

# Die elektronische Patientenakte

## Datenschutzrechtliche Herausforderungen

**Dr. Philipp Siedenburg**

Schürmann Rosenthal Dreyer Rechtsanwälte

Herbstakademie 2022

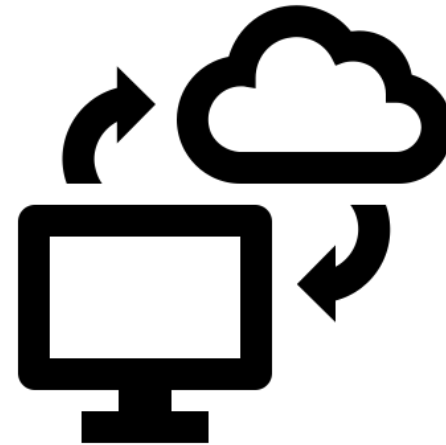
## Agenda:

- Einführung – Was ist die ePA?
- Technischer und normativer Kontext der ePA
- „Gesundheitsversorgung as a Service“ – Wie funktioniert die ePA?
- Datenschutzrechtliche Herausforderungen
- Schluss

## Einführung – Was ist die ePA?



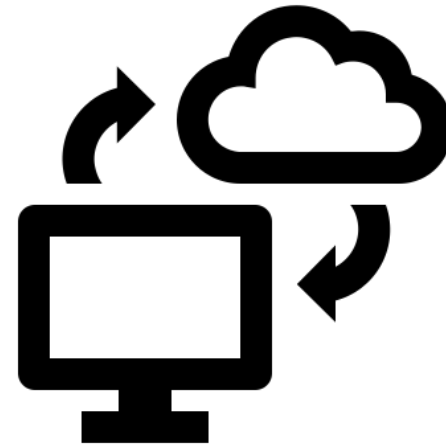
**Wichtigstes Digitalisierungsprojekt  
im deutschen Gesundheitswesen**



## Was ist die ePA?



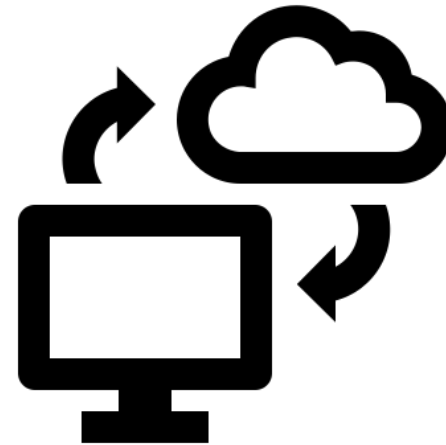
Tool zur Verbesserung der  
Informationslage in der med.  
Versorgung



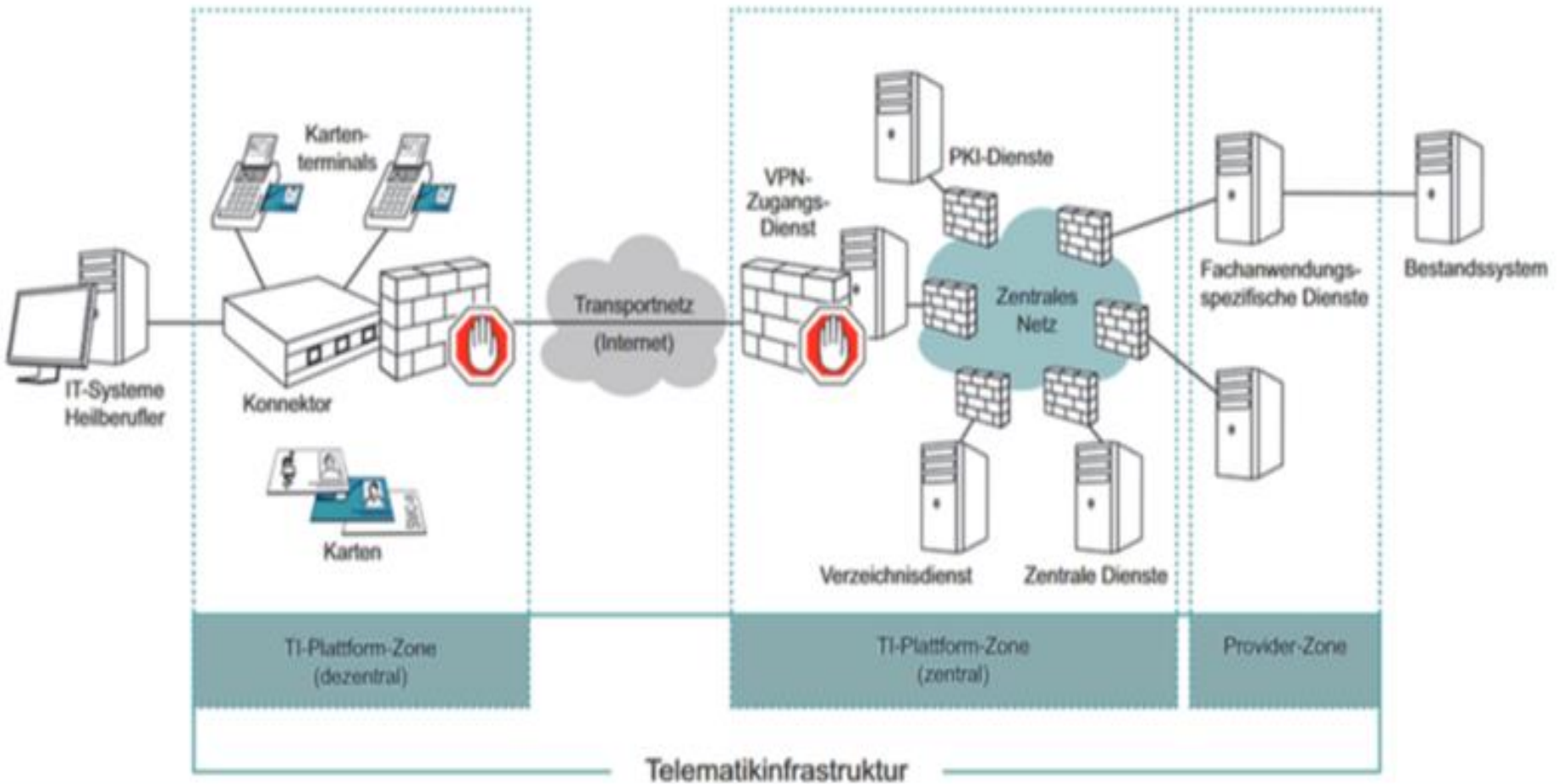
## Was ist die ePA?



