BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Datenschutz und die elektronische Patientenakte

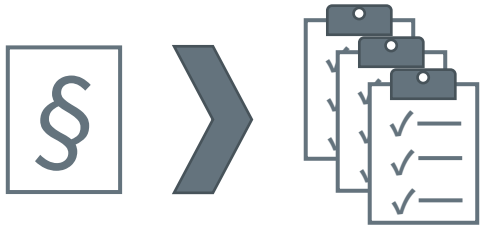
Fachtagung
Datenschutz im Gesundheitswesen 2021

Manuel Peter
Referat 21 – Projekte der angewandten Informatik, Telematik
Manuel.Peter@bfdi.bund.de

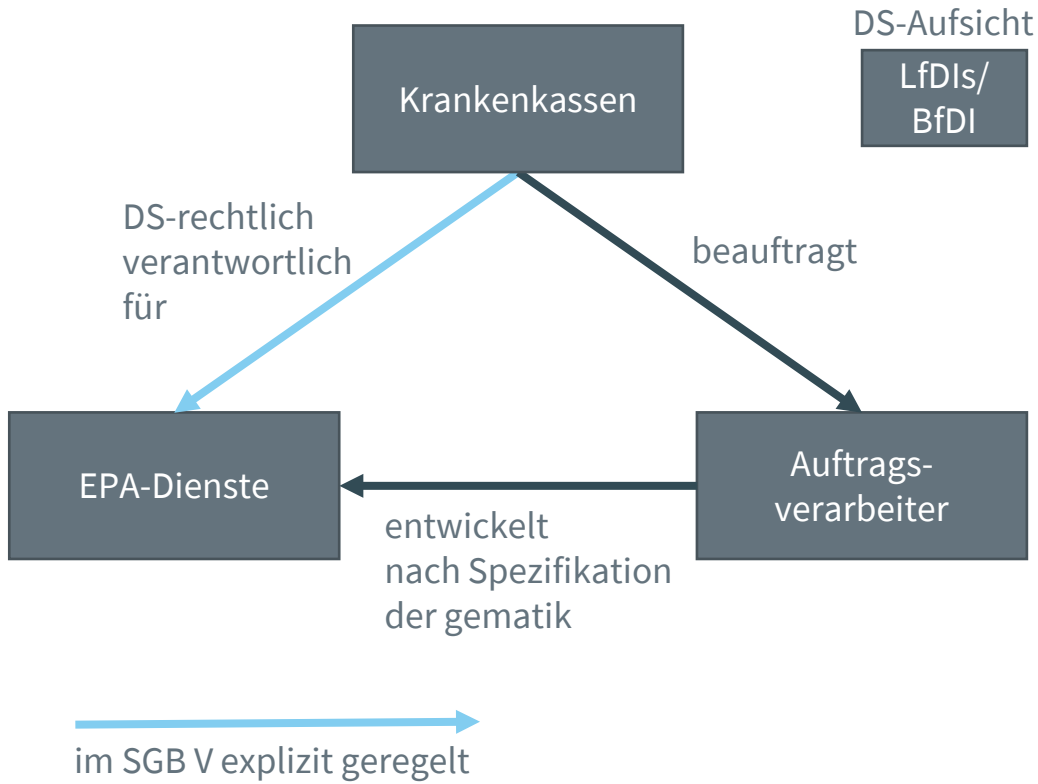
1

Überblick über Entstehungsprozess und gesetzliche Verantwortlichkeit

Die Entstehung von Diensten und Komponenten in der TI ist ein dreiphasiger Prozess. Der BfDI tritt während der Gesetzgebung beratend auf.

Prozessphase	Akteur	BfDI
Gesetzgebung 	**Gesetzgeber**	berät kein Vetorecht
Spezifikation 	**Gematik** erstellt Spezifikation auf Gesetzesgrundlage	berät während Konzeption und wird bei Spezifikation beteiligt
Entwicklung und Betrieb 	**Anbieter** entwickeln nach Spezifikation	Datenschutzrechtliche Aufsicht im Betrieb bei jeweiliger Aufsichtsbehörde des Anbieters

Das SGB V weist die DS-rechtliche Verantwortlichkeit für EPA-Dienste den Krankenkassen zu. Aufsichtsbehörden müssen ihre Maßnahmen an sie richten.



