vertrag mit einer der Geheimhaltung unterstehenden Gesundheitsfachperson besteht (lit. h).
    - Bearbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats für im öffentlichen Interesse liegende **Archivzwecke**, für wissenschaftliche oder historische **Forschungszwecke** oder für **statistische Zwecke** (lit. j).

Bearbeitungsgrundsätze Transparenz und Einwilligung

- Zweifel sind angebracht:
  - Einwilligung muss **vor Aufnahme der Bearbeitung** erteilt werden und erfolgt daher zu einem Zeitpunkt, in dem die Tragweite der Einwilligung in der Regel nicht abgeschätzt werden kann.
  - Kenntnis der Bearbeitungszwecke durch die betroffene Person bleibt eine **Fiktion**.
  - Ausnahme von lit. h führt dazu, dass sich App-Betreiber aus der Verantwortung stehlen, indem sie eine Gesundheitsfachperson vorschalten und sich selbst in die **Rolle des Auftragsverarbeiters** zurückstufen.

Bearbeitungsgrundsätze
Zweckbindung

*«Any processing of personal data must be **compatible with the purposes** for which you originally collected the data, **as communicated to the users** of your app.»*

Draft Code of Conduct on privacy for mobile health applications

Bearbeitungsgrundsätze Zweckbindung

- Zweckbindung ist ein Gebot der **Fairness**.
- **Forschungsprivileg** für sekundäre Bearbeitungszwecke:
  - Bearbeitung von Personendaten zu nicht personenbezogenen Zwecken in der Forschung, Planung und Statistik (**Rechtfertigungsgrund** nach Art. 13 Abs. 2 lit. e DSG).
  - Weiterverarbeitung für Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (**Relativierung der Zweckbindung** nach Art. 5 Abs. 1 lit. b DSGVO), unter Einhaltung angemessener organisatorischer und technischer Massnahmen gemäss Art. 89 Abs. 1 DSGVO.
- **Marketingprivileg**:
  - Opt-out-Lösung (Art. 21 Abs.2 DSGVO).
  - Darf bei Widerspruch die Nutzung der App unterbunden werden?

Bearbeitungsgrundsätze
Privacy by Design

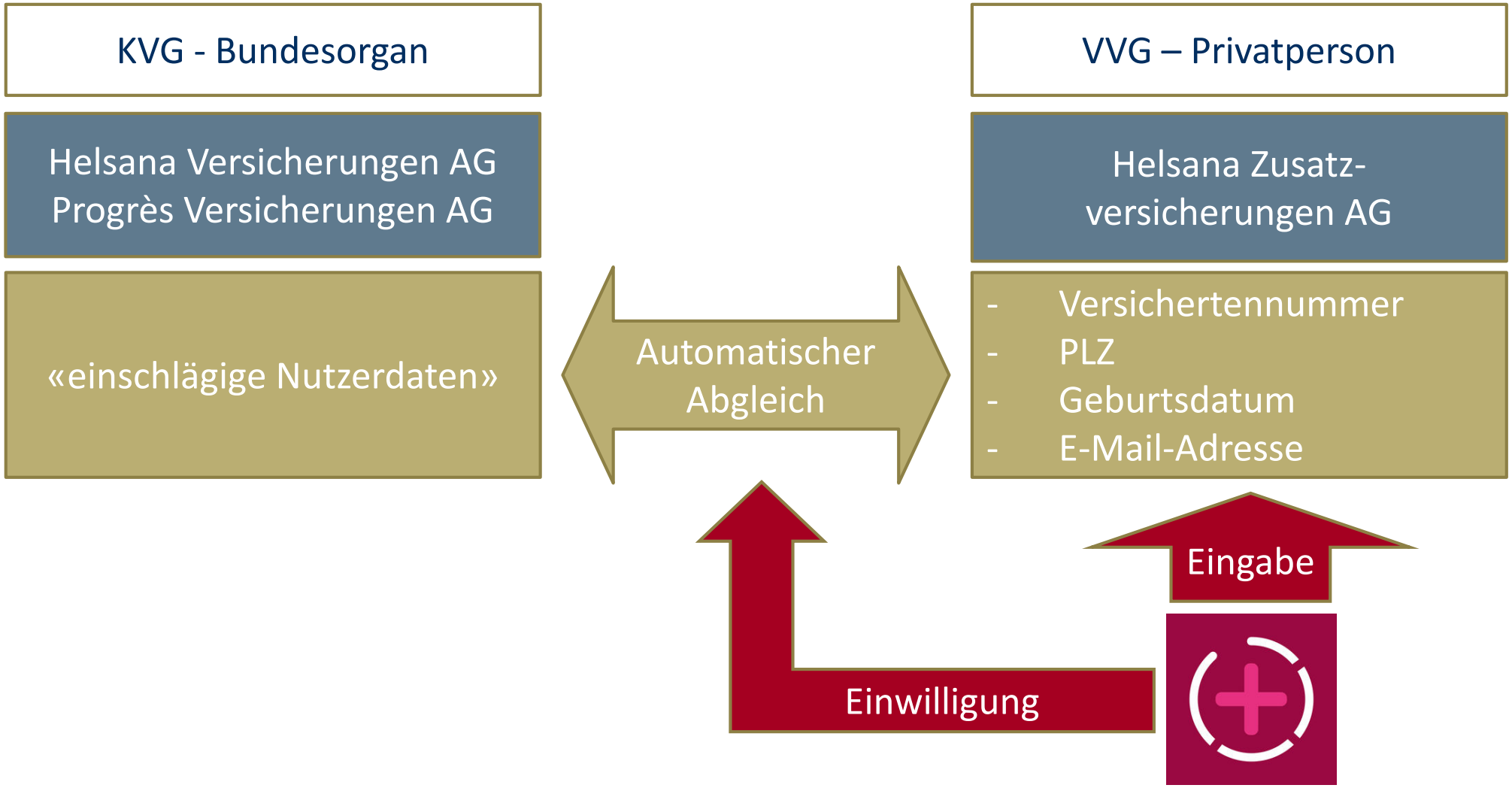
*«Privacy by design means that the privacy implications of your app and its use have been considered **at each step of its development**, and that you have made design and implemented choices that will **support the privacy** of your users wherever possible.»*