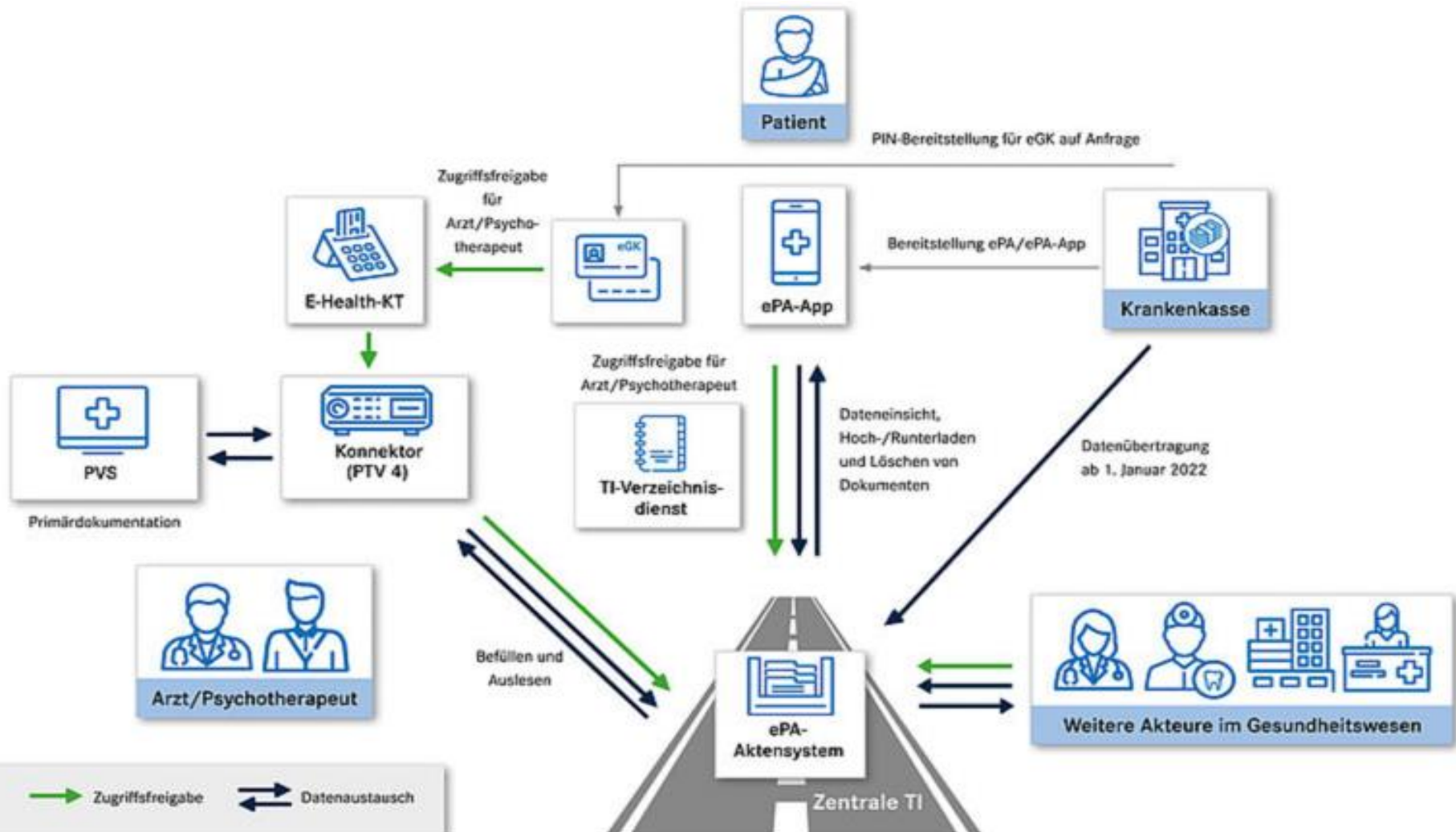
**Cloud-Speicher unter der Kontrolle  
der Patient:innen**



# Technischer Kontext: Telematikinfrastruktur



# Technischer Kontext: Telematikinfrastuktur



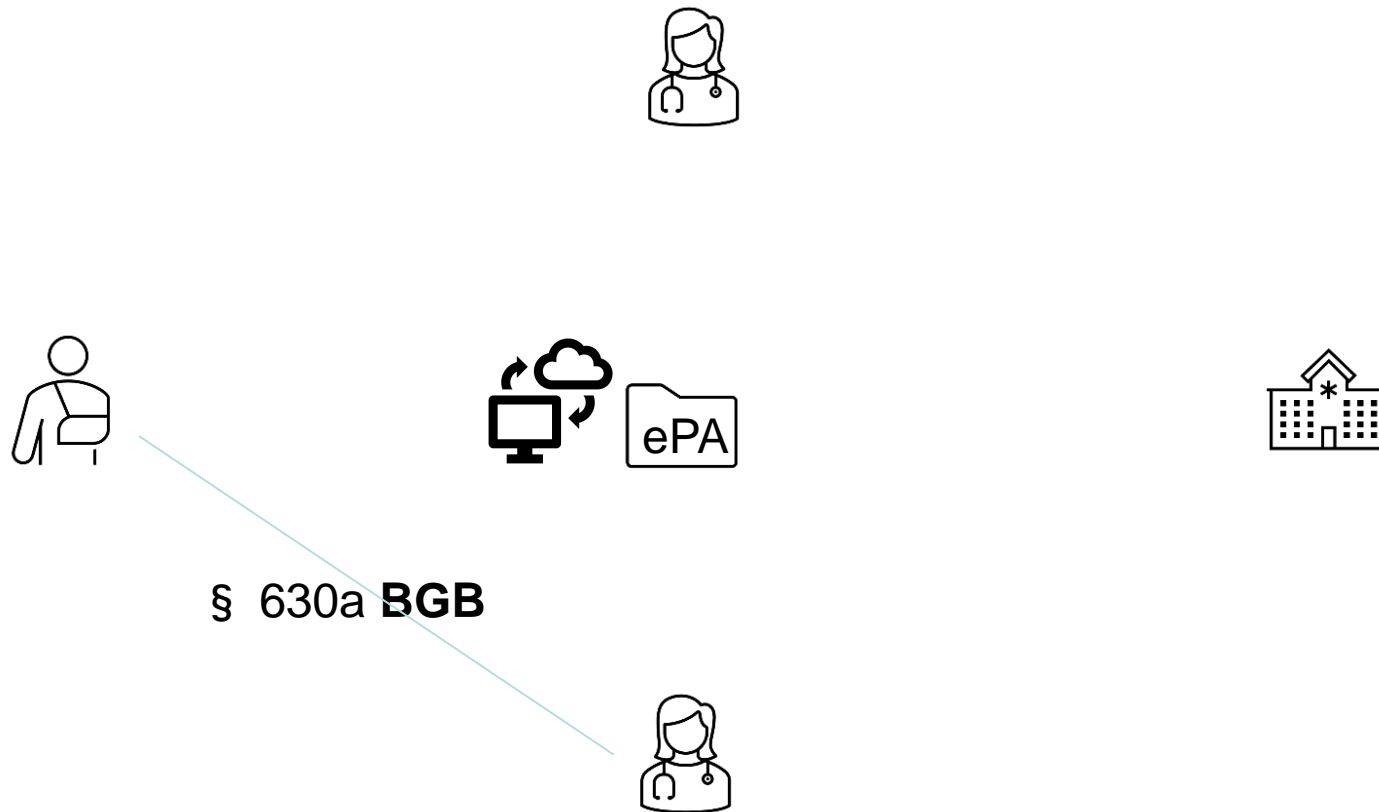
Quelle: BfArM, Telematikinfrastruktur (TI) - Ein Überblick über die Telematikinfrastruktur (TI) und die damit verbundenen Systeme und Services. (2021). Berlin: BfArM. URL: https://www.bfarm.de/SharedDocs/Pressemitteilungen/DE/2021/07/telematikinfrastruktur-ueberblick.html