Das SGB V legt die datenschutzrechtliche Verantwortung der EPA explizit fest:

- § 307 Abs. 4 SGB V: **Anbieter** von Komponenten und Diensten sind **datenschutzrechtlich verantwortlich**
- § 341 Abs. 4 SGB V: **Krankenkassen sind** gemäß § 307 Abs. 4 SGB V **datenschutzrechtlich verantwortlich für die EPA-Dienste**. Sie können Auftragsverarbeiter beauftragen.
- DS-rechtliche **Aufsicht** während des Betriebs hat **je nach Krankenkasse** entweder eine **Landesdatenschutzbehörde oder der BfDI**

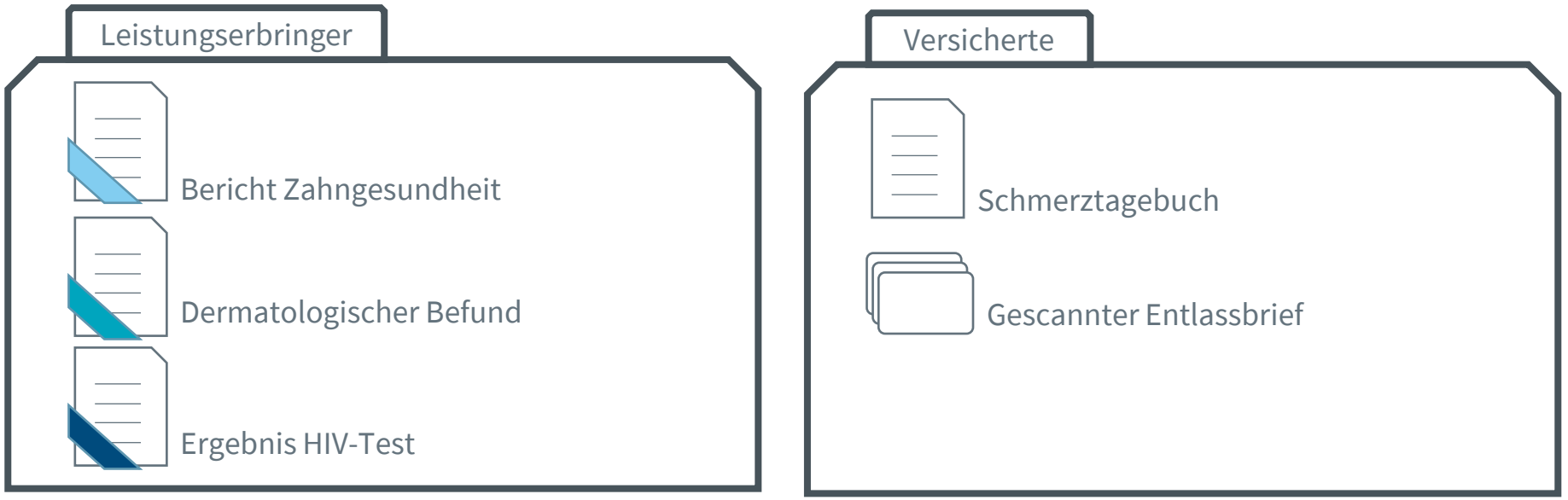
2

Drei Hauptkritikpunkte:

- Berechtigungsmanagement
- Benachteiligungen für Frontend-Nicht-Nutzer
- Authentisierungsverfahren ohne eGK

Die EPA besteht 2021 aus zwei Fächern. Versicherte können LEI nur grobgranular Berechtigungen für ein komplettes Fach gewähren.