Draft Code of Conduct on privacy for mobile health applications

Bearbeitungsgrundsätze Privacy by Design

- Verpflichtung, im **Planungs- und Verarbeitungsstadium** die erforderlichen Massnahmen vorzusehen, um die Datenschutzgrundsätze einzuhalten (Art. 25 Abs. 1 DSGVO).
- Würdigung:
  - Systemdatenschutz schafft **Vertrauen** in neue Technologien.
  - Adressat ist Verantwortlicher für die Datenbearbeitung, **nicht App-Entwickler**. Der regulierende Eingriff erfolgt **zu spät**.
  - ErwG 78 DSGVO: *«[D]ie Hersteller der Produkte, Dienste und Anwendungen [sollten] **ermutigt werden**, das Recht auf **Datenschutz bei der Entwicklung und Gestaltung** der Produkte, Dienste und Anwendungen **zu berücksichtigen** und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen»*.

Mobile Health im Gesundheitssystem BVGer A-3548/2018 («Helsana+ App»)



Mobile Health im Gesundheitssystem BVGer A-3548/2018 («Helsana+ App»)

- Rechtmässigkeit der Datenbearbeitung (Art. 4 Abs. 1 DSG):
  - Prinzip der Einheitsprämie (Art. 61 Abs. 1 KVG).
  - Unzulässige Rückerstattung von Grundversicherungsprämien als «Entgelt» für Datenlieferung?
  - Eine Verletzung gesetzlicher Bestimmungen führt nur dann zur Unrechtmässigkeit einer Datenbearbeitung, wenn die verletzte Norm den Schutz der Persönlichkeit bezweckt.
- Rechtmässigkeit der Einwilligung
  - Monetärer Vorteil (Bargeldboni von max. CHF 75 pro Jahr bei nur grundversicherten Personen) bewirkt keinen unzulässigen Zwang zur Teilnahme am Helsana+ Programm.
  - Folglich keine Verletzung des Kopplungsverbots.