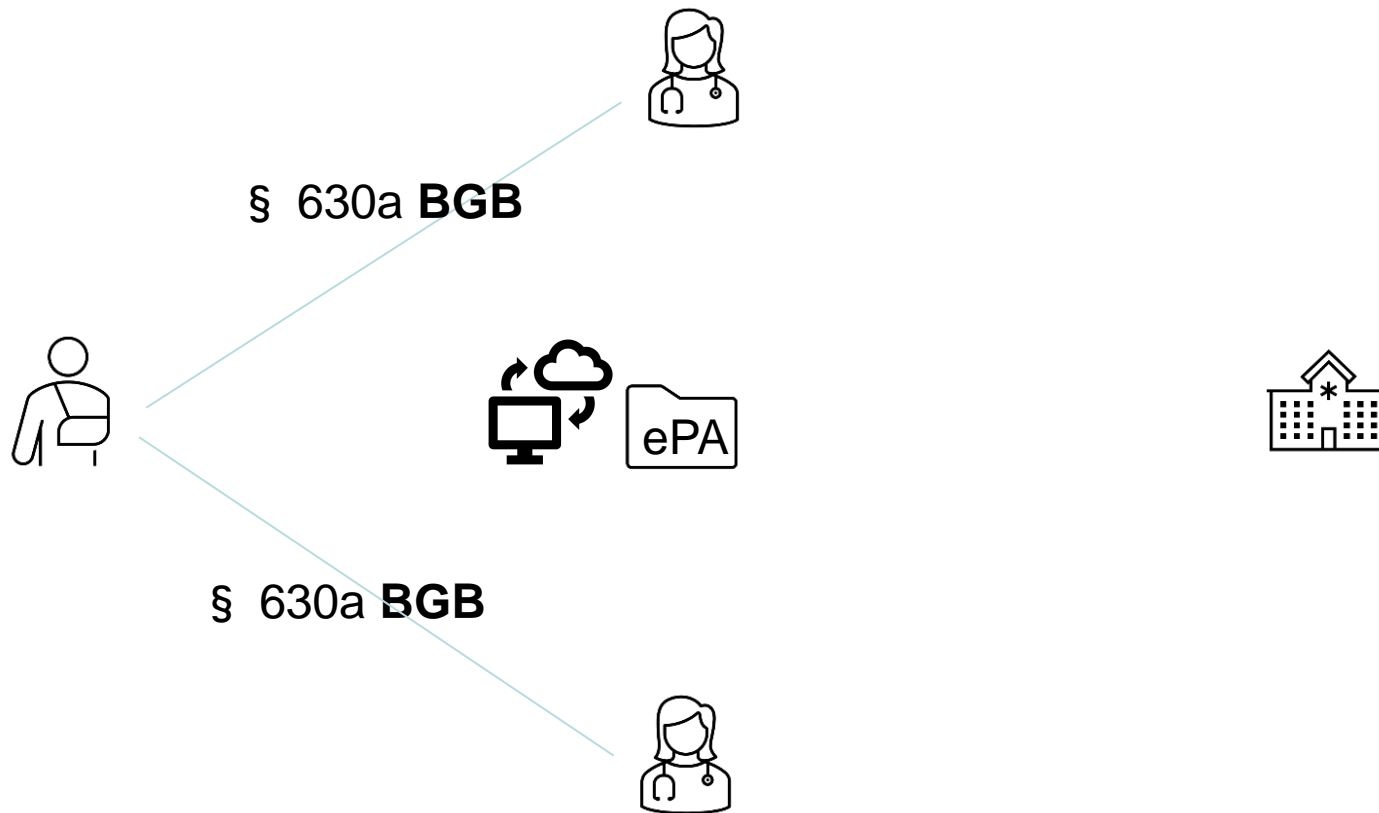
# Normativer Kontext: Behandlungsvertrag und Versicherungsverhältnis

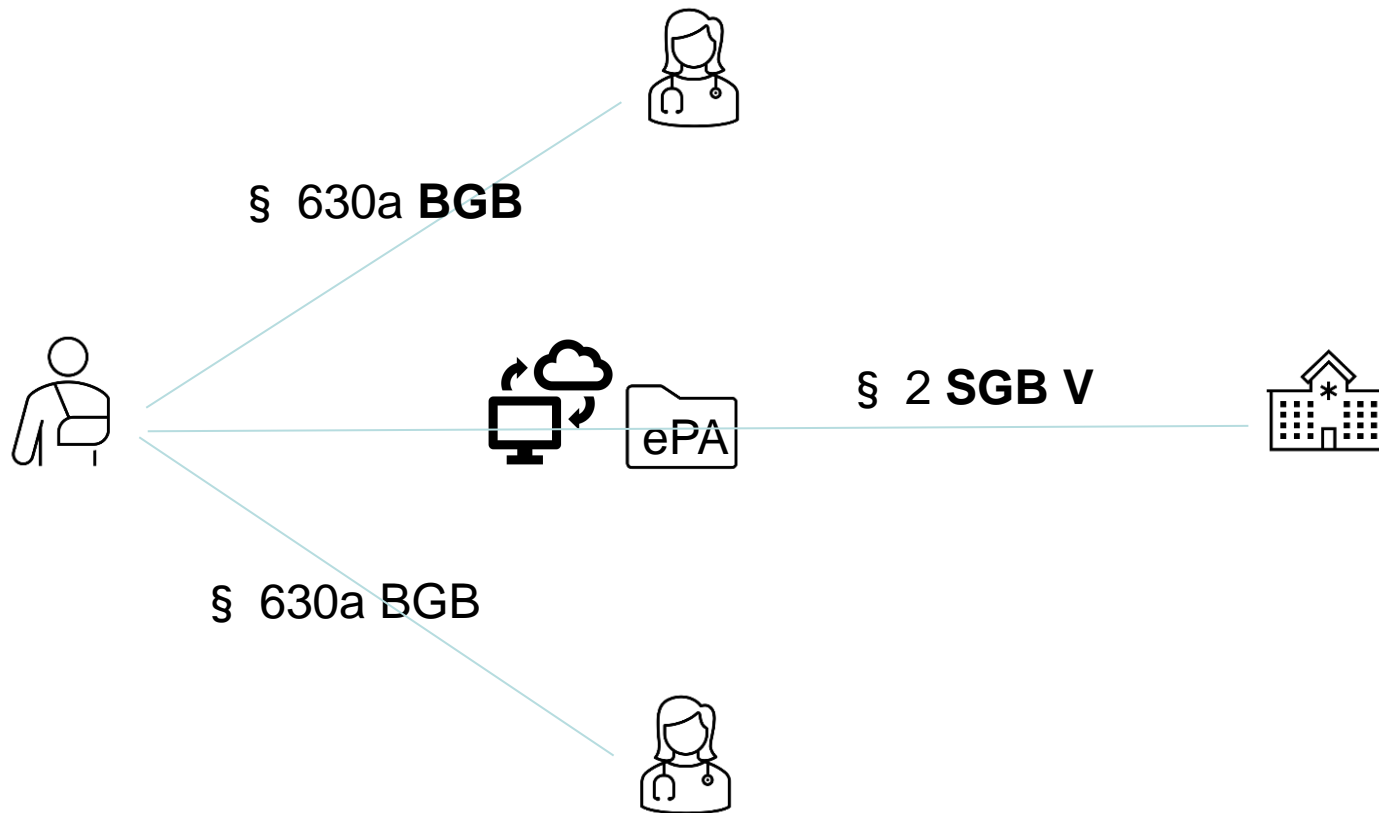


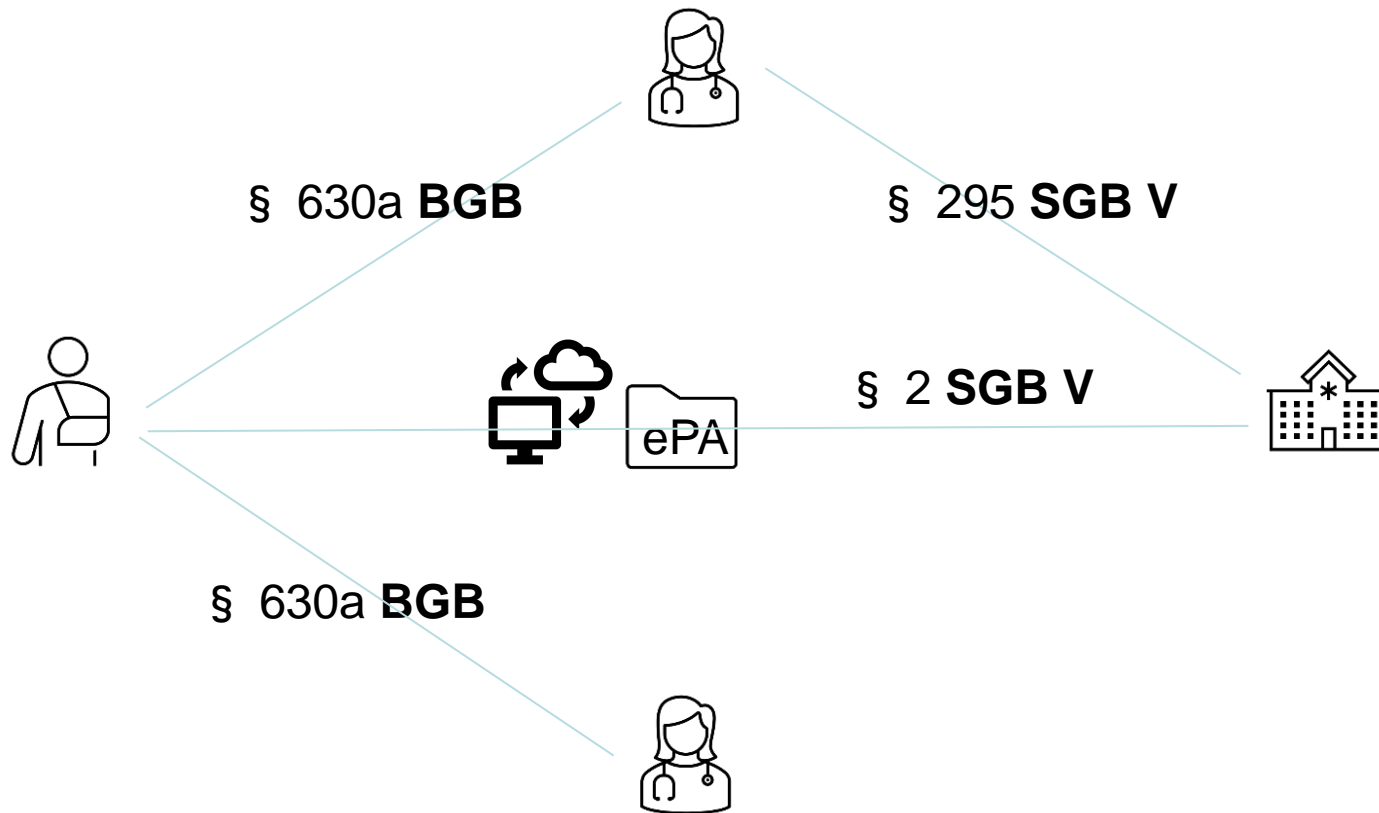


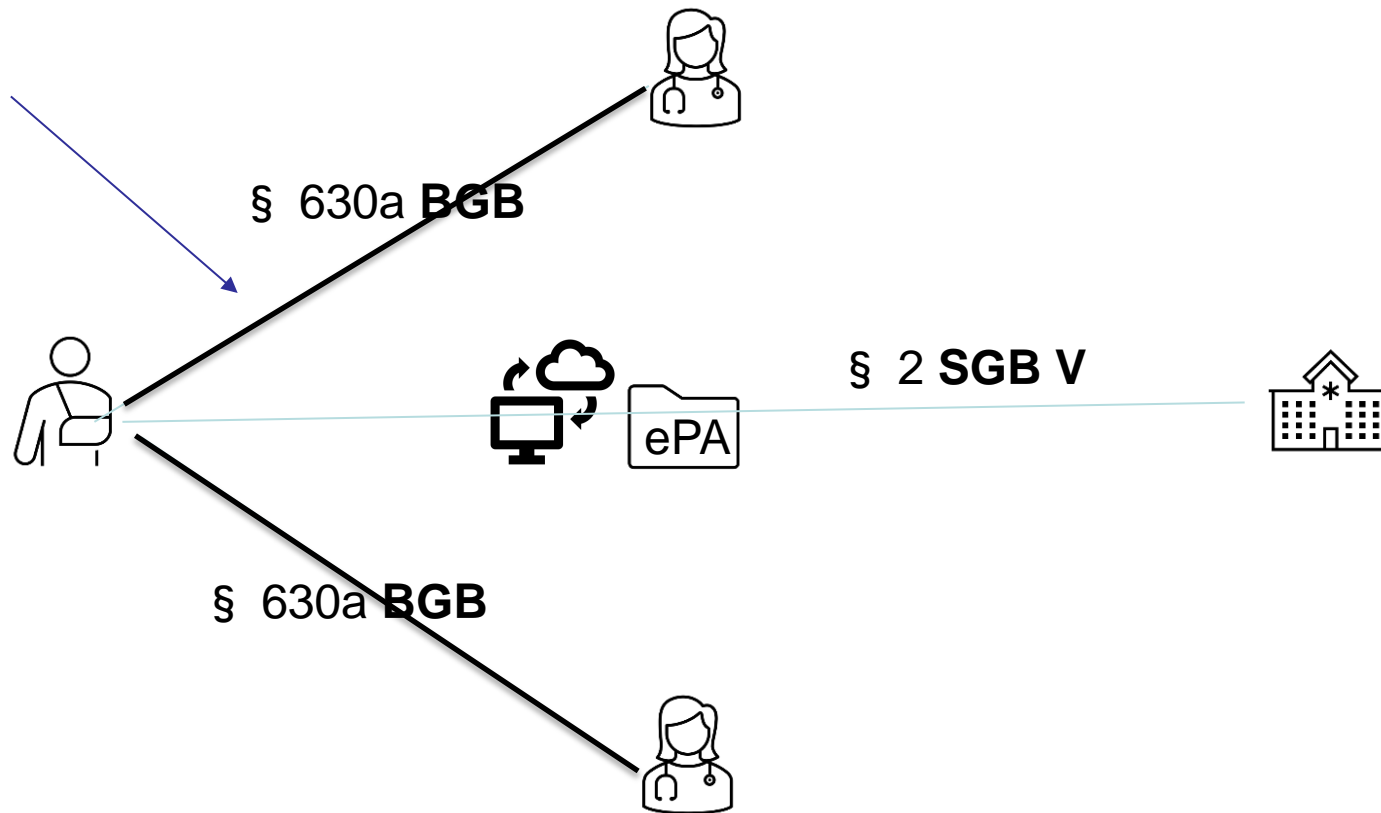
# Normativer Kontext: Behandlungsvertrag und Versicherungsverhältnis

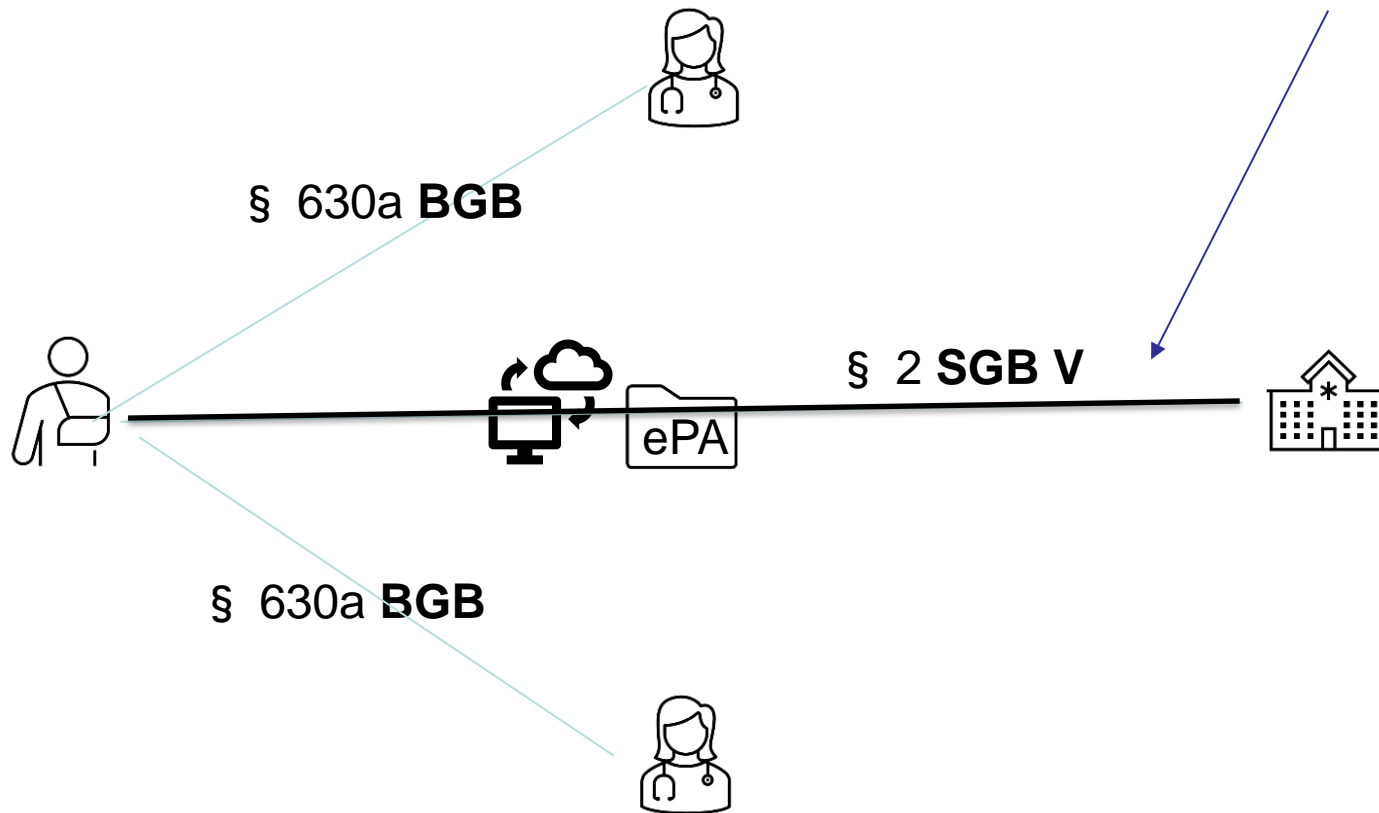


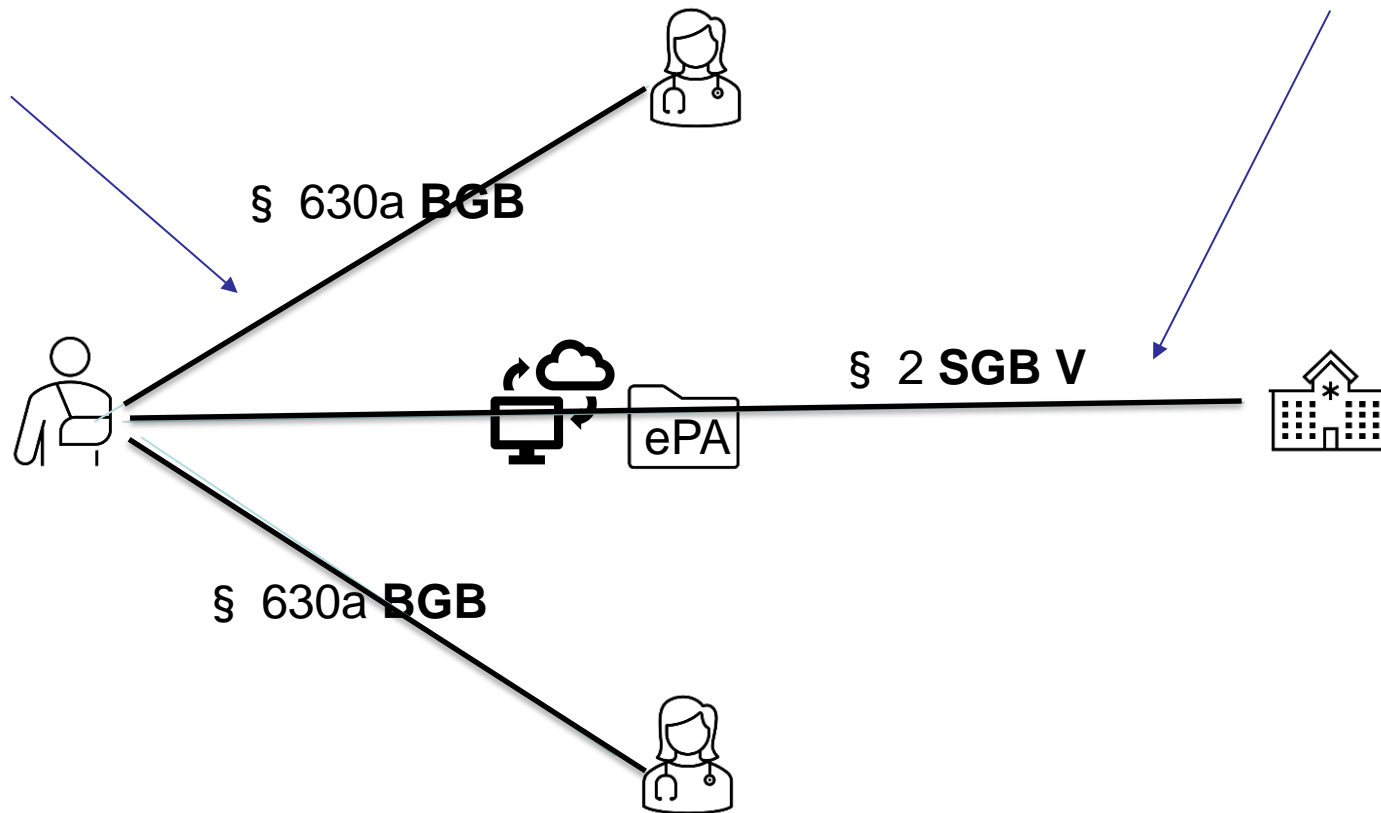










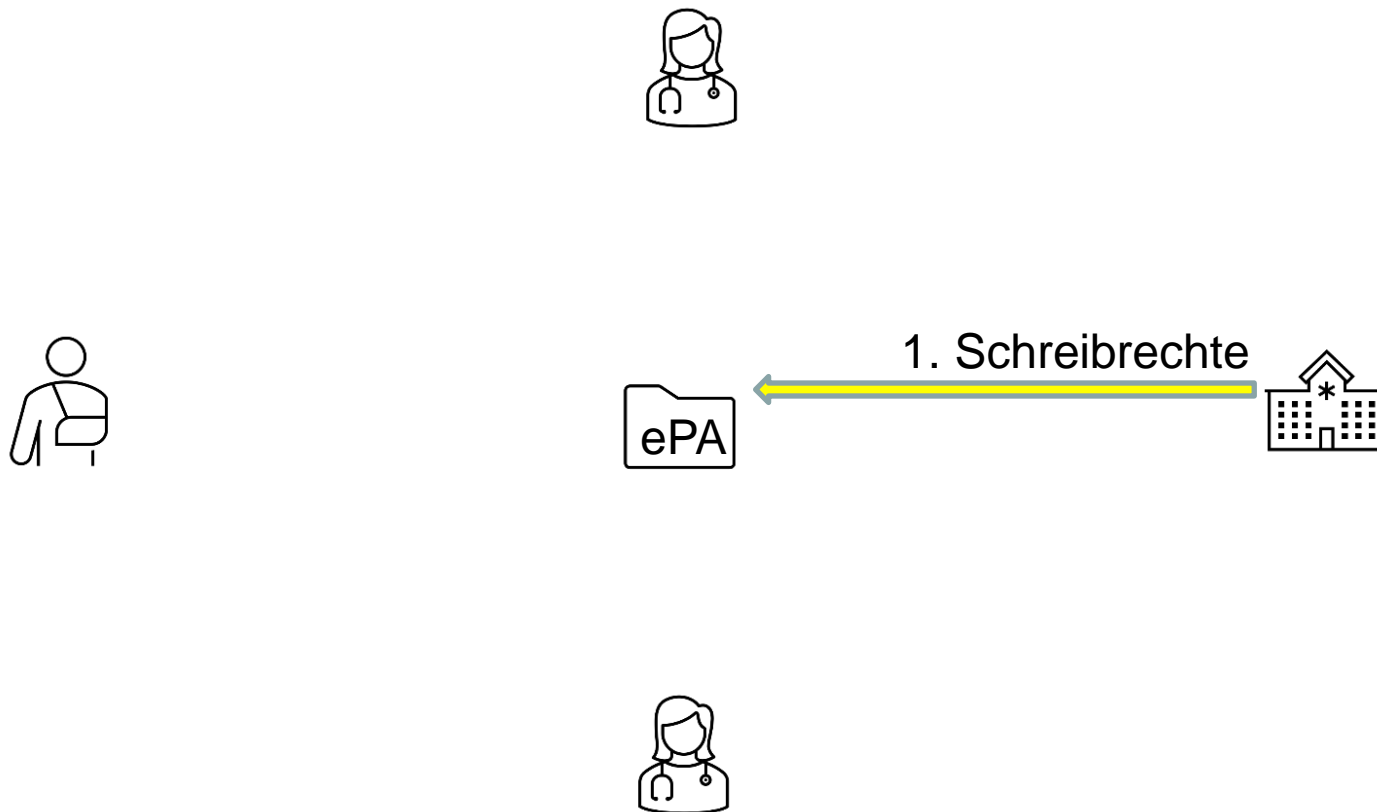


# „Gesundheitsversorgung as a Service“ – Wie funktioniert die ePA?





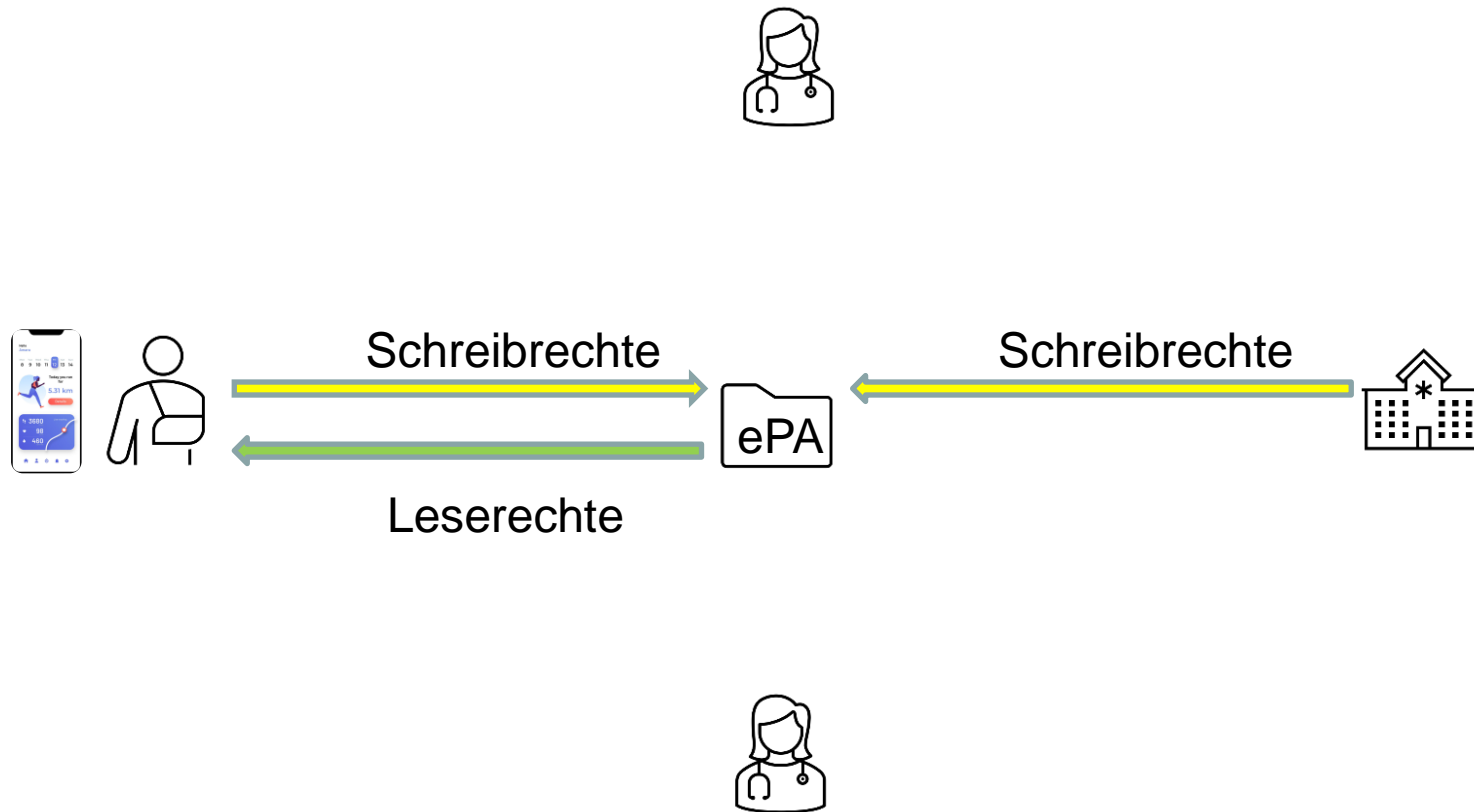
# „Gesundheitsversorgung as a Service“ – Wie funktioniert die ePA?

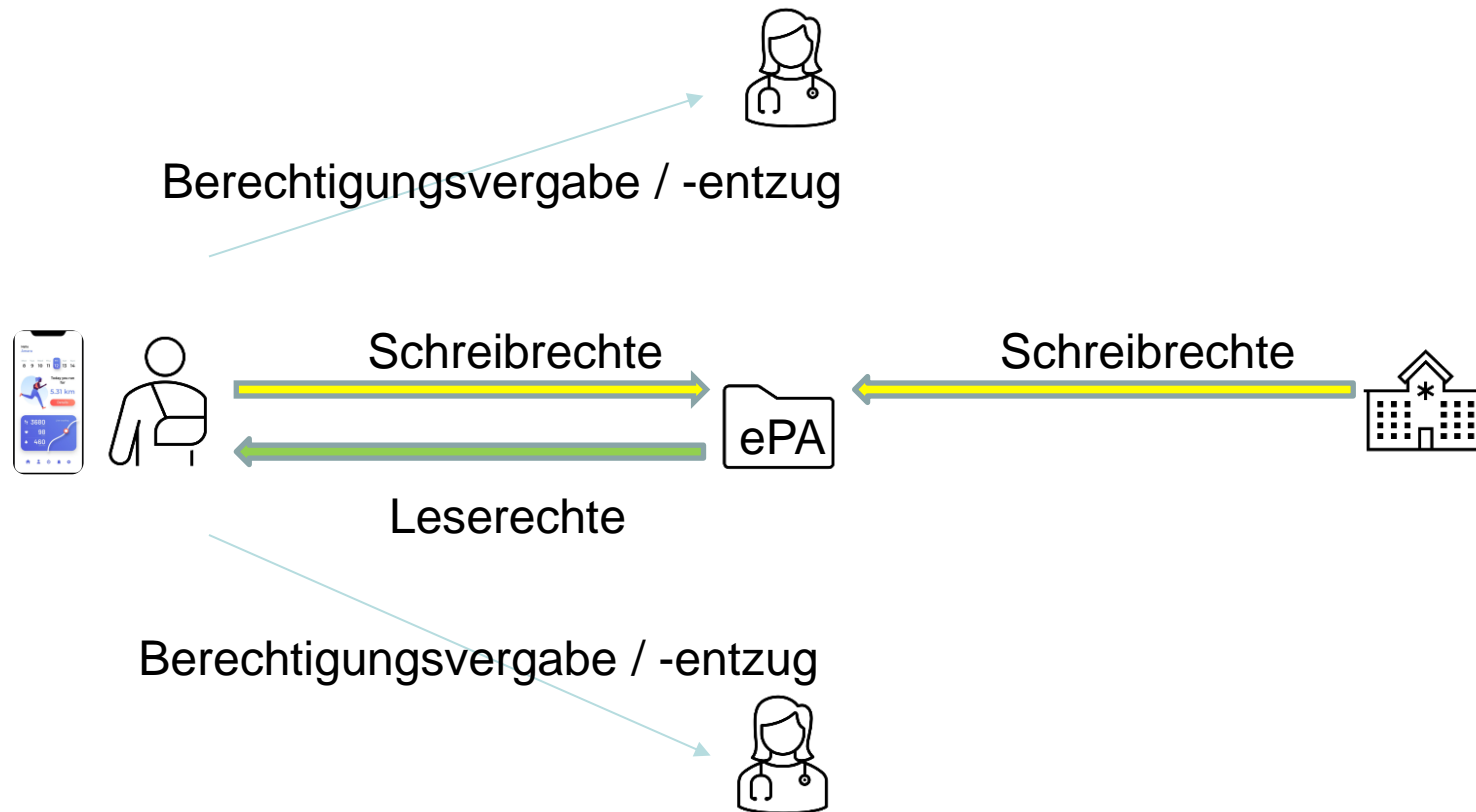


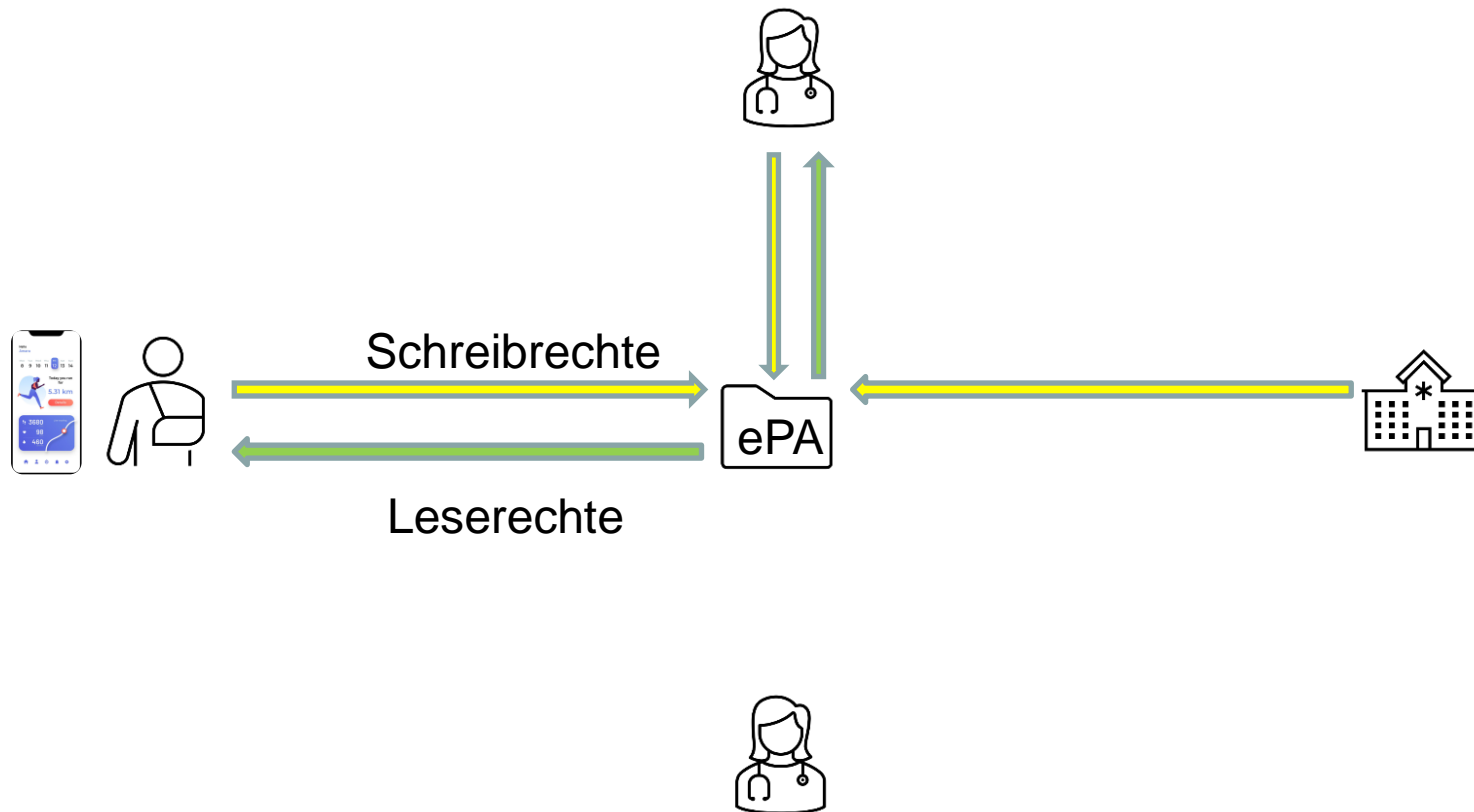


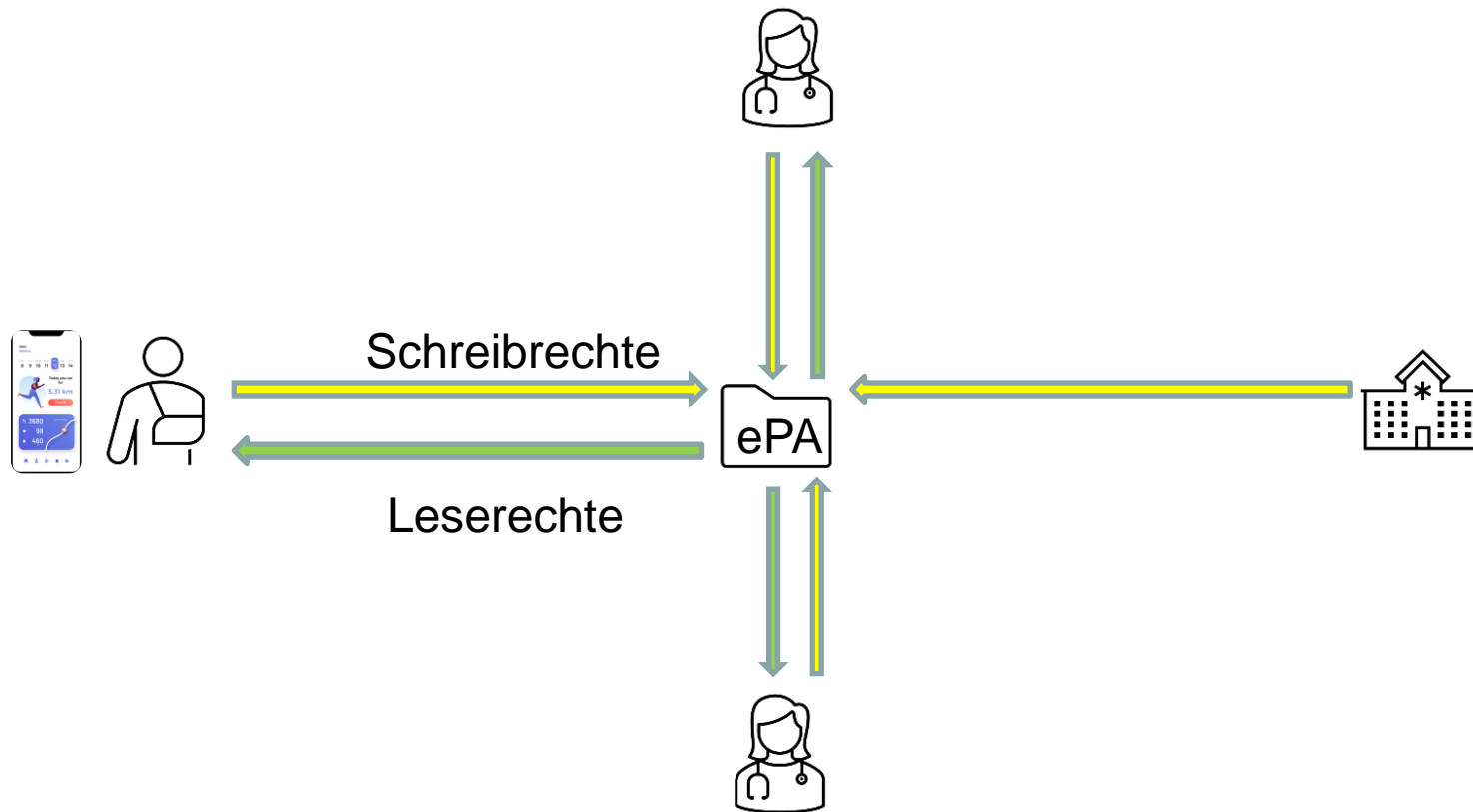
1. Schreibrechte

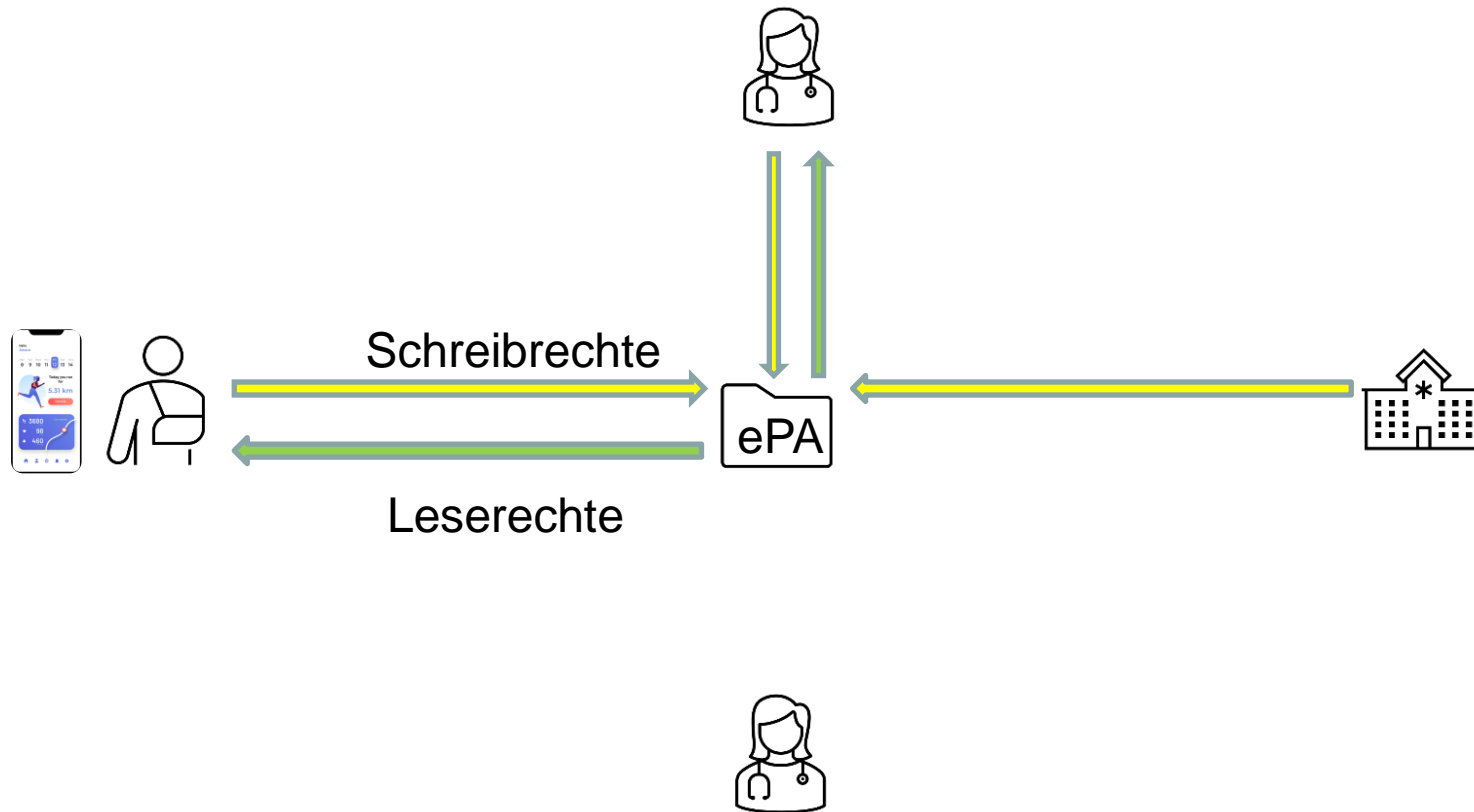












# Datenschutzrechtliche Herausforderung I – Verantwortung





# Datenschutzrechtliche Herausforderungen I

## SGB V – Regelung der Verantwortung der gesetzlichen Krankenkassen

- Art. 4 Nr. 7 HS. 1 DSGVO
- Art. 4 Nr. 7 HS. 2 DSGVO, § 341 Abs. 4 S. 1 SGB V:  
„Die Krankenkassen, die ihren Versicherten eine elektronische Patientenakte zur Verfügung stellen, sind gemäß § 307 Abs. 4 die für die Verarbeitung der Daten zum **Zweck der Nutzung der elektronischen Patientenakte** Verantwortlichen nach Artikel 4 Nummer 7 der Verordnung (EU) 2016/679.
- § 342 Abs. 1 Satz 4 SGB V:  
„(Versicherten soll, PS) auf Verlangen Informationen, insbesondere zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen sowie zu Behandlungsberichten, für eine einrichtungs-, fach- und sektorenübergreifende Nutzung für **Zwecke der Gesundheitsversorgung**, insbesondere zur gezielten Unterstützung von Anamnese und Befunderhebung, **barrierefrei elektronisch bereitgestellt** werden.“

(Hervorhebungen eingefügt)

## Die Regelung der Verantwortung aus Sicht der Krankenkassen: „Verantwortung ohne Kenntnis und Kontrolle“

- mangels Leserechten *keine Kenntnis* über vorhandene Daten
  - Bsp.: Urlaubsfotos
- mangels Zugriffsrechten *keine Kontrolle* über vorhandenen Datensatz
  - Bsp.: Schadsoftware

→ Haftung??? Haftungsbegrenzung???

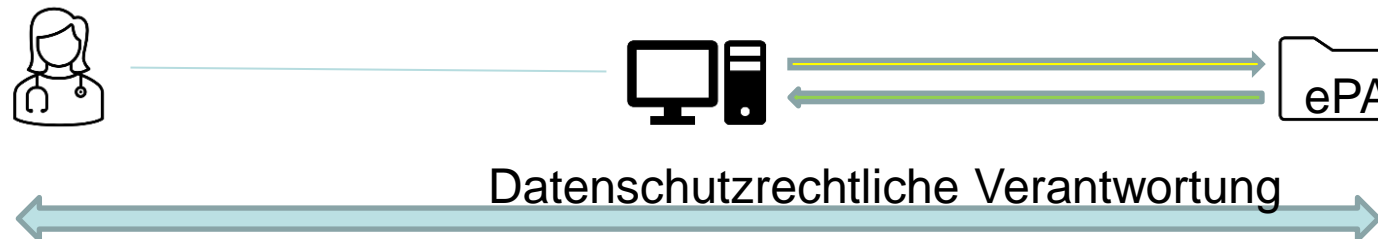
## Datenschutzrechtliche Herausforderungen II

### Rechtmäßigkeit der Datenverarbeitung der Leistungserbringer

- Art. 6 Abs. 1 lit. b, Art. 9 Abs. 2 lit. h DSGVO, § 22 Abs. 1 Nr. 1b BDSG:  
**Erforderlichkeit für Zwecke der Gesundheitsvorsorge** (...) für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich (...) oder **aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs** (...)

Aus Sicht der **Leistungserbringer** zwei Datenverarbeitungstätigkeiten im Zusammenhang mit der ePA:

- **Upload** von Daten aus PVS/KIS in die ePA (= „Übermittlung“)
- **Download** von Daten aus ePA in das PVS/KIS (= „Erhebung“)



- § 352 HS. 1 SGB V:  
„Auf die Daten in der elektronischen Patientenakte nach § 341 Absatz 1 Satz 1 **dürfen mit Einwilligung der Versicherten** nach § 339 ausschließlich folgende Personen zugreifen: 1.Ärzte, (...)“
- § 353 Abs. 1 SGB V:  
„Die Versicherten erteilen die nach § 352 **erforderliche Einwilligung** in den Zugriff auf Daten der elektronischen Patientenakte nach § 341. Hierzu bedarf es einer eindeutigen bestätigenden Handlung durch technische Zugriffsfreigabe über die Benutzeroberfläche eines geeigneten Endgeräts.“
- § 339 Abs. 1 SGB V:  
„Zugriffsberechtigte Leistungserbringer und andere zugriffsberechtigte Personen dürfen nach Maßgabe der §§ 352, 356, 357 und 359 auf personenbezogene Daten, insbesondere Gesundheitsdaten, der Versicherten in einer Anwendung nach § 334 Absatz 1 Satz 2 Nummer 1 bis 5 und 7 zugreifen, **soweit** die Versicherten hierzu ihre vorherige **Einwilligung** erteilt haben.“

## Die Regelung zur Rechtmäßigkeit aus Sicht der Leistungserbringer: „Freifahrtschein für unbegrenzten Zugriff auf Patientendaten?“

- Rechtmäßigkeit des Zugriffs auf Patientendaten aufgrund einer weiten Einwilligung??
  - Bsp.: Zugriff der Zahnärztin auf Daten aus Psychotherapie??
- **Sinn und Zweck der §§ 334 ff. SGB V (Anwendungen der TI)??**
- **Europarechtskonforme Auslegung:** Einwilligung des Versicherten als notwendige, aber nicht als hinreichende Bedingung

## Schluss:

- bis heute über 270 Änderungen des SGB V, große Dynamik des Gesundheitsdatenschutzrechts
- weitere Änderungspläne im Koalitionsvertrag
  - Opt-Out (Änderung Rechtsgrundlage DV Krankenkassen)
  - TI 2.0
  - gematik = „Nationale Gesundheitsagentur“
- ePA als neuartige Anwendung der TI mit datenschutzrechtlichen Herausforderungen, den nur teilweise durch Auslegung begegnet werden kann