Schematische Darstellung der zwei Fächer in der EPA



Berechtigungsmanagement

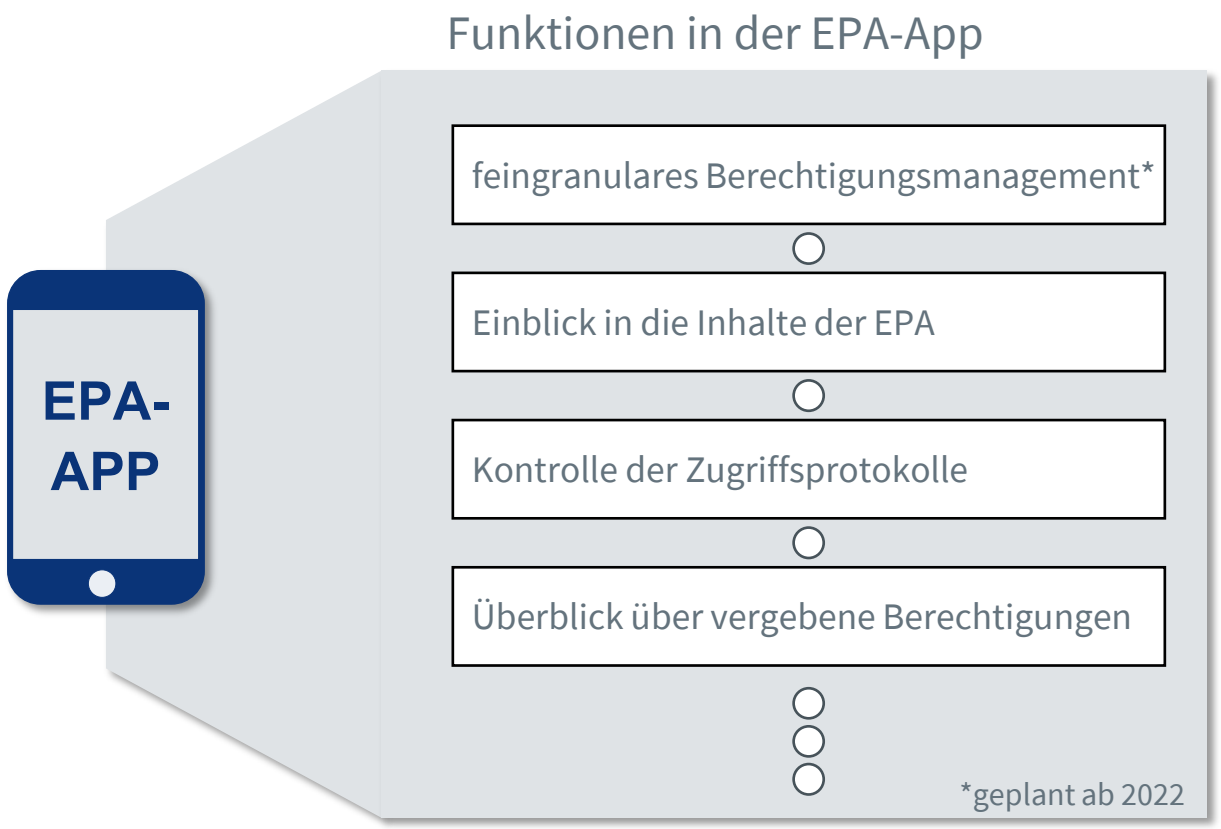
	LE-Fach	V-Fach
Dr. Muster	☒	☒
Dr. Baum	☐	☒

- berechtige LEI können Dokumente lesen einstellen und löschen
- Versicherte können Dokumente löschen

- Versicherte können Dokumente einstellen und löschen

Meta-Datum: einstellender LE

Wichtige Funktionen zur Wahrnehmung ihrer Rechte stehen Front-Nicht-Nutzern nicht zur Verfügung.



Erläuterung

- Elementar **wichtige Funktionen** stehen **nur in der App** (Frontend) zur Verfügung

- **Menschen, die Frontend nicht nutzen** wollen oder können, können **Grundrechte nicht selbständig wahrnehmen**.

Das SGB V fordert eine Authentisierungsmittel ohne Einsatz der eGK für den Einsatz am Endgerät. BfDI forderte die Umsetzung „al.vi“ zu verbessern.

Zwei Authentisierungsmittel

	Authentifizierung mit eGK	Authentifizierung ohne eGK
§	§ 336 Abs. 1 SGB V: Zugriff **mittels eGK**	§ 336 Abs. 2 SGB V: Zugriff auch **ohne Einsatz der eGK**
✓	• Schlüsselmaterial auf Chip • Kartenleser oder Smartphone mit NFC notwendig	• gematik entwarf „Alternative Versichertenidentität“ (al.vi) • Zweite kryptografische Identität in zentralem Signaturdienst in TI

- **Kritik des BfDI** hier nicht am Gesetz sondern **an konkreter Umsetzung**
- Al.vi entspricht einer Fernsignatur
- Sicherheitsniveau entspricht nicht der eGK-Lösung

BfDI

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550

poststelle@bfdi.bund.de
www.bfdi.bund.de