Mobile Health im Gesundheitssystem BVGer A-3548/2018 («Helsana+ App»)

– Globale elektronische Zustimmung in dynamischen Abgleich der Grundversicherteneigenschaft verstösst gegen das Schriftlichkeits- und Einzelfallgebot von Art. 84a Abs. 5 KVG:

Art. 84*a*[215] Datenbekanntgabe

[5] In den übrigen Fällen dürfen Daten in Abweichung von Artikel 33 ATSG an Dritte wie folgt bekannt gegeben werden:[234]

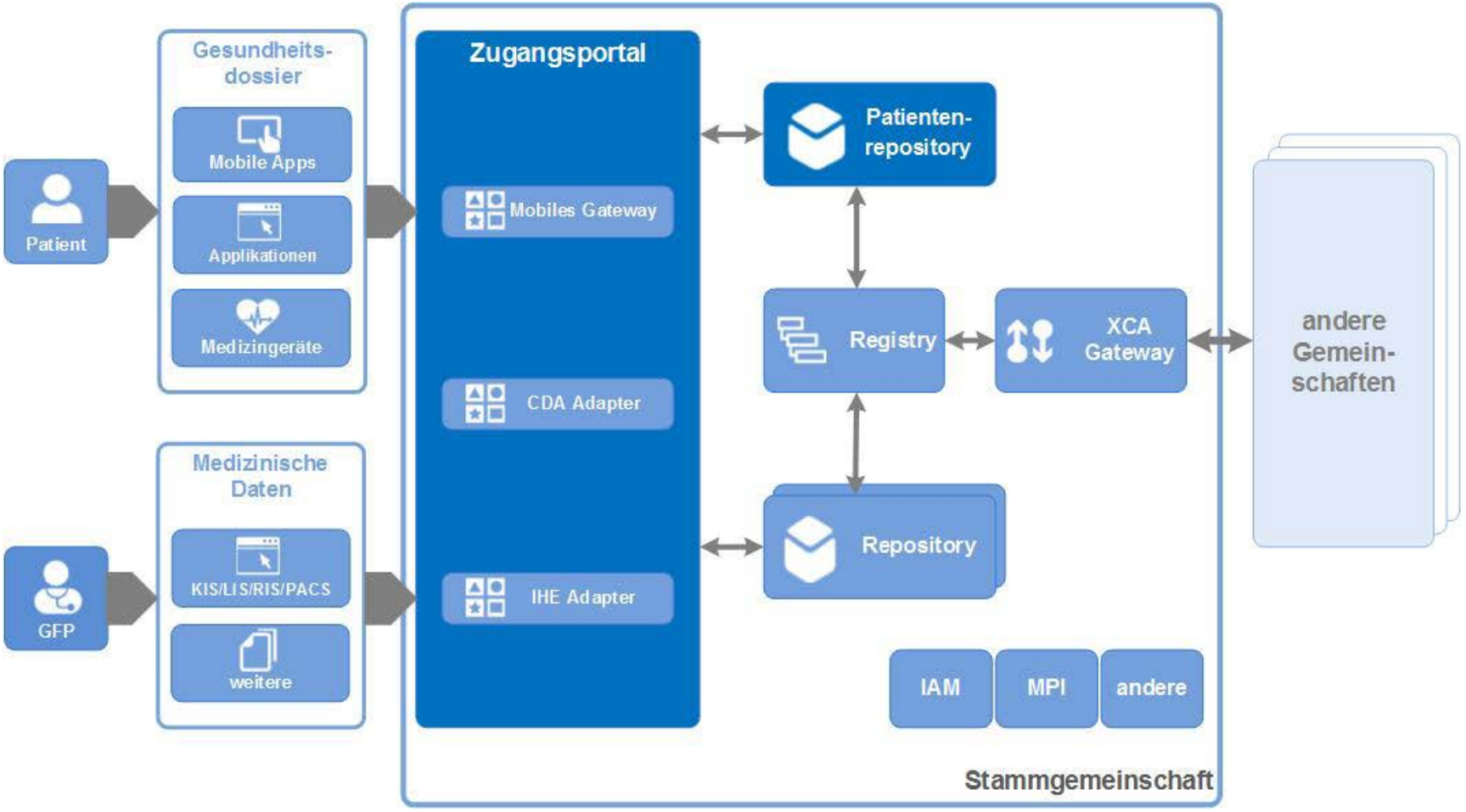
a. nicht personenbezogene Daten, sofern die Bekanntgabe einem überwiegenden Interesse entspricht;

b. Personendaten, sofern die betroffene Person im Einzelfall schriftlich eingewilligt hat oder, wenn das Einholen der Einwilligung nicht möglich ist, diese nach den Umständen als im Interesse der versicherten Person vorausgesetzt werden darf.

Mobile Health im Gesundheitssystem BVGer A-3548/2018 («Helsana+ App»)

- Was ist aus Sicht des Datenschutzes gewonnen?
  - Angebot gibt es weiterhin.
  - Hochladen der Versichertenkarte zum Nachweis der Grundversicherung als Ersatz für (ungültige) Einwilligung.
  - Zur Durchsetzung von zweckfremden Regelungszielen (Verbot der individuellen Prämienrückerstattung) ist der Datenschutz (noch) das falsche Mittel (anders aber Art. 5 Abs. 1 lit. b DSGVO: *«Personen-bezogene Daten müssen für festgelegte, eindeutige und **legitime Zwecke** erhoben werden»*).
  - Überspannte Anforderungen an die Gültigkeit von Einwilligungen bewirken eine **Flucht in alternative Berechtigungsgrundlagen** und beeinträchtigen die informationelle Selbstbestimmung.

Mobile Health im Gesundheitssystem Elektronisches Patientendossier



Quelle: HINT AG, Patientenseitige Daten im elektronischen Patientendossier, 2015

Mobile Health im Gesundheitssystem Elektronisches Patientendossier

- Speicherung der mHealth-Daten in einer **Zwischenablage** ausserhalb des Vertrauensraums.
- Überführung der Daten aus der Zwischenablage in den Vertrauensraum immer nur dann, wenn der Patient hierfür seine **Einwilligung** erteilt hat (Zwei-Faktor-Authentifizierung). Automatisierter dynamischer Transport von Vitaldaten wird dadurch verhindert.
- Ermöglichung einer ***machine-to-machine*-Authentifizierung** würde Mobile Health Apps auf Stufe von Primärsystemen heben und Einhaltung entsprechender Datenschutz- und Datensicherheitsstandards auf **hohem Schutzniveau** erfordern.
- Gewährleistung des Datenschutzes innerhalb der gesamten Verarbeitungsstrecke (**Systemdatenschutz**) als Vertrauenskapital.
- Zu viel Datenschutz ist **kontraproduktiv**: Parallele zu «Helsana+ App».

Mobile Health im Gesundheitssystem Elektronisches Patientendossier

Nr.	Massnahme
1	[…]
2	[…]
3	Ermöglichen einer **automatisierten Datenbereitstellung** durch mHealth Apps (*machine-to-machine*) unter entsprechend strengen Anforderungen an Datenschutz und Datensicherheit (bedingt Änderung auf Verordnungsstufe).
4	[…]
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.
6	Aufstellen von **Vorgaben für die vertragliche Anbindung** von mHealth Apps. Erarbeiten einer (freiwilligen) **Mustervorlage für einen Integrationsvertrag**, der die Anbindung von mHealth Apps an die ePD-Schnittstelle auf der Grundlage schweizerischen Rechts datenschutzkonform regelt.

Vier Thesen für einen wirksameren Datenschutz in Mobile Health

- Wer als mHealth App-Betreiber eine Funktion zur Verfügung stellt, soll dafür **datenschutzrechtliche Verantwortung** übernehmen, und der Einsatz von mHealth Apps im Gesundheitswesen ist an konkrete Datensicherheits-anforderungen und datenschutzrechtliche Mindeststandards zu knüpfen (**Systemdatenschutz**).
- Die Anforderungen an eine gültige **Einwilligung** in die Bearbeitung von Gesundheitsdaten sind in der Regel (zu) hoch und führen zu einer Flucht in diffuse Interessenabwägungen.
- Die Monetarisierung von Personendaten für sekundäre Bearbeitungszwecke wie Direktmarketing oder wissenschaftliche Forschung sollte enttabuisiert werden, indem bei Widerspruch eine **Zahlschranke** für die Nutzung der mHealth App eingeführt werden darf.
- Wer aufgrund seines Datenprofils personalisierte Informationen, Empfehlungen oder Entscheidungen erhält, sollte darüber in dem **Zeitpunkt** aufgeklärt werden, wenn das Ergebnis kommuniziert wird, um kontextbezogen mehr erfahren und korrigierend eingreifen zu können.

walderwyss rechtsanwälte