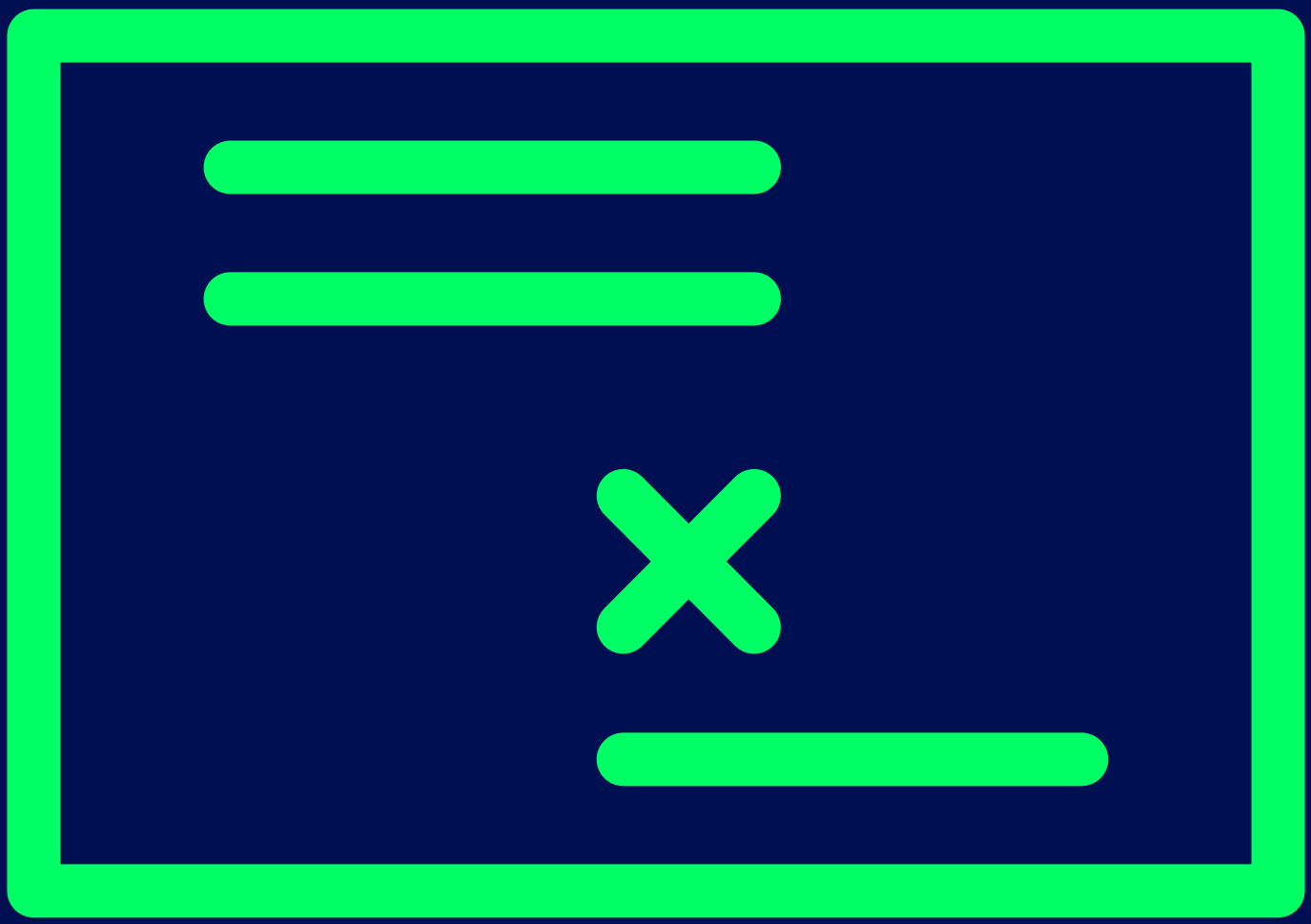
E-Rezept

gematik



Datenschutz-Folgenabschätzung

für die E-Rezept-App der gematik

Vorausgehende Hinweise

Dieses Dokument enthält die Version 1.0 des Berichts zur Datenschutz-Folgenabschätzung (DSFA[1]) für die E-Rezept-Anwendung (E-Rezept-App), die von der gematik GmbH (gematik) spezifiziert, hergestellt und angeboten wird.

Die DSFA wird laufend überprüft, um zu bewerten, ob die wesentlichen bisherigen Ergebnisse weiterhin gültig sind oder eine Aktualisierung erforderlich ist. Eine Aktualisierung der DSFA ist jedenfalls dann erforderlich, wenn geänderte technische oder rechtliche Rahmenbedingungen, neue Erkenntnisse oder geplante Änderungen der E-Rezept-App (z. B. Funktionserweiterungen) zu einer geänderten Risikobewertung führen können. Daher handelt es sich bei dem vorliegenden DSFA-Bericht um ein „lebendiges Dokument", das von Zeit zu Zeit aktualisiert und in einer neuen Version zur Verfügung gestellt wird.

In diesem DSFA-Bericht wird ausschließlich aus Gründen der leichteren Lesbarkeit auf eine geschlechtsspezifisch differenzierende Verwendung von juristischen und technischen Fachbegriffen verzichtet (z. B. „Nutzer", „Angreifer"). Selbstverständlich bezieht sich der jeweilige Begriff auf Personen jeglichen Geschlechts.

1 Aus Gründen der besseren Lesbarkeit werden die Begriffe „DSFA" und „DSFA-Bericht" nachfolgend teilweise synonym bzw. in Abhängigkeit des jeweiligen Kontexts verwendet.

Inhalt

1 Executive Summary

Der vorliegende Bericht dokumentiert die Ergebnisse der Datenschutz-Folgeabschätzung (DSFA) zur Entwicklung, Bereitstellung und Nutzung der E-Rezept-App in Deutschland. Bei der E-Rezept-App handelt es sich um einen Bestandteil der Fachanwendung E-Rezept, zu der neben der E-Rezept-App noch weitere Komponenten und Dienste der Telematikinfrastruktur (TI) gehören. Gegenstand des DSFA-Berichts ist damit weder die Fachanwendung an sich noch die Gesamtheit ihrer einzelnen Komponenten und Dienste, sondern die E-Rezept-App als Bestandteil der Fachanwendung E-Rezept und Komponente der TI.

In der E-Rezept-Fachanwendung werden zum Teil personenbezogene Daten verarbeitet. Zum Teil handelt es sich auch um besonders sensible Gesundheitsdaten. Diese Datenverarbeitung betrifft alle Versicherten, die eine Verschreibung von Arzneimitteln mittels der E-Rezept-App einlösen möchten. Aus der Qualität der verarbeiteten Daten und der voraussichtlichen Quantität der Verarbeitung ergibt sich damit grundsätzlich die Notwendigkeit, eine DSFA durchzuführen. Allerdings ist die Durchführung einer DSFA geknüpft an die datenschutzrechtliche Verantwortlichkeit. Das ist in aller Regel sachgerecht, da über die erwarteten

Folgen einer Datenverarbeitung regelmäßig derjenige am besten Auskunft geben kann, der die Zwecke und Mittel der Verarbeitung bestimmt. Die Mehrheit der Verarbeitungsvorgänge, die in diesem DSFA-Bericht dokumentiert und bewerteten werden, findet jedoch außerhalb des Verantwortungsbereichs der gematik statt. Die Betrachtung von Verarbeitungstätigkeiten im Zusammenhang mit der E-Rezept-App erfolgt überwiegend, um den Kontext der in der Verantwortlichkeit der gematik erfolgenden Verarbeitungen herstellen und diskutieren zu können. Eine DSFA durch die gematik ist daher weder gesetzlich vorgesehen noch wird sie von den deutschen oder europäischen Aufsichtsbehörden gefordert. Die gematik hat sich gleichwohl zur Durchführung einer DSFA entschieden. Sie sieht es als ihren Auftrag an, den Schutz personenbezogener Daten auch dort voranzutreiben, wo sie für eine Datenverarbeitung nicht unmittelbar verantwortlich ist, und begreift diesen Bericht als Chance, durch transparente Dokumentation und Aufklärung über absehbare Risiken und bereits getroffene Abhilfemaßnahmen Vertrauen in das E-Rezept und in digitale Gesundheitsanwendungen im Allgemeinen zu schaffen. Um dieses Ziel möglichst umfassend zu verwirklichen, bezieht dieser DSFA-Bericht die politischen, historischen und technischen Kontexte, in die der Prüfgegenstand eingebettet ist, umfassend ein.

Im nachfolgenden DSFA-Bericht werden Datenverarbeitungsvorgänge beschrieben und Risiken bewertet. Er konzentriert sich auf die folgenden Verarbeitungsprozesse:

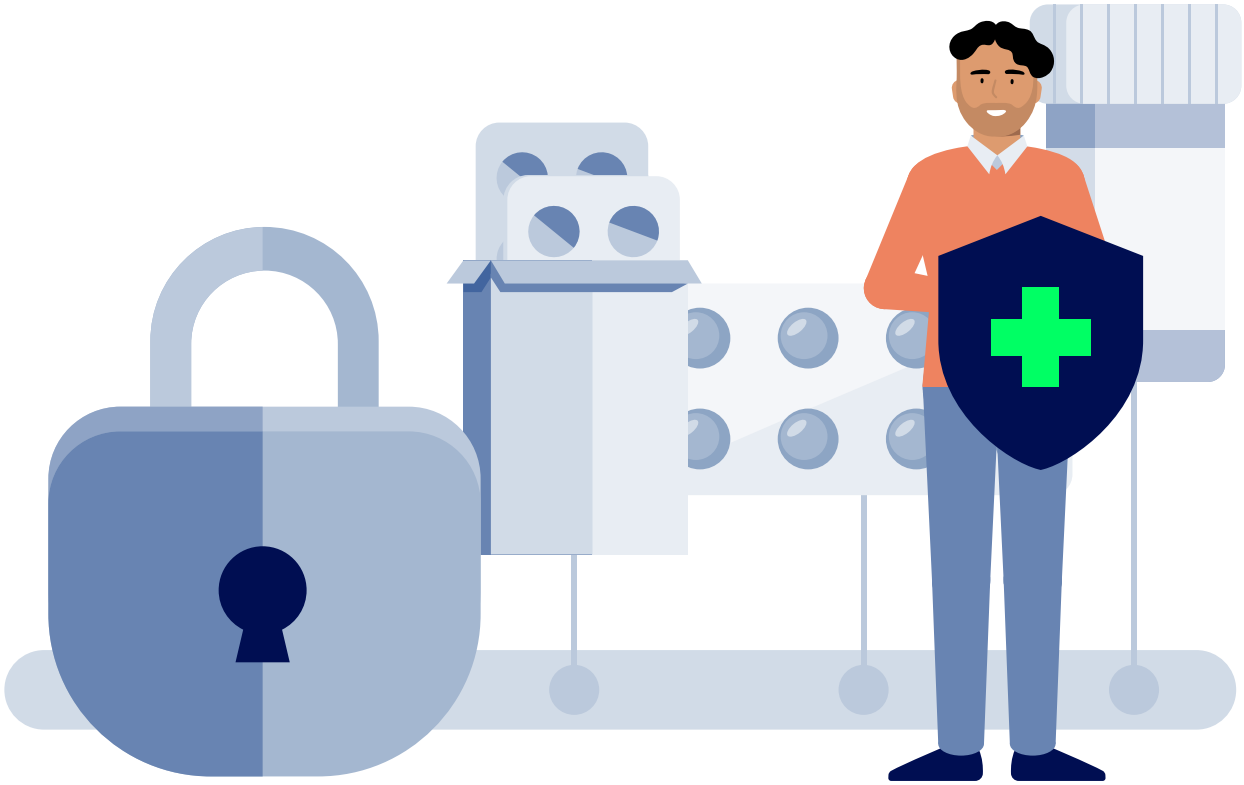
- Installation und Deinstallation der App,
- Start und Einrichtung der App,
- Anmeldung am E-Rezept-Fachdienst und Identity Provider,
- Einlösen von E-Rezepten,
- Apothekensuche und -bestimmung,
- Mitteilungsfunktion,
- E-Rezepte verwalten und teilen,
- Nutzungsanalyse.

Dabei wird ein besonderes Augenmerk auf das Rollenkonzept der DSGVO, die Verantwortlichkeit für verschiedene Verarbeitungsvorgänge und die Rechtmäßigkeit der Verarbeitung gelegt.

Im Anschluss an die Beschreibung der Verarbeitungstätigkeiten werden die Risiken für die betroffenen Personen erfasst und nach ihrer Eintrittswahrscheinlichkeit und Gefährdung hinsichtlich der Gewährleistungsziele nach dem Standard-Datenschutzmodell (SDM) der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) eingeordnet. Dabei wird die Perspektive der betroffenen Personen eingenommen, wobei nicht nur die Auswirkungen auf den Einzelnen, sondern auch Risikoaspekte einbezogen werden, die die gesamte Masse der Nutzer betreffen. Betrachtet werden Risiken, die nach Berücksichtigung bereits etablierter Maßnahmen verbleiben und die technischen und organisatorischen Maßnahmen (TOM), die zur Verfügung stehen, um diese Risiken zu begrenzen. Dabei werden insbesondere Risiken betrachtet, die für E-Rezept-App wesentlich sind. So wird beispielsweise das Risiko des App-Spoofings durch die Verwendung eines API-Keys gesenkt, der verhindert, dass gefälschte Apps auf den E-Rezept-Fachdienst zugreifen.

Insgesamt ergibt die Risikoanalyse, dass fünf niedrige und 14 Risiken im mittleren Bereich bestehen. Die allgemeinen Risiken elektronischer Datenverarbeitung sind stets gegeben und werden der Übersichtlichkeit halber nicht explizit aufgeführt.

Im Ergebnis ist festzuhalten, dass keine Risiken bestehen, die die Nutzung der E-Rezept-App untragbar machen würden. Im Gegenteil ist vielmehr erkennbar, dass die E-Rezept-App stabil und hinreichend sicher genutzt werden kann. Die Einhaltung der gesetzlichen und behördlichen Vorgaben ist gewährleistet und wird durch diesen Bericht fortlaufend dokumentiert.



2 Einleitung

Der vorliegende Bericht dokumentiert die Ergebnisse einer durchgeführten DSFA für die Entwicklung, Bereitstellung und Nutzung der E-Rezept-App in Deutschland. Er dient insbesondere der Prüfung und Dokumentation der damit verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung ihrer Daten und richtet sich insofern an die interessierte Öffentlichkeit. Zudem dient er als Nachweis der Einhaltung der Grundsätze des Datenschutzrechts – insbesondere der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO – gegenüber deutschen und europäischen Aufsichtsbehörden.

Die Durchführung und Dokumentation von Folgenabschätzungen ist in Art. 35 DSGVO geregelt. Zeichnet sich ab, dass eine Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, so ist der Verantwortliche zur Durchführung einer DSFA verpflichtet, Art. 35 Abs. 1 S. 1 DSGVO. Von diesem Grundsatz wird nachfolgend insofern abgewichen, dass sich die gematik dazu entschieden hat, eine DSFA durchzuführen, obwohl sie dazu gesetzlich nicht verpflichtet ist, und hierbei auch solche Verarbeitungstätigkeiten einbezogen werden, für welche die gematik nicht verantwortlich ist. Diese Besonderheiten rechtfertigen sich durch die besondere Natur des Prüfgegenstands. Die Entschei-

dung, eine DSFA durchzuführen, und der besondere Zuschnitt dieser DSFA ergeben sich zwanglos aus der besonderen Aufgaben- und Rollenverteilung im Zusammenhang mit der Entwicklung und Einführung des E-Rezepts in Deutschland, die im Verlauf dieses DSFA-Berichts weiter beleuchtet werden. Die gematik sieht die Durchführung und Dokumentation der DSFA als Gelegenheit an, ihren gesetzlichen Auftrag zu erfüllen und den Schutz personenbezogener Daten voranzutreiben.

Der nachfolgende DSFA-Bericht gliedert sich in drei Teile:

Zunächst wird die Frage erörtert, ob und warum eine DSFA im konkreten Fall (nicht) erforderlich war. Anschließend werden die gesellschaftlichen, historischen, normativen und technischen Kontexte dargestellt, in die der Prüfgegenstand eingelassen ist. Im nächsten Schritt werden die einzelnen Verarbeitungsvorgänge der E-Rezept-App, die dabei verarbeiteten Daten und die Zwecke der Verarbeitung näher beschrieben.

Im Anschluss an die Beschreibung der einzelnen Verarbeitungstätigkeiten wird eine Bewertung ihrer Zulässigkeit vorgenommen. Zu diesem Zweck wird zunächst bewertet, ob es sich bei den verarbeiteten Daten um personenbezogene Daten und bei den personenbezogenen Daten um Gesundheitsdaten handelt. Anschließend wird untersucht, wer für die Datenverarbeitung im Einzelfall konkret verantwortlich ist, um in einem nächsten Schritt die Rechtmäßigkeit dieser Verarbeitung zu erörtern. Zunächst werden die Rechtsgrundlagen der Verarbeitung diskutiert. Im Anschluss daran werden Notwendigkeit und Verhältnismäßigkeit der einzelnen Verarbeitungstätigkeiten mit Blick auf die allgemeinen Vorgaben der DSGVO und die besonderen Zwecke des Prüfgegenstands untersucht. Dabei wird der Perspektive der betroffenen Personen und ihren Rechten besonders Rechnung getragen.

Herzstück dieser Bewertung ist die Risikoanalyse. Im Anschluss an die Untersuchung der datenschutzrechtlichen Rechtmäßigkeit der einzelnen Verarbeitungstätigkeiten werden die verschiedenen Risiken für den Schutz personenbezogener Daten herausgearbeitet und verschiedene Maßnahmen, Garantien und Verfahren präsentiert, die diese Risiken eindämmen, den Schutz personenbezogener Daten sicherstellen und die Einhaltung der rechtlichen Vorgaben und Bestimmungen nachweisen sollen.[1]

Der Bericht endet mit abschließenden Hinweisen, wie die Sicherung des Datenschutzes im Zusammenhang mit der Fortentwicklung der E-Rezept-App nachhaltig sichergestellt werden soll.

2.1 Ansprechpartner und Kontaktdaten der gematik

gematik GmbH
Friedrichstraße 136, 10117 Berlin

Telefon: +49 030 400 41-0
Telefax: +49 30 400 41-111

info@gematik.de | www.gematik.de

Geschäftsführer: Dr. med. Markus Leyck Dieken
Datenschutzbeauftragter: Christian Retta
datenschutz@gematik.de

1 EG 90 DSGVO

2.2 DSFA-Team

Die vorliegende DSFA wurde durch ein interdisziplinäres Team durchgeführt. Dieses Team setzt sich zusammen aus Vertretern der gematik aus den Bereichen Produkt, Sicherheit, Datenschutz und Recht sowie aus Rechtsanwälten der beauftragten Kanzlei Schürmann Rosenthal Dreyer Rechtsanwälte PartG mbB. Die Mitglieder des DSFA-Teams verfügen über die relevanten Fachkenntnisse, um datenschutzrechtliche Risiken zu identifizieren, Maßnahmen zur Risikominimierung zu treffen und deren Auswirkungen auf die Zweckerreichung der E-Rezept-App abzuschätzen.

Teilergebnisse der DSFA wurden regelmäßig zwischen der gematik und der Kanzlei abgestimmt. Der Datenschutzbeauftragte (DSB) der gematik stand dem DSFA-Team beratend zur Seite, wobei eine regelmäßige Einbindung des DSB in die Durchführung der DSFA nicht erfolgt ist, um die Unabhängigkeit bei der Prüfung ihrer Ergebnisse zu wahren.

Darüber hinaus hat die gematik den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) über den aktuellen Entwicklungsstand und die Einführung der E-Rezept-App unterrichtet und zu kritischen oder unklaren datenschutzrechtlichen Aspekten im Rahmen seiner gesetzlichen Aufgaben dessen Beratung in Anspruch genommen, sodass diese in der DSFA berücksichtigt werden konnten.

2.3 Abkürzungsverzeichnis

AES	Advanced Encryption Standard
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
API	Application Programming Interface
APN	Apple Push Notification
ApoG	Apothekengesetz
ASL	Active Script List
AVS	Apothekenverwaltungssoftware
AWS	Amazon Webservices
BÄK	Bundesärztekammer
BDNP	Base de Dados Nacional de Prescrição
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BMG	Bundesministerium für Gesundheit
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagdrucksache
BZÄK	Bundeszahnärztekammer
CA	Certification Authority
CAN	Card Access Number
CDU	Christlich-Demokratische Union
DAV	Deutscher Apothekerverband
DAZ	Deutsche Apotheker Zeitung
Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz	Gesetz zur digitalen Modernisierung von Versorgung und Pflege
DKG	Deutsche Krankenhausgesellschaft
DP	Dossier Pharmaceutique
DSB	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder
DVPMG	Siehe Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz
E-Health-Gesetz	Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen
E-Health-Netzwerk	Netzwerk für elektronische Gesundheitsdienste
EDPB	European Data Protection Board
eFA	eFallAkte
EG	Erwägungsgrund
eGK	Elektronische Gesundheitskarte
EHDS	European Health Data Space
EHRxF	European Electronic Health Record exchange Formats
eHSG	eHealth stakeholder group
EL	Ergänzungslieferung

eMP	Elektronischer Medikationsplan
ePA	Elektronische Patientenakte
EPS	Electronic Prescription Service
EU	Europäische Union
EuGH	Europäische Gerichtshof
EUPL	European Union Public Licence
EVS	Elektronisch Voorschrijf Systeem
EWR	Europäischer Wirtschaftsraum
FCM	Firebase Cloud Messaging
FDP	Freie Demokratische Partei
FIP	International Pharmaceutical Federation
FMK	Fælles Medicinkort
FSE	Fascicolo Sanitario Elettronico
gematik	gematik GmbH
GG	Grundgesetz
GKV-Modernisierungsgesetz	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
GKV-Spitzenverband	Spitzenverband Bund der Gesetzlichen Krankenkassen
GMG	Siehe GKV-Modernisierungsgesetz
GSAV	Gesetz für mehr Sicherheit in der Arzneimittelversorgung
HSDA	Historia de Salud Digital Única de Andalucía
IDP	Identity Provider
IK-Nummer	Institutionskennzeichen-Nummer
IKP	Internetowe Konto Pacjenta
ISO	International Organization for Standardization
KBV	Kassenärztliche Bundesvereinigung
KIS	Krankenhausinformationssysteme
KNMG	Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst
KV	Kassenärztliche Vereinigung
KVNR	Krankenversicherungsnummer
KZBV	Kassenzahnärztliche Bundesvereinigung
MHR	My Health Record
NDGA	Netzgesellschaft Deutscher Apotheker mbH
NFC	Near Field Communication
NFDM	Notfalldatenmanagement
NHS	National Health Service
NHSBSA	NHS Business Service Authority
NLL	Nationella läkemedelslistan
NRE	Numero di Ricetta Elettronica
NZS	Neue Zeitschrift für Sozialrecht
PARIS	Prescription & Autorisation Requesting Information System
Patientendaten-Schutz-Gesetz	Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur
PCKE	Proof Key for Code Exchange
PDS	Prescription Delivery Service
PDSG	Siehe Patientendaten-Schutz-Gesetz
PEM Móvel	Prescrição Eletrónica Médica Móvel
PES	Prescription Exchange Services
PIA	Privacy Impact Assessment
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
PKV	Verband der privaten Krankenversicherungen
PVS	Praxisverwaltungssoftware
QES	Qualifizierte elektronische Signatur
REZ ID	alphanumerische e-Rezept ID
RISE	Research Industrial Systems Engineering
RSP	Receita Sem Papel
SDK	Software Development Kit
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
SHA	Secure Hash Algorithm
SPD	Sozialdemokratische Partei Deutschlands
SSO	Single Sign-on
STS	Sistema Tessera Sanitaria
TEHDAS	Towards the European Health Data Space
TI	Telematikinfrastruktur
TKG	Telekommunikationsgesetz
TOM	Technische und organisatorische Maßnahmen
TSVG	Terminservice- und Versorgungsgesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein
VSDM	Versichertenstammdatenmanagement
VVT	Verzeichnis von Verarbeitungstätigkeiten

3 Notwendigkeit der DSFA

Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO sind in bestimmten Fällen verpflichtet, die Folgen der von ihnen verantworteten Verarbeitungsvorgänge für den Schutz personenbezogener Daten abzuschätzen, und diese Betrachtung und die daraus abgeleiteten Erkenntnisse in einem Bericht zu dokumentieren, Art. 35 Abs. 1 S. 1 DSGVO. Ob ein Verantwortlicher einer solchen Pflicht zur Durchführung einer DSFA unterliegt, ist mit Blick auf die gesetzlichen und behördlichen Vorgaben im Einzelfall zu ermitteln. Die Notwendigkeit einer DSFA kann sich aus dem Abgleich der Verarbeitungstätigkeiten mit einer Muss-Liste, aus einer Schwellenwertanalyse oder einer allgemeinen Vorabprüfung des Risikos ergeben. Diese drei Prüfungsschritte sind zunächst näher zu bestimmen, bevor sie auf den Prüfungsgegenstand bezogen werden können.

3.1 Muss-Liste

Die deutschen und europäischen Aufsichtsbehörden haben Verarbeitungstätigkeiten, für die eine DSFA zwingend durchzuführen ist, in sogenannten Muss-Listen zusammengefasst. Für den Prüfgegenstand gilt die Liste von Verarbeitungsvorgängen nach Artikel 35 Abs. 4 DSGVO, für die im Zuständigkeitsbereich des BfDI eine DSFA durchzuführen ist.[2] Danach ist eine DSFA zwingend erforderlich, wenn mindestens zwei der folgenden Merkmale vorliegen:

1. Die Verarbeitung umfasst eine Bewertung oder Einstufung der Betroffenen, darunter das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen.

2. Die Verarbeitung umfasst eine automatisierte Entscheidungsfindung mit einer Wirkung, die zwar nicht alleine die Grundlage für Entscheidungen mit Rechtswirkung oder ähnlichen bedeutsamen Auswirkungen für die Betroffenen darstellen, aber einen wesentlichen Beitrag zu solchen Entscheidungen liefern.

3. Die Verarbeitung hat die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel und greift auf beispielsweise über Netzwerke erfasste Daten oder auf eine systematische Überwachung auch nicht öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 lit. c DSGVO) zurück.

4. Bei der Verarbeitung werden vertrauliche oder höchst persönliche Informationen verarbeitet, insbesondere aus den folgenden Kategorien:

   a. Besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 oder Art. 10 DSGVO,

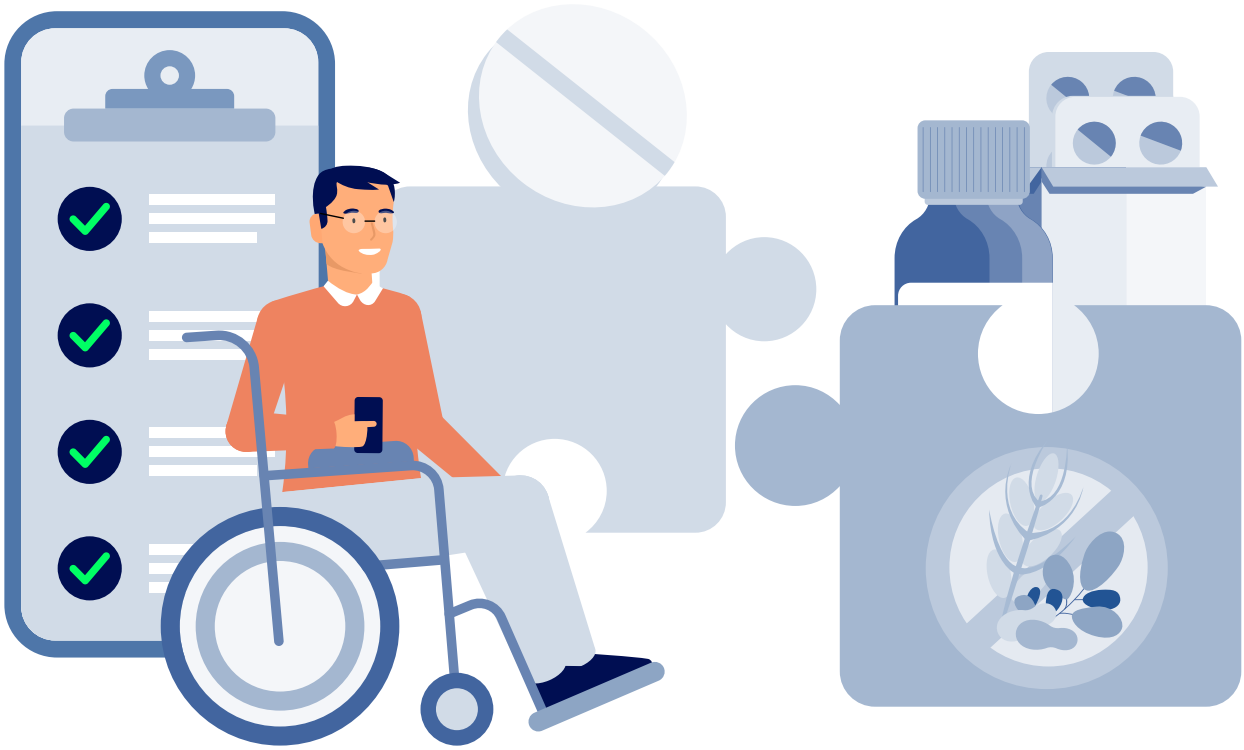
   b. Gesundheitsdaten im Sinne des § 67 Abs. 1 SGB X,

   c. Sozialdaten,

   d. Finanzdaten, die umfassende Informationen über die finanziellen Verhältnisse der Betroffenen zulassen, oder die für einen Zahlungsbetrug missbraucht werden können (beispielsweise Kontendaten oder Zahlungsdaten von Konten).

5. Es handelt sich um eine Datenverarbeitung in großem Umfang.

2 BfDI, Liste von Verarbeitungsvorgängen gemäß Artikel 35 Abs. 4 DSGVO für Verarbeitungstätigkeiten öffentlicher Stellen des Bundes, Stand: Version 1.1-BfDI vom 01.10.2019, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeArt35.pdf (zuletzt abgerufen am 15.12.2022).



6. Im Rahmen der Verarbeitung werden Datensätze aus zwei oder mehreren Verarbeitungen zusammengeführt und/oder abgeglichen, die zu unterschiedlichen Zwecken und/oder von verschiedenen Verantwortlichen durchgeführt wurden, und zwar in einer Weise, die über die vernünftigen Erwartungen der Betroffenen hinausgehen.

7. Bei der Verarbeitung werden Daten zu schutzbedürftigen Betroffenen verarbeitet. Dies umfasst insbesondere die folgenden Gruppen:

   a. Kinder,

   b. Arbeitnehmer/Beamte im Falle einer Verarbeitung durch den Arbeitgeber/Dienstherrn,

   c. Teile der Bevölkerung mit besonderem Schutzbedarf (insbesondere psychisch Kranke, Asylbewerber, Senioren, Patienten),

   d. Betroffene in Situationen, in denen ein besonders ungleiches Verhältnis zwischen der Stellung des Betroffenen und des für die Verarbeitung Verantwortlichen vorliegt.

8. Bei der Verarbeitung werden neue Technologien oder organisatorische Lösungen in einer Art und Weise eingesetzt, die dem gegenwärtigen Stand der Technik voraus ist und deswegen die Abschätzung der Auswirkungen auf die Betroffenen und die Gesellschaft erschwert.

9. Die Verarbeitung an sich hindert die Betroffenen an der Ausübung eines Rechts, der Nutzung einer Dienstleistung oder der Durchführung eines Vertrags.

3.2 Schwellenwertanalyse

Die Schwellenwertanalyse basiert auf einer Liste von Kriterien, die von der Artikel-29-Datenschutzgruppe erstellt und vom Europäischen Datenschutzausschuss (European Data Protection Board, EDPB) bestätigt worden ist: den „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 ‚wahrscheinlich ein hohes Risiko mit sich bringt' ".[3] Sobald mindestens zwei der darin beschriebenen Kriterien erfüllt sind, muss eine DSFA durchgeführt werden:

1. Bewerten oder Einstufen,

2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung,

3. Systematische Überwachung,

4. Vertrauliche Daten oder höchst persönliche Daten,

5. Datenverarbeitung in großem Umfang,

6. Abgleichen oder Zusammenführen von Datensätzen,

7. Daten zu schutzbedürftigen Betroffenen,

8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen,

9. Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert" (Art. 22 DSGVO und EG 91).

Bei Beantwortung der Frage, ob eines der vorbezeichneten Kriterien erfüllt ist, ob also beispielsweise ein „Bewerten oder Einstufen" im Sinne der Schwellenwertanalyse vorliegt, müssen zwei Gesichtspunkte besonders beachtet werden. Einerseits kommt es nicht auf die Sichtweise des Verantwortlichen an, sondern allein auf die Sicht eines objektiven Beobachters und die vernünftigen Erwartungen der Betroffenen; andererseits gelten die Kriterien in Zweifelsfällen als erfüllt.

3.3 Allgemeine Vorabprüfung des Risikos

Schließlich ist eine DSFA auch dann erforderlich, wenn die Verarbeitung – insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung – voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 35 Abs. 1 DSGVO). Art. 35 Abs. 3 DSGVO nennt beispielhaft drei Fälle, in denen ein solches Risiko anzunehmen ist:

a. systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen,

b. umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO oder

c. systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

3 Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", S. 9 ff., in deutscher Übersetzung abrufbar unter: https://www.datenschutz-bayern.de/technik/orient/wp248.pdf, bestätigt durch das EDPB: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf

3.4 Anwendung auf den Einzelfall

Die Verarbeitung durch den Prüfgegenstand dient insbesondere der Verarbeitung von personenbezogenen und Gesundheitsdaten; sie betrifft alle Nutzer der E-Rezept-App. Damit sind Kriterien auf allen drei Stufen der Notwendigkeitsprüfung erfüllt: Die Verarbeitung entspricht mehr als zwei Merkmalen der einschlägigen Muss-Liste (Nr. 4 lit. a, 5, 7 lit. c und 8) und erfüllt mindestens zwei Kriterien – Nr. 4 und 5 – der Schwellenwertanalyse; schließlich gelangt auch eine allgemeine Vorabprüfung des Risikos zur Erforderlichkeit einer DSFA: der Prüfgegenstand erfüllt den Tatbestand der zweiten Fallgruppe des Art. 35 Abs. 3 DSGVO – die umfangreiche Verarbeitung sensibler personenbezogener Daten – und birgt daher voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen.

Aus der Qualität und Quantität der maßgeblichen Datenverarbeitungsvorgänge ergibt sich damit grundsätzlich die Notwendigkeit, eine DSFA durchzuführen. Allerdings bestimmt die gematik die Zwecke und Mittel der Datenverarbeitung der E-Rezept-App nur zu einem sehr geringen Teil selbst.[4] Der Großteil der Verarbeitung findet außerhalb ihres Verantwortungsbereichs statt, nämlich auf dem vom Nutzer kontrollierten Smartphone und in den Diensten der TI, die das Backend für das E-Rezept-System bereitstellen.[5]

Die Datenverarbeitung, die von der gematik selbst datenschutzrechtlich verantwortet wird, begründet nach den oben genannten Prüfkriterien isoliert betrachtet voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen, sodass eine DSFA nach den gesetzlichen Vorgaben der DSGVO und den Bestimmungen nationaler und supranationaler Behörden im Einzelfall nicht zwingend geboten ist. Die gematik hat sich gleichwohl zur Durchführung einer DSFA entschieden. Grund dafür ist einerseits die Überzeugung, dass die Berücksichtigung der gesellschaftlichen, rechtlichen und technischen Zusammenhänge für eine gewissenhafte Einschätzung der eigenen Verarbeitungsvorgänge unerlässlich ist, andererseits der Umstand, dass die von anderen Anbietern verantworteten Verarbeitungsvorgänge auf den von der gematik festgelegten Spezifikationen beruhen. Eine DSFA, die absehbare Risiken identifiziert und umgesetzte Abhilfemaßnahmen transparent kommuniziert, unterstützt nicht nur die Einbeziehung weiterer Verantwortlicher und Verarbeitungsvorgänge, sondern hilft zugleich dabei, den Aktualisierungsbedarf in Bezug auf die datenschutzrelevanten Spezifikationen von Diensten und Komponenten im E-Rezept-System zu identifizieren. Insoweit versteht die gematik die Berücksichtigung der von anderen verantworteten Verarbeitungstätigkeiten auch als Instrument zur Erfüllung ihrer gesetzlichen Pflicht aus § 311 Abs. 4 SGB V, bei der Wahrnehmung ihrer Aufgaben die Einhaltung der Vorschriften zum Schutz personenbezogener Daten sicherzustellen.

4 Zum Umfang des datenschutzrechtlichen Verantwortungsbereichs der gematik siehe 7.2.

5 Für die Verarbeitung personenbezogener Daten durch diese Dienste sind gemäß Art. 307 Abs. 4 SGB V die jeweiligen Anbieter verantwortlich. Siehe hierzu 7.2.5.

4 Kontext des Prüfgegenstands

Der Prüfgegenstand steht nicht für sich, sondern ist in verschiedenen gesellschaftlichen, historischen, normativen und technischen Zusammenhängen zu betrachten. Um die DSFA im Allgemeinen und die Risikoanalyse im Besonderen möglichst transparent und nachvollziehbar gestalten und die Ergebnisse in einer Art und Weise präsentieren zu können, die allgemein verständlich ist und ihrerseits eine leichte Überprüfbarkeit gewährleistet, ist eine Darstellung dieser Zusammenhänge – des Kontexts des Prüfgegenstands – unumgänglich. Dabei werden nicht alle Umstände erläutert, die in irgendeiner Weise im Zusammenhang mit der E-Rezept-App stehen und daher von Belang sein könnten, sondern nur solche, die für eine datenschutzrechtliche Prüfung in besonderem Maße relevant sind. Eine solche Relevanz kann sich insbesondere dann ergeben, wenn Umstände für die Identifikation, Einstufung und Mitigation von Datenschutzrisiken bedeutsam sind. Demgegenüber können allgemeine Kontext-Risiken bei der gebotenen Fokussierung auf die unmittelbaren Risiken bei Gebrauch der App nicht berücksichtigt werden.

4.1 Digitalisierung des Gesundheitswesens

Die Digitalisierung des Gesundheitswesens bildet den gesellschaftlichen und politischen Kontext des E-Rezepts. Sie wird oft beschrieben als Reaktion auf neue technologische Möglichkeiten sowie auf gesamtgesellschaftliche Herausforderungen wie die Zunahme chronisch Kranker, das Versorgungsgefälle zwischen ländlichen und urbanen Räumen, den Fachkräftemangel und die Alterung der Bevölkerung. Vor diesem Hintergrund birgt die Digitalisierung des Gesundheitswesens große Chancen für die Gesundheitswirtschaft und -verwaltung, für die Versorgung der Patienten und für die Forschung. Sie erleichtert die Kommunikation zwischen den Beteiligten, eliminiert bestimmte Fehlerquellen und ermöglicht die Entwicklung neuer Diagnose- und Behandlungsmöglichkeiten. Vor allem aber vereinfacht die Digitalisierung den Zugang zu Gesundheitsleistungen unabhängig vom Wohnort und von der Mobilität einzelner Versicherter.

Die Digitalisierung des Gesundheitswesens erscheint im Hinblick auf die medizinische Versorgungslage in Deutschland und die demographische Entwicklung geboten, um die Versorgung langfristig und flächendeckend auf hohem Qualitätsniveau gewährleisten zu können. Die Bundesregierung und das Bundesministerium für Gesundheit (BMG) arbeiten daher laufend an der Konzeptionierung einer nachhaltigen Digitalisierungsstrategie und der Umsetzung dieser Strategie im deutschen Gesundheitswesen. Wichtige Meilensteine auf diesem Weg waren etwa die Einführung der elektronischen Gesundheitskarte (eGK), der Aufbau der TI oder die Entscheidung des Gesetzgebers, digitale Anwendungen wie die elektronische Patientenakte (ePA) oder das E-Rezept einzuführen.

4.2 Gesetzgebungsverlauf

Den mit der Digitalisierung des Gesundheitswesens verbundenen Chancen stehen gewisse Risiken besonders im Bereich des Datenschutzes gegenüber. Um diesen Risiken wirksam zu begegnen und den Prozess der Digitalisierung lenkend mitgestalten zu können, hat der Gesetzgeber in den letzten Jahren zahlreiche Gesetzesänderungen insbesondere des SGB V auf den Weg gebracht. Bei chronologischer Betrachtung des Gesetzgebungsverlaufs zeigt sich, dass wiederkehrende Themen wie der Speicherort der Daten oder der Funktionsumfang des E-Rezepts die Diskussion wie rote Fäden durchziehen. Die Diskussion zwischen Kostenträgern und Leistungserbringern, insbesondere zwischen den Krankenkassen auf der einen und den Ärzten und Zahnärzten auf der anderen Seite, aber auch hinsichtlich des Ausgleichs von effektiver Gesundheitsversorgung und Datenschutz haben die Einführung und Entwicklung der E-Rezept-Anwendung bestimmt.

Bereits in den neunziger Jahren wurde die Einführung eines E-Rezepts in Deutschland diskutiert.[6] Nachdem im Jahr 2001 mehr als fünfzig Menschen im Zusammenhang mit der Einnahme des cholesterinsenkenden Medikaments Lipobay und dessen unvorhergesehener Wechselwirkung mit anderen Medikamenten verstorben waren („Lipobay-Skandal"), arbeitete das BMG unter Ministerin Ulla Schmidt (SPD) nachdrücklich an der Einführung einer eGK. Im Rahmen zweier **Pilotprojekte**, der „Gesundheitskarte Schleswig-Holstein" und der „Gesundheitskarte Düren", wurden erstmals auch in Deutschland E-Rezepte getestet. Dem damaligen Konzept entsprechend wurden diese Rezepte verschlüsselt auf einen zentralen Server geladen und eine Berechtigung zum Abruf der Daten (sogenannte Tickets) anschließend auf der Gesundheitskarte gespeichert. Die Karte fungierte damit als Ticket-Träger. Apotheker konnten Tickets auslesen, Rezepte herunterladen und entschlüsselt in die Warenbewirtschaftung übernehmen.

Nach erfolgreicher Pilotphase forcierte der Gesetzgeber im Jahr 2004 die Einführung der eGK. Mit dem Gesetz zur **Modernisierung** der gesetzlichen Krankenversicherung, (GKV-Modernisierungsgesetz, GMG) beauftragte er die Spitzenorganisationen der Selbst-

6 Bereits 1997 veröffentlichte die Unternehmensberatung Roland Berger & Partner GmbH eine Studie zu den „Perspektiven der Telemedizin in Deutschland". Diese Studie, die im Auftrag des Bundesministeriums für Bildung, Wissenschaft, Forschung und Technologie sowie des Bundesministeriums für Gesundheit erstellt wurde, bewertete das elektronische Rezept als „erste Stufe zur Realisierung einer Gesundheitsplattform" (S. 118).

verwaltung des deutschen Gesundheitswesens damit, bis zum 1. Januar 2006 die erforderliche Infrastruktur für die eGK und ihre Anwendungen zu entwickeln. Der Anwendungsumfang der eGK sollte damals schon ein E-Rezept umfassen. Daher musste die von den Krankenkassen zu entwickelnde eGK ausdrücklich auch dafür geeignet sein, Angaben für die Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form aufzunehmen, § 291a Abs. 2 Nr. 1 SGB V aF. Ein bestimmtes technisches Verfahren zur Realisierung der Anwendungen war im GMG indes nicht vorgesehen. Laut Gesetzesbegründung wurden die gesetzlichen Vorgaben ausdrücklich technikoffen gestaltet, um verschiedene Ansätze zu ermöglichen. Als Beispiele wurden die Speicherung von Daten auf der eGK und – wie in Schleswig-Holstein und Düren – die Bereitstellung von „Schlüssel- und Pointerfunktionen für Datenbestände auf einem Server" genannt.[7] In der Folge wurden vor allem zwei Ansätze für eine Umsetzung des E-Rezepts diskutiert. Ein Ansatz bestand darin, das Rezept dezentral auf der eGK zu speichern. Ärzte, Zahnärzte oder Apotheker sollten nur mit der Einwilligung des Versicherten auf die Rezeptdaten im Speicher der eGK zugreifen können. Der andere Ansatz sah dagegen vor, dass der verschreibende Arzt oder Zahnarzt die Daten an einen zentralen Server übermittelt, wo Apotheker sie bei Einlösen des Rezeptes dann abrufen können.

Der damalige Bundesbeauftragte für den Datenschutz (BfD), Joachim Jacob, hielt beide Lösungswege grundsätzlich für gangbar. Er merkte lediglich an, dass eine Chipkarte mit Prozessor sicherer sei als eine schlichte Speicherchipkarte, und dass eine zentrale Speicherung hohe Anforderungen an die Verfügbarkeit und Sicherheit der entsprechenden Server stelle.[8] An anderer Stelle mahnte er an, dass in jedem Fall die erforderlichen TOM zu ergreifen seien, um die Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit der Patientendaten zu schützen.[9] Beide Ansätze wurden daher abermals getestet.[10]

Verantwortlich für die nähere Ausgestaltung der TI und damit für die Entscheidung zwischen beiden Umsetzungsalternativen und ihre Konkretisierung waren nach § 291a SGB V aF die Selbstverwaltungsorganisationen im deutschen Gesundheitswesen. Sie sollten einstimmig über die Modalitäten eines elektronischen, digitalen oder papierlosen Rezepts entscheiden. Dieser Zwang zur Einstimmigkeit führte in den Augen sowohl der Selbstverwaltung als auch des Gesetzgebers dazu, dass Entscheidungen nicht immer in der gebotenen Zeit getroffen werden konnten.[11] Daher gründeten die Spitzenorganisationen Anfang 2005 eine GmbH, die relevante Entscheidungen mit qualifizierter Mehrheit treffen können sollte: die gematik. Mit dem **Gesetz zur Organisationsstruktur der Telematik im Gesundheitswesen** vom 22. Juni 2005 wurde ein neuer § 291b in das SGB V eingefügt, der die Organisationsstruktur der Gesellschaft regelte. Gesellschafter waren zu diesem Zeitpunkt der Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband, 50 %) sowie die Kassenärztliche Bundesvereinigung (KBV, 15 %), die Deutsche Krankenhausgesellschaft (DKG, 12 %), der Deutsche Apothekerverband (DAV, 8 %), die Bundesärztekammer (BÄK, 5 %), die Bundeszahnärztekammer (BZÄK, 5 %) sowie die Kassenzahnärztliche Bundesvereinigung (KZBV, 5 %). Gesellschafterbeschlüsse konnten nur mit einer Zwei-Drittel-Mehrheit gefällt werden. So war sichergestellt, dass weder Kostenträger noch Leistungserbringer für sich genommen Beschlüsse herbeiführen konnten.

Im November 2005 ordnete das BMG umfangreiche Labor- und Feldtests an. Eine Verordnung über Testmaßnahmen, die 2006 neu verkündet wurde, gab insgesamt vier Teststufen vor, um die technischen Komponenten der eGK und ihr Zusammenspiel zu überprüfen. Nach diversen Schwierigkeiten und Bedenken vor allem seitens der Ärzteschaft[12] startete der sogenannte Basis-Rollout der eGK im Jahr 2009. Dieser Massentest stellte sich aus Sicht der gematik-Gesellschafter und des damaligen Bundesgesundheitsministers, Philipp Rösler (FDP), jedoch nicht als befriedigend heraus. Daher wurde die Einführung des E-Rezepts im Jahr 2010 vorläufig gestoppt und mit einem unbefristeten **Moratorium** belegt. Der Gesundheitsminister wollte zunächst abwarten, bis „die Industrie erst einmal nachweist, dass die gespeicherten Daten technisch sicher sind", bevor er sich abermals an die Realisierung eines E-Rezepts wagen wollte.[13]

7 BT-Drs. 15/1525, S. 144.

8 BfD, Tätigkeitsbericht 1999/2000 (= BT-Drs. 14/5555), S. 160.

9 BfD, 19. Tätigkeitsbericht 2001-2002, S. 146f.

10 Krauskopf/Schneider, Soziale Krankenversicherung, Pflegeversicherung, 59. EL Oktober 2007, SGB V § 291a Rn. 20.

11 BT-Drs. 15/4924, S. 1, 7.

12 Im Mai 2011 sprach sich der 113. Ärztetag dafür aus, das „verfehlte Projekt Elektronische Gesundheitskarte (eGK) in der weiter verfolgten Zielsetzung endgültig aufzugeben". Die neuere Judikatur des Bundesverfassungsgerichts zum Thema Vorratsdatenspeicherung widerspreche „insbesondere auch allen weitergehenden Anwendungen im Rahmen einer Telematikinfrastruktur, wie der Erstellung von E-Rezepten oder elektronischen Patientenakten, die derzeit nur verschoben, nicht aber ad acta gelegt wurden".

13 zit. n. DAZ 52 (2009), S. 1.

Die damals initiierte Bestandsaufnahme endete 2011 mit einem Beschluss der gematik, ihre Entscheidungsstrukturen zu verschlanken. Geteilte Verantwortlichkeiten wurden ersetzt durch spezifische Projektverantwortlichkeiten.[14] Außerdem wurde zur Klärung strittiger Fragen ein Schlichtungsverfahren eingeführt, das bereits mit 50 % der Stimmen initiiert werden konnte. Zwischen 2011 und 2014 wurden insgesamt fünf solcher Verfahren durchgeführt. Zuletzt wurde beispielsweise um die Frage des Speicherortes der Medikationsdaten gestritten. Während die Kostenträger für eine zentrale Speicherung in der TI plädierten, forderten die Leistungserbringer die dezentrale Speicherung auf der eGK.[15] Mit dem Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (**E-Health-Gesetz**) vom 21. Dezember 2015 wurde das Schlichtungsverfahren in § 291c SGB V aF verankert.[16] Zwar konkretisierte das E-Health-Gesetz vom elektronischen Medikationsplan (eMP) bis hin zur ePA zahlreiche Anwendungen der eGK. Das E-Rezept wurde nach dem Moratorium von 2010 allerdings zunächst nicht weiterverfolgt.

Erst im Jahr 2018 wurde die Idee eines E-Rezepts erneut aufgegriffen. Mit dem **Gesetz für mehr Sicherheit in der Arzneimittelversorgung** (GSAV) unter Gesundheitsminister Jens Spahn (CDU) wurde erstmals ein konkreter Plan zur schrittweisen Einführung des E-Rezepts verabschiedet. Durch das GSAV wurden die Spitzenorgane der Selbstverwaltung im Gesundheitswesen durch § 129 Abs. 4a SGB V aF verpflichtet, innerhalb von sieben Monaten nach Inkrafttreten des Gesetzes im August 2019 – also bis Ende März 2020 – die Voraussetzungen für den Einsatz des E-Rezepts zu regeln und solche Vereinbarungen und Verträge anzupassen, die der Verwendung eines solchen Rezeptes entgegenstehen.[17] Zudem wurde die gematik beauftragt, bis zum 30. Juni 2020 die technischen Voraussetzungen zur Einführung elektronischer Verordnungen für apothekenpflichtige Arzneimittel zu schaffen, § 291a Abs. 5d SGB V aF.[18]

Parallel dazu wurden die Organisations- und Entscheidungsstrukturen der gematik abermals reformiert. Im Jahr 2019 beschloss der Deutsche Bundestag das **Terminservice- und Versorgungsgesetz** (TSVG), das – nach einem entsprechenden Änderungsantrag – auch die Übernahme der Mehrheitsanteile der gematik durch den Bund regelte. Für Gesellschafterbeschlüsse sollte fortan eine einfache Mehrheit ausreichen, sofern nicht zwingende Gründe entgegenstanden. Beide Änderungen sollten nach Ansicht des Gesetzgebers der Erleichterung der Beschlussfassung und der Beschleunigung der Verfahren dienen und außerdem verhindern, dass Kostenträger und Leistungserbringer sich gegenseitig blockierten.

Nachdem die gematik die im GSAV geforderten Spezifikationen am Stichtag, dem 30. Juni 2021, verabschiedet hatte, beschloss der Deutsche Bundestag im Juli 2021 das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (**Patientendaten-Schutz-Gesetz, PDSG**). Ziel dieses Gesetzes war erklärtermaßen, die sich durch die Digitalisierung für die medizinische und pflegerische Versorgung bietenden Chancen weiter zu nutzen. Zu diesem Zweck wurde die verpflichtende Einführung des E-Rezepts zunächst zum 1. Januar 2022 beschlossen. Ärzte und Zahnärzte wurden verpflichtet, verschreibungspflichtige Arzneimittel elektronisch zu verordnen und für die Übermittlung an Patienten dieser Verordnung die Dienste und Komponenten der TI zu nutzen. Für Apotheker sah das Gesetz eine korrespondierende Pflicht vor, verschreibungspflichtige Arzneimittel fortan auf Grundlage elektronischer Verordnungen und unter Nutzung der Dienste und Komponenten der TI abzugeben, § 360 Abs. 2 S. 1, Abs. 3 S. 1 SGB V. Außerdem wurde der gematik die Aufgabe übertragen, eine barrierefreie Anwendung für mobile Endgeräte zu entwickeln, die die Übermittlung ärztlicher Verschreibung ermöglichen sollte: die E-Rezept-App. Vorgesehen war nun, das eigentliche Rezept zentral zu speichern. Versicherte sollten über eine Anwendung auf ihrem mobilen Endgerät auf das Rezept zugreifen, es einsehen, löschen und bei einer Apotheke ihrer Wahl einlösen können.[19]

Um die Nutzbarkeit des E-Rezepts in der Fläche zu gewährleisten, wurde im Juni 2021 das Gesetz zur digitalen Modernisierung von Versorgung und Pflege (**Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz, DVPMG**) verabschiedet. Dieses Gesetz verpflichtete weitere Leistungserbringergruppen zum Anschluss an die TI, zudem wurde der gesetzlich vorgegebene Leistungsumfang beträchtlich erweitert: Jeder Versicherte sollte nun die Möglichkeit erhal-

14 Der GKV-Spitzenverband sollte gemeinsam mit der KBV für die Basis-TI und allein für das Versichertenstammdatenmanagement (VSDM) verantwortlich sein, die BÄK für das Notfalldatenmanagement (NFDM), die KBV für die Kommunikation der Leistungserbringer untereinander (Kom-Le) und die DKG für die eFallAkte (eFA).

15 Vorstand der BÄK, Sachstandsbericht über die Zusammenarbeit in der Gesellschaft für Telematikanwendungen der Gesundheitskarte – gematik GmbH, S. 5f.

16 BT-Drs. 257/15, S. 3; Kostorz, in: NZS 2016, 247, 248.

17 BT-Drs. 19/8753, S. 33, 61.

18 BT-Drs. 19/8753, S. 62, 69.

19 BT-Drs. 19/18793, S. 103.

ten, Informationen zu eingelösten E-Rezepten in seine ePA einzustellen und diese als eine Art Medikationsakte zu nutzen. Über die E-Rezept-App sollte es außerdem möglich sein, qualitätsgesicherte Informationen aus dem nationalen Gesundheitsportal beispielsweise hinsichtlich einzelner Arzneimittel, Wirkstoffe oder Indikatoren einzusehen. Jeder Versicherte sollte auf ihn ausgestellte Rezepte allein durch Vorlage eines gültigen Identitätsnachweises einlösen und das E-Rezept somit auch dann nutzen können, wenn er nicht über ein mobiles Endgerät verfügte oder dieses nicht für den Zugriff auf medizinische Anwendungen nutzen wollte.[20] Schließlich sollte die Rezepteinlösung in Apotheken im europäischen Ausland ermöglicht werden.[21]

Im Juli 2021 lief die offizielle **Testphase des E-Rezepts** an. Zunächst wurde noch an der verpflichtenden Einführung zum 1. Januar 2022 festgehalten. Diese Verpflichtung wurde allerdings Ende Dezember 2021 aufgegeben, um weitere Erfahrungen mit dem E-Rezept sammeln und die relevanten Systeme sicher umstellen zu können. Als Zielvorgabe wurde nun bestimmt, dass mindestens 30.000 E-Rezepte erfolgreich eingelöst und abgerechnet werden sollten.

Im April 2022 konnte die gematik die Einlösung von 10.000 E-Rezepten verbuchen. Kurz darauf brachte sie eine Beschlussvorlage in die Gesellschafterversammlung ein, die eine verpflichtende Einführung des E-Rezepts zum 1. September 2022 vorsah. Die KBV kritisierte dieses Vorgehen und argumentierte, die Praxistauglichkeit des E-Rezepts sei bislang nicht nachgewiesen, die Konzeption im vorgelegten Beschluss „erkennbar zum Scheitern verurteilt".[22] Auf einer anschließend einberufenen Sondergesellschafterversammlung wurde daher eine **Verlängerung der Testphase** beschlossen. Erst wenn in Schleswig-Holstein und Westfalen-Lippe bestimmte Erfolgskriterien erfüllt seien und dies von der gematik positiv festgestellt worden sei, sollte – ebenfalls auf freiwilliger Basis – der Einstieg in die nächste Stufe mit zunächst sechs und später acht weiteren Regionen erfolgen. Mindestens 25 Prozent der ausgegebenen Verschreibungen sollten elektronisch ausgestellt werden. Die Quote von Patienten, die aufgrund von Fehlern der Verschreibung zur Praxis zurückkehrte, sollte bei unter drei Prozent liegen. Außerdem sollte gewährleistet sein, dass Patienten umfassend über das E-Rezept informiert werden.

Unterdessen ist die E-Rezept-App verfügbar und einsatzfähig. Die gesetzlich vorgesehenen Funktionalitäten sind vollständig vorhanden.

20 Im Juli 2022 legte die gematik einen entsprechenden Entwurf für ein „Feature: Abruf der E-Rezepte in der Apotheke mit personenbezogenem Identitätsnachweis" vor. Darin wurde beschrieben, dass neben die zwei bestehenden Optionen zur Einlösung eines E-Rezepts – der Einlösung durch Vorlage eines Ausdrucks mit analogem Datencode oder digital mittels der E-Rezept-Anwendung – eine dritte Option treten sollte: die Einlösung durch Vorlage eines Identitätsnachweises des Versicherten, in diesem Fall: der eGK. Gespeichert werden sollte das E-Rezept nicht – wie noch um die Jahrtausendwende herum angedacht – auf der eGK selbst; ihre Vorlage sollte lediglich den Apotheker ermöglichen, alle auf einen Versicherten ausgestellte E-Rezepte aus dem E-Rezept-Fachdienst abzurufen, gematik, Feature: Abruf der E-Rezepte in der Apotheke mit personenbezogenem Identitätsnachweis; dies., Pressemitteilung vom 22. Juli 2022.

21 BT-Drs., 19/27652, S. 82f., 123, 132.

22 KBV, Pressemitteilung vom 16. Mai 2022.

4.3 Erfahrungen in anderen Ländern

Die Entscheidung, medizinische Verordnungen elektronisch zu verschreiben, ist nicht nur in Deutschland gefällt worden. Auch in anderen Ländern wurden Einführung, Umfang und Umsetzung eines elektronischen, digitalen oder papierlosen Rezepts und Wege zur „Dematerialisierung“ des Papierrezepts diskutiert.[23] Bereits im Jahr 2021 kam eine großangelegte Studie der International Pharmaceutical Federation (FIP) daher zum Ergebnis, dass von 78 untersuchten Ländern in Afrika, Amerika, Europa, Südostasien, im östlichen Mittelmeerraum und im Westpazifik bereits 45 Länder (58 %) gesetzliche Regelungen zu elektronischen Verschreibungen getroffen haben.[24]

Eine Studie aus dem Jahr 2019[25] unterschied zwischen drei Grundfunktionen, die das E-Rezept erfüllen könne: der Verordnung selbst, der Ausgabe dieser und dem Bericht über die erfolgte Ausgabe (Report) an den Verordner. Daran anknüpfend wurde weiter zwischen drei Ländergruppen unterschieden: Länder, in denen alle drei Funktionen flächendeckend verfügbar waren und das E-Rezept zudem um eine E-Medikationsliste ergänzt wurde (Australien, Belgien, Dänemark, Estland, Portugal und Schweden); Länder, in denen E-Rezepte regional oder (funktional) begrenzt verfügbar waren (Frankreich[26], Israel, Italien, Kanada, die Niederlande, Spanien oder das Vereinigte Königreich); und Länder, die weder zur ersten noch zur zweiten Gruppe zählten (Österreich, Polen und die Schweiz).

Anhand dieser Einteilung soll die Umsetzung des E-Rezepts in den einzelnen Ländern hier schlaglichtartig und unter besonderer Berücksichtigung des Prüfgegenstandes beleuchtet werden, um diese Erfahrung für die weitere Prüfung verfügbar zu machen.

4.3.1 Spitzengruppe: Australien, Belgien, Dänemark, Estland, Portugal und Schweden

In **Australien** werden E-Rezepte lokal generiert und über kommerzielle Rezeptaustauschdienste (Prescription Exchange Services, PES) an einen Rezeptlieferdienst (Prescription Delivery Service, PDS) übermittelt. Patienten können Rezepte entweder via QR-Codes, sogenannte Tokens, einlösen, oder Apotheken Zugriff auf eine speziell zu diesem Zweck entwickelte Token-Management-Lösung (Active Script List; ASL) einräumen, welche die Verwaltung mehrerer aktiver Rezepte erleichtern soll. Tokens können ausgedruckt, via SMS oder E-Mail übermittelt und in Apps verwaltet werden, die die Agentur für digitale Gesundheit (Digital Health Agency) zuvor einer Datenschutzfolgenabschätzung (Privacy Impact Assessment, PIA) unterzogen und genehmigt hat. Der Verordner generiert das E-Rezept in seiner Praxis, übermittelt es via PES an einen PDS und erstellt zugleich einen entsprechenden Token/Eintrag in der ASL. Der Apotheker erhält via Token/ASL Zugriff auf den PDS (und damit das Rezept). Hat der Patient seine Zustimmung erteilt, werden die Medikationsdaten außerdem in die nationale Plattform für digitale Gesundheitsdaten (My Health Record, MHR) übernommen, wo sie von autorisierten Gesundheitsdienstleistern eingesehen werden können. Patienten können ihre Gesundheitsakte in MHR jederzeit löschen oder den Zugang zu ihr beschränken.

In **Belgien** wurde das E-Rezept (Recip-e) bereits 2013 eingeführt. Seit dem 1. Januar 2020 sind belgische Ärzte grundsätzlich dazu verpflichtet, Verordnungen elektronisch auszustellen. Dies kann prinzipiell auf zwei Arten geschehen: durch die Verwendung ambulant oder stationär eingesetzter Software zur Verwaltung einer elektronischen Patientenakte oder durch die Nutzung eines speziellen Informationssystems zur

23 Vgl. Health Information and Quality Authority, ePrescribing: An International Review (2018); Health Consumer Powerhouse, Euro Health Consumer Index 2018; FIP, Online pharmacy operations and distribution of medicines. Global Survey Report FIP Community Pharmacy Section (2021).

24 FIP, Online pharmacy operations and distribution of medicines. Global Survey Report FIP Community Pharmacy Section (2021), S. 11.

25 Bertelsmann Stiftung, Elektronische Rezepte (2019), abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/VV__SHS_ERezepte.pdf (zuletzt abgerufen am 15.12.2022).

26 Die Entscheidung der Bertelsmann-Studie, Frankreich in die Mittelgruppe einzugruppieren, wird hier nicht nachvollzogen, da Frankreich zwar über eine elektronische Medikationsakte (Dossier Pharmaceutique, DP) verfügt, Rezepte aber derzeit nur vereinzelt – im Rahmen einer Pilotphase – ausstellt. Frankreich hat mit dem Gesetz Nr. 2019-774 über die Organisation und die Transformation des Gesundheitssystems und der Verordnung Nr. 2020-1408 vom 18. November 2020 über die Einführung der elektronischen Verschreibung inzwischen die Grundlage geschaffen, um E-Rezepte bis Ende 2024 einzuführen, dürfte aber, jedenfalls nach momentanem Stand, zur Schlussgruppe gehören.

Beantragung von Rezepten und Autorisierungen (Prescription & Autorisation Requesting Information System, PARIS). Das E-Rezept wird auf einem zentralen Server, dem sogenannten Recip-e-Server, gespeichert. Bis zum 15. September 2021 war ein Verordner verpflichtet, dem Patienten einen Beleg über die Verschreibung auszudrucken und zu übergeben. Seit dem 15. September 2021 ist die Aushändigung eines solchen Ausdrucks allerdings nicht länger zwingend. Der Patient hat die Möglichkeit, einen Beleg digital durch die Tools, die ihm die Verschreibungssoftware zur Verfügung stellt, oder via App (z. B. MyHealthViewer, Mes médicaments) einzusehen oder auf der Seite von MaSanté.be herunterzuladen. Er hat mehrere Möglichkeiten, das E-Rezept einzulösen: indem er das Papierrezept oder einen ausgedruckten oder digital verfügbaren Beleg der Verschreibung in der Apotheke vorzeigt, indem er dem Apotheker einen Ausweis mit eID-Funktion oder seine nationale Registernummer vorlegt.

In **Dänemark** besteht seit 2002 die Möglichkeit, Rezepte elektronisch zu verschreiben. Ärzte nehmen die Verschreibung in ihrem Praxissystem vor; anschließend wird das E-Rezept in eine nationale Gesundheitsdatenbank, die Fælles Medicinkort (FMK), hochgeladen. Patienten können die elektronischen Verschreibungen der letzten beiden Jahre über lokale IT-Lösungen beispielsweise in Arztpraxen oder Krankenhäusern, über das nationale Gesundheitsportal oder über die Medicinkortet-App einsehen; außerdem können sie Dritten dort Zugriff auf ihre Gesundheitsdaten einräumen und nachvollziehen, wer auf diese Daten in der Vergangenheit zugegriffen hat. Ärzte, Krankenpfleger und Apotheker – aber auch häusliche Pflegedienstleister – können auf die Daten dann zugreifen, wenn sie die Patientendaten für eine Behandlung oder eine Medikamentenausgabe benötigen. Rezepte können eingelöst werden, indem ein Patient sich gegenüber einem Apotheker ausweist und seine Gesundheitskarte (Medicinkortet) vorlegt. Der Apotheker kann dann auf das Verschreibungsmodul zugreifen, das Rezept herunterladen und die Bestellung bearbeiten. Die Medikamentenausgabe wird automatisch an den Verschreiber gemeldet; Patienten haben außerdem die Möglichkeit, die Verlängerung einer Verschreibung digital anzufordern.

In **Estland** besteht seit 2010 die Möglichkeit, Medikamente elektronisch zu verschreiben; seit 2019 werden dort 99,9 % aller ausgegebenen Rezepte elektronisch ausgegeben. Ärzte füllen E-Rezepte lokal am Computer aus und übermitteln sie anschließend digital an eine zentrale Rezeptdatenbank. Dort sind elektronische Verschreibungen für Apotheker einsehbar, sobald ein Patient sich in der Apotheke ausgewiesen hat. Der Apotheker kann bereits verschriebene Verordnungen einsehen, alle erforderlichen Informationen in der Rezeptzentrale abrufen – beispielsweise den Abgabestatus – und Notizen hinzufügen. Auf der Seite des estnischen Gesundheitsportal können Patienten alle auf sie ausgestellten Rezepte einsehen.

In **Portugal** wurde das papierlose Rezept (Receita Sem Papel, RSP) 2015 eingeführt. Seit Juli 2022 sind Ärzte generell verpflichtet, Verordnungen papierlos auszustellen. RSP werden lokal – beispielsweise mit den Verschreibungsanwendungen iMED oder Prescrição Eletrónica Médica Móvel (PEM Móvel) – generiert und mit einer qualifizierten elektronischen Signatur signiert; die so signierten Rezepte werden anschließend in einer zentralen Verschreibungsdatenbank (Base de Dados Nacional de Prescrição, BDNP) gespeichert. Der Patient erhält einen Zugangs- und Dispensiercode (Código de Acesso e Dispensa) sowie einen Wahlrechtscode (Código de Direito de Opção) – entweder per E-Mail, per Messenger-Dienst (z. B. WhatsApp) oder in der Form eines ausgedruckten Behandlungsleitfadens (Guia de Tratamento). Dieser Behandlungsleitfaden kann auch über den Bürgerservice im nationalen Gesundheitsportal aufgerufen und ausgedruckt werden. Der Patient übermittelt dem ausgewählten Apotheker das E-Rezept vorab oder zeigt es in der Apotheke vor. Der Zugangs- und Dispensiercode ermöglicht es dem Apotheker auf das E-Rezept zuzugreifen, der Wahlrechtscode ermöglicht dem Patienten ein höherpreisiges Medikament zu wählen.

In **Schweden** wurde 1983 das weltweit erste E-Rezept ausgestellt; inzwischen werden 99 % aller schwedischen Verordnungen elektronisch verschrieben. Seit 2005 haben Patienten die Möglichkeit, Rezepte in regionalen Gesundheitsdatenbanken zu hinterlegen; seit Mai 2021 arbeitet man daran, diese Daten in einer zentralen Datenbank, der Nationalen Arzneimittelliste (Nationella läkemedelslistan, NLL), zusammenzuführen und Rezepte (nur noch) dort zu speichern. E-Rezepte sollen lokal durch Ärzte, Hebammen oder Krankenpfleger erstellt und anschließend in der NLL gespeichert werden. Hinterlegt werden außerdem der Name des Patienten und seine Sozialversicherungsnummer. Gesundheitsdienstleister in ganz Schweden haben über ein spezielles Verschreibungsportal (Förskrivningskollen) Zugriff auf die NLL und können Gesundheitsdaten aus der Datenbank abrufen, wenn der Patient zustimmt. Ohne Zustimmung des Patienten können autorisierte Personen lediglich die Verschreibungen der letzten beiden Jahre einsehen – der Patient hat allerdings die Möglichkeit, diese Ansicht zu beschränken. Er selbst kann seine Daten über die nationalen Gesundheitsportale (Läkemedelskollen, 1177) und die entsprechenden Apps einsehen.

4.3.2 Mittelgruppe: Israel, Italien, Kanada, die Niederlande, Spanien, oder das Vereinigte Königreich.

In **Israel** wurden elektronische Verordnungen im Jahr 2010 eingeführt. Israelische Ärzte sind vertraglich an eine der vier gemeinnützigen Krankenkassen (Kupat Cholim) gebunden. Sie übermitteln Verordnungen elektronisch an die IT-Systeme der mit ihnen kooperierenden Krankenkasse. Bis 2019 war es nur möglich, E-Rezepte bei einer Apotheke einzulösen, die mit der eigenen Krankenkasse kooperiert. Seit 2019 ist es möglich, das Rezept überall einzulösen. Apotheker sind gesetzlich nicht dazu verpflichtet, Rezepte zu bedienen, die auf eine Krankenkasse ausgestellt sind, mit der sie nicht kooperieren. Anders für die Kupat Cholim. Sie müssen Apothekern auf Wunsch des Patienten stets Zugriff auf ihre Rezeptdatenbank einräumen.

In **Italien** findet das E-Rezept seit 2008 Anwendung. Ärzte stellen Patientendaten und Medikationsdaten im Gesundheitskartensystem (Sistema Tessera Sanitaria, STS) ein und übermitteln dem Patienten eine digitale Verschreibungsnummer (Numero di Ricetta Elettronica, NRE) sowie eine – ursprünglich analoge – Erinnerung an die Verschreibung. Um ein Rezept einzulösen, braucht der Patienten bzw. der Apotheker lediglich die NRE. Mit einem Übergangsgesetz, das als Reaktion auf die Covid-19-Pandemie verabschiedet und inzwischen verlängert wurde, führte die Regierung digitale Alternativen für die analoge Verschreibungserinnerung ein. NRE und Verschreibungserinnerung können nun auch über die elektronische Gesundheitsakte (Fascicolo Sanitario Elettronico, FSE) per E-Mail, SMS oder Messenger-Dienst oder per Telefon übermittelt werden.

In **Kanada** liegt der Fokus der nationalen E-Rezept-Infrastruktur (PrescribeIT) auf der sicheren Kommunikation zwischen Ärzten und Apothekern: E-Rezepte werden in PrescribeIT erstellt und verschlüsselt von der ausstellenden Praxis an eine ausgewählte Apotheke übermittelt. Verordner (Ärzte, Krankenpfleger, medizinisches Fachpersonal) können abfragen, ob ein E-Rezept bereits eingelöst wurde und noch nicht eingelöste Verordnungen stornieren, Apotheker können eine Verordnung digital beantragen; außerdem können Fachkräfte verschlüsselt miteinander kommunizieren. Die Medikamentenhistorie des Patienten wird in PrescribeIT gespeichert. Der Patient selbst hat nicht Zugriff auf PrescribeIT, kann aber von den Verantwortlichen Auskunft über die Informationen verlangen, die bei ihnen gespeichert sind.

In den **Niederlanden** wurde 1998 ein elektronisches Verschreibungssystem (Elektronisch Voorschrijf Systeem, EVS) eingeführt, das auf der Grundlage von Anamnese- und Diagnosedaten Medikationsempfehlungen ausgab. Seit 2014 verpflichtet eine Richtlinie der niederländischen Ärztevereinigung (Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst, KNMG) Ärzte dazu, das EVS grundsätzlich für das Ausstellen von Verschreibungen zu nutzen. Das System übermittelt Rezepte an Apotheken, es prüft Verschreibungen auf ihre Stimmigkeit (Dosierung, Dopplungen, Widersprüche) und das verschriebene Medikament auf Verträglichkeit (Wechselwirkungen, Unverträglichkeiten). Rezepte können, wenn der Patient sich bei einer Apotheke seiner Wahl registriert hat, auch elektronisch an diese Apotheke übermittelt werden.

In **Spanien** ist Gesundheitspolitik nicht Aufgabe der Zentralregierung, sondern der 17 autonomen Regionen. Nicht alle Regionen bieten einen E-Rezept-Dienst an. Die Regionen, die E-Rezepte anbieten, nutzen eine eigene Infrastruktur, die allerdings auf interoperabler Grundlage betrieben wird. So kann ein E-Rezept, das in einer Region ausgestellt wurde, auch in einer anderen eingelöst werden. Das älteste Verschreibungssystem Spaniens, das Elektronische Rezept des öffentlichen Gesundheitssektors Andalusiens (Receta Electrónica del Sistema Sanitario Publico De Andalucía, Receta XXI), wird seit 2003 kontinuierlich entwickelt und betrieben. Angeschlossene Gesundheitszentren, Kliniken und Arztpraxen können via Receta XXI Verordnungen ausstellen, einsehen und ändern, ihre Einlösung überwachen und miteinander kommunizieren. Receta XXI ist Teil des übergreifenden Diraya-Systems. Über Diraya sind verschiedene Systeme und Elemente miteinander vernetzt, die individuelle Gesundheitsdaten wie die Medikationshistorie eines Patienten erfassen und in einer digitalen Gesundheitsakte (Historia de Salud Digital Única de Andalucía, HSDA) speichern. Ein E-Rezept kann auf zwei Arten verordnet werden: durch ein zunächst analoges Rezept, dessen Inhalt dann in der HSDA nachgetragen wird, oder durch ein vollständig digitales Rezept, das via Receta XII direkt in der HSDA erstellt und dort gespeichert wird. Patienten haben auch in diesem Fall das Recht auf einen analogen Ausdruck und Zugang zu den Daten, die in der HSDA gespeichert sind.

Im **Vereinigten Königreich** existiert ein elektronischer Rezeptdienst (Electronic Prescription Service, EPS), der die Übermittlung von E-Rezepten zwischen Verordnern (Allgemeinmedizinern, Krankenpflegern), Apothekern und der zentralen Rechnungsstelle (NHS Business Service Authority, NHSBSA) ermöglicht. Die Teilnahme am EPS ist freiwillig und erfolgt (nur) mit Einwilligung des Patienten. Elektronische Verordnungen werden über ein zentrales System namens Spine gesendet, das den sicheren Austausch von Gesundheitsdaten und Pflegeinformationen von Patienten zwischen unterschiedlichen Institutionen ermöglichen soll. Zunächst wird das E-Rezept vorbereitet und einem Verordner zugewiesen; der Verordner signiert das E-Rezept dann elektronisch und übermittelt es anschließend in Spine, wo der Apotheker es herunterladen kann. In Spine finden sich die gesammelten Behandlungsunterlagen (Summary Care Records,) eines Patienten, die aus den Patientenakten erstellt werden und die von autorisiertem Fachpersonal eingesehen werden können.

4.3.3 Schlussgruppe: Österreich, Polen und die Schweiz

Nach einer erfolgreichen Pilotphase in Kärnten erfolgt seit Anfang 2022 schrittweise die Einführung des E-Rezepts in ganz **Österreich**. Dabei ist vorgesehen, dass Ärzte ein E-Rezept lokal erstellen, die Daten verschlüsselt über das Gesundheitsinformationsnetz übermitteln und es anschließend zentral – im sogenannten e-card System – speichern. Bis zur flächendeckenden Einführung des E-Rezeptes wird dem Patienten entweder eine analoge Kopie des E-Rezepts ausgehändigt oder eine digitale Kopie übermittelt, die in beiden Fällen einen QR-Code und eine alphanumerische e-Rezept ID (REZ-ID) enthält. In der Apotheke wird der Code gescannt und das e-Rezept aus dem e-card-System heruntergeladen. Patienten können ihre E-Rezepte über die Internetseiten ihrer Sozialversicherung oder die entsprechende App einsehen.

Seit Januar 2019 ist es auch in **Polen** möglich, elektronische Rezepte auszustellen und einzulösen. Seit dem 8. Januar 2020 sind Ärzte verpflichtet, Verordnungen elektronisch auszustellen. Rezepte werden zentral in der elektronischen Gesundheitsakte (Internetowe Konto Pacjenta, IKP) gespeichert. Es gibt vier Möglichkeiten, das E-Rezept einzulösen: Patienten erhalten – wenn sie die entsprechenden Daten im IKP hinterlegt und die entsprechende Option ausgewählt haben – entweder einen Zugriffscode per SMS oder einen QR-Code per E-Mail, einen Ausdruck oder eine Benachrichtigung in der myIKP-App.

In der **Schweiz** wurde Anfang 2020 die Verordnung über die Arzneimittel reformiert, um die elektronische Übermittlung von Rezepten und ihre Integration in das elektronische Patientendossier zu ermöglichen. Im August 2022 startete der Anbieter OnlineDoctor die erste Testphase auf dem Schweizer Markt. Ärzte erstellen dort ein E-Rezept in einer zugelassenen Web-Anwendung, signieren es und laden es anschließend bei OnlineDoctor hoch. Dort kann der Patient das Rezept dann einsehen und an eine teilnehmende Versand- oder Vor-Ort-Apotheke übermitteln. Weitere Anbieter, die ein E-Rezept planen, sind FMH und pharmaSuisse.

4.3.4 Das E-Rezept im Ländervergleich

Dieser kursorische Überblick zeigt, dass E-Rezepte weltweit auf dem Vormarsch sind. Selbst Länder, in denen zum Stichtag im Jahr 2019 noch keine E-Rezepte im Umlauf waren (Österreich, Polen, Schweiz) oder in denen E-Rezepte bislang nur mit eingeschränktem Funktionsumfang angeboten wurden (Israel, Italien), haben zwischenzeitlich zur Spitzengruppe aufgeschlossen. In Polen ist es sogar gelungen, in nur kurzer Zeit in die Riege der Länder aufzusteigen, deren E-Rezepte innerhalb Europas interoperabel genutzt werden können (Estland, Finnland, Kroatien und Portugal). E-Rezepte werden dabei eigentlich immer zentral gespeichert, sodass für das Abrufen prinzipiell die Identifikation des Patienten ausreicht. Eine dezentrale Speicherung auf der Gesundheitskarte ist derzeit nirgendwo realisiert. In einigen Ländern (Italien, Polen, Portugal, Österreich) benötigt man jedoch einen Code, eine Nummer oder einen Token, um auf das Rezept zuzugreifen.

E-Rezept-Anwendungen für mobile Endgeräte werden nicht in allen Ländern genutzt. Wo sie nicht genutzt werden, werden Verweise auf das E-Rezept per E-Mail, per Anruf, SMS oder sogar per Messenger versendet. Wo sie genutzt werden, werden diese Anwendungen teilweise vom Staat entwickelt oder zur Verfügung gestellt (Dänemark, Österreich, Schweden). Manchmal handelt es sich um Zusatzfunktionen der Verschreibungssoftware (Belgien) oder um Angebote privater Dienstleister (Schweiz). Allerdings stellen fast alle Staaten eine digitale Gesundheitsplattform zur Verfügung, auf der Patienten ihre Gesundheitsdaten einsehen können. Ausnahmen werden vor allem dort gemacht, wo E-Rezepte direkt von Ärzten an Apotheker oder Krankenkassen übermittelt werden (Israel, Kanada). Auch zirkuliert eine Reihe von Anwendungen, die zwar elektronische Verschreibungen nicht unterstützen, aber andere Funktionalitäten bieten, wie z. B. die Suche nach einem Behandler in der Nähe.

Das hängt auch damit zusammen, dass die Einführung und Entwicklung elektronischer Verschreibungen mehreren Zwecken dient und unterschiedliche Zwecke jeweils im Fokus stehen: Vielfach geht es darum, Prozesse zu verbessern, Fehlerquellen zu eliminieren oder Aufwand und Kosten zu senken; manchmal (z. B. in Skandinavien) geht es aber auch darum, die Gesundheitsversorgung zu optimieren oder (z. B. in Südwesteuropa) darum, Korruption zu bekämpfen. Daran orientiert sich dann die konkrete Ausgestaltung und der Funktionsumfang des E-Rezepts.

4.4 Aufgaben, Aufträge und Pflichten der gematik

Mit der Einführung einer E-Rezept-Anwendung bezweckt der deutsche Gesetzgeber in erster Linie die Chancen, die die Digitalisierung für die medizinische und pflegerische Versorgung in Deutschland bietet, weiter zu nutzen. Im Vordergrund stehen – neben der Versorgungssicherheit – vor allem Datenschutz, Komfort und Patientenautonomie. Jeder Versicherte soll die Möglichkeit erhalten, auf ihn ausgestellte Verordnungen elektronisch zu verwalten; außerdem soll es über die E-Rezept-Anwendung möglich sein, qualitätsgesicherte Informationen beispielsweise hinsichtlich einzelner Arzneimittel, Wirkstoffe oder Indikatoren einzusehen. Zu diesem Zweck hat der Gesetzgeber der gematik bereits im Jahr 2019 aufgetragen, die Voraussetzungen für die Übermittlung ärztlicher Verordnungen für apothekenpflichtige Arzneimittel in elektronischer Form zu schaffen, Nr. 16 Art. 12 des Gesetzes für mehr Sicherheit in der Arzneimittelversorgung. Mit dem PDSG wurden Aufgaben, Aufträge und Pflichten der gematik dann neu gefasst und im SGB V verankert.

4.4.1 Aufgaben der gematik

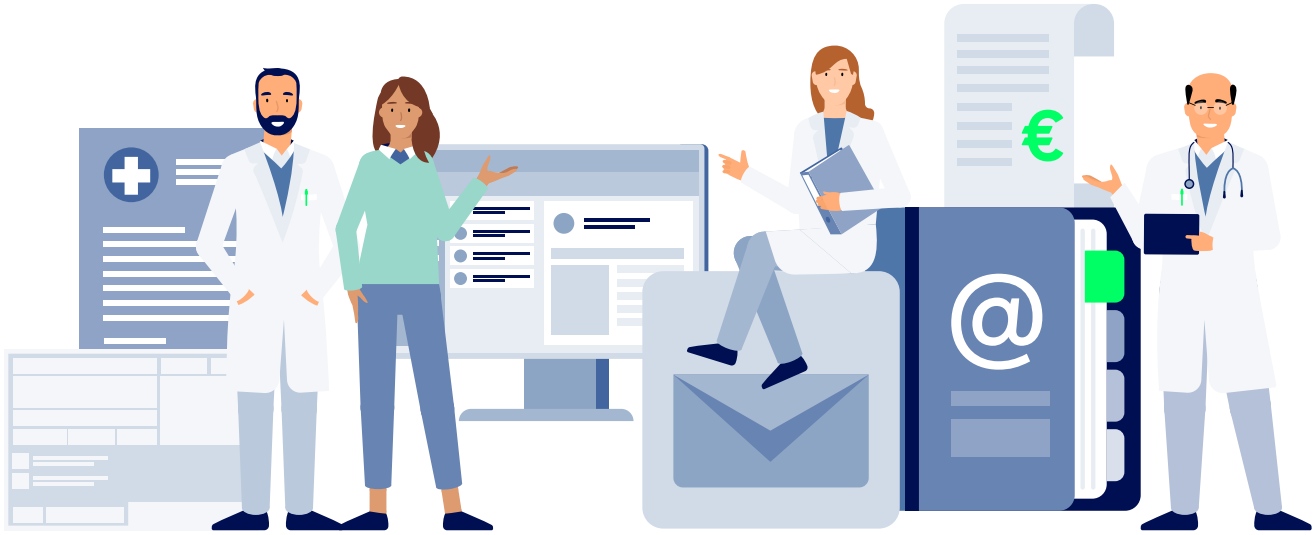
Nach § 311 Abs. 1 Nr. 10 SGB V hat die gematik insbesondere die Aufgabe, solche Komponenten der TI als Dienstleistungen von allgemeinem wirtschaftlichem Interesse zu entwickeln und zur Verfügung zu stellen, die den Zugriff der Versicherten auf die Anwendung zur Übermittlung ärztlicher Verordnungen im Sinne des § 334 Abs. 1 S. 2 Nr. 6 („elektronische Verordnungen“) nach Maßgabe des § 360 Abs. 10 SGB V[27] ermöglichen.

4.4.2 Aufträge der gematik

In § 312 SGB V hat der Gesetzgeber diese Aufgabe durch eine Reihe weitergehender Aufträge spezifiziert. So soll die gematik insbesondere die erforderlichen Maßnahmen treffen, damit

- vertragsärztliche elektronische Verordnungen für apothekenpflichtige Arzneimittel elektronisch übermittelt werden können (Nr. 1),
- vertragsärztliche elektronische Verordnungen für Betäubungsmittel sowie für Arzneimittel nach § 3a Abs. 1 S. 1 der Arzneimittelverschreibungsverordnung elektronisch übermittelt werden können (Nr. 2),
- den Versicherten Dispensierinformationen über das auf der Grundlage der vertragsärztlichen Verordnung nach den Nr. 1 oder 2 abgegebene Arzneimittel, dessen Chargennummer und ggf. Dosierung elektronisch verfügbar gemacht werden können (Nr. 3),
- zugriffsberechtigte Leistungserbringer mittels der elektronischen Gesundheitskarte sowie entsprechend den Zugriffsvoraussetzungen nach § 361 Abs. 2 SGB V auf elektronische Verordnungen zugreifen können (Nr. 6),
- vertragsärztliche elektronische Verordnungen von digitalen Gesundheitsanwendungen durch Ärzte, Zahnärzte und Psychotherapeuten ab dem 1. Januar 2023 elektronisch übermittelt werden können (Nr. 7),

27 Bei dem Verweis auf § 360 Abs. 5 SGB V dürfte es sich um ein redaktionelles Versehen handeln. Dem § 360 Abs. 5 SGB V in der bis zum 8. Juni 2021 geltenden Fassung entspricht der heute geltende § 360 Abs. 10 SGB V.



- vertragsärztliche elektronische Verordnungen von häuslicher Krankenpflege nach § 37 SGB V sowie außerklinischer Intensivpflege nach § 37c SGB V elektronisch übermittelt werden können (Nr. 12) und

- vertragsärztliche elektronische Verordnungen von Soziotherapien nach § 37a SGB V durch Ärzte und Psychotherapeuten elektronisch übermittelt werden können (Nr. 13).

Außerdem wurde der gematik der Auftrag zur Schaffung der technischen Voraussetzungen und Festlegung der entsprechenden Verfahren erteilt, damit Versicherte bestimmte Daten einer elektronischen Verordnung ihrer Krankenkasse vor Inanspruchnahme der jeweils verordneten Leistungen elektronisch zur Bewilligung übermitteln können, § 312 Abs. 7 (in Verbindung mit § 312 Abs. 1 S. 1 Nr. 1, 2, 12, 13 und 16 bzw. § 360 Abs. 2, 5, 6 oder 7 SGB V).

Die gematik hat diese Aufträge in bestimmten Zeitetappen bis zum 1. Juli 2024 zu erfüllen.

4.4.3 Pflichten der gematik

In § 360 Abs. 10 und 12 SGB V werden die Aufgaben und Aufträge der gematik weiter um bestimmte Pflichten ergänzt. Nach § 360 Abs. 10 S. 1 SGB V ist die gematik dazu verpflichtet, die Komponenten der TI, die den Zugriff der Versicherten auf E-Rezepte ermöglichen, als Dienstleistung von allgemeinem wirtschaftlichem Interesse zu entwickeln und zur Verfügung zu stellen. Gemäß § 360 Abs. 10 S. 3 und 4 SGB V hat sie Funktionsfähigkeit und Interoperabilität dieser Komponenten sicherzustellen und die Sicherheit der Komponenten des Systems durch ein externes Sicherheitsgutachten nachzuweisen. Sie ist außerdem verpflichtet, die Voraussetzungen dafür zu schaffen, dass Versicherte über diese Komponenten auf Informationen des Nationalen Gesundheitsportals nach § 395 SGB V zugreifen können. Auch müssen den Versicherten die Informationen des Portals mit Daten, die in ihrer elektronischen Verordnung gespeichert sind, verknüpft angeboten werden können, § 360 Abs. 12 Nr. 1 SGB V. Schließlich muss die gematik die Voraussetzungen dafür schaffen, dass Versicherte über diese Komponenten, nach vorheriger Einwilligung und technischer Freigabe, Daten ihrer elektronischen Verordnung prinzipiell der nationalen eHealth-Kontaktstelle anderer Mitgliedstaaten der Europäischen Union übermitteln können, § 360 Abs. 12 Nr. 2 SGB V.

4.5 Technische Umgebung und Komponenten des E-Rezept-Systems

Die E-Rezept-App ist eine Komponente der deutschen Fachanwendung E-Rezept und über verschiedene Schnittstellen mit verschiedenen Komponenten und Diensten innerhalb und außerhalb der TI verbunden. Nachfolgend werden zunächst die TI und die Fachanwendung E-Rezept näher beschrieben. In einem zweiten Schritt werden die wesentlichen Funktionen der E-Rezept-App skizziert, um das Ineinandergreifen der dezentralen und zentralen Komponenten und Dienste im Prozess der elektronischen Verordnung und bei der Nutzung der E-Rezept-App zu veranschaulichen. Da es sich beim Prüfgegenstand um eine mobile Anwendung für Smartphones handelt und Apps zwingend auf die Nutzung gewisser Funktionalitäten und Konnektivitäten des Smartphones und seines Betriebssystems angewiesen sind, werden abschließend die Betriebssystemdienste erörtert, die ebenfalls zur näheren technischen Umgebung des Prüfgegenstandes gehören.

4.5.1 Komponenten und Dienste der TI

Die TI ist definiert als interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur, die der Vernetzung von Leistungserbringern, Kostenträgern, Versicherten und weiteren Akteuren des Gesundheitswesens sowie der Rehabilitation und der Pflege dient, § 306 Abs. 1 S. 2 SGB V. Ihre technische Struktur ist im SGB V vorgegeben. Danach umfasst die TI drei verschiedene Zonen („Infrastrukturen“) mit je eigenen Netzen, in denen unterschiedliche Akteure den Betrieb eines je eigenen Teils der TI verantworten, § 306 Abs. 2 SGB V. Zu unterscheiden sind eine dezentrale Infrastruktur, eine zentrale Infrastruktur und eine Anwendungsinfrastruktur.

4.5.1.1 Dezentrale Infrastruktur

Die dezentrale Infrastruktur besteht aus den in den Leistungserbringerumgebungen befindlichen Komponenten der TI zur Authentifizierung und zur elektronischen Signatur (d. h. Kartenterminals und Authentifikationskarten wie den elektronischen Heilberufsausweis), zur Verschlüsselung und Entschlüsselung sowie zur sicheren Verarbeitung von Daten in der zentralen Infrastruktur (d. h. Konnektoren), § 306 Abs. 2 Nr. 1, Abs. 4 S. 3 SGB V.

4.5.1.2 Zentrale Infrastruktur

Die zentrale Infrastruktur besteht aus sicheren Zugangsdiensten als Schnittstelle zur dezentralen Infrastruktur (VPN-Zugangsdienst) sowie dem gesicherten Netz und den hierfür betriebenen Diensten, § 306 Abs. 2 Nr. 2, Abs. 4 S. 2 SGB V.[28]

4.5.1.3 Anwendungsinfrastruktur

Die Anwendungsinfrastruktur besteht aus Diensten für Anwendungen nach Kapitel 11 des SGB V, § 306 Abs. 2 S. 1 Nr. 3 SGB V (Fachdiensten und Fachanwendungen). Fachanwendungen in diesem Sinne sind gemäß § 334 Abs. 1 S. 2 SGB V:

- die elektronische Patientenakte nach § 341 (Nr. 1),
- Hinweise der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen zur Organ- und Gewebespende (Nr. 2),
- Hinweise der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Vorsorgevollmachten oder Patientenverfügungen nach § 1901a BGB (Nr. 3),
- der Medikationsplan nach § 31a einschließlich Daten zur Prüfung der Arzneimitteltherapiesicherheit (elektronischer Medikationsplan; Nr. 4),
- medizinische Daten, soweit sie für die Notfallversorgung erforderlich sind (elektronische Notfalldaten; Nr. 5),
- elektronische Verordnungen (das „E-Rezept“) (Nr. 6) und
- die elektronische Patientenkurzakte nach § 358 SGB V (Nr. 7).

28 Auch sogenannte zentrale Dienste. Ein Beispiel für einen zentralen Dienst ist der von der gematik betriebene Verzeichnisdienst, § 313 SGB V.

Weitere Anwendungen der TI ohne Nutzung der eGK nach § 327 SGB V können darüber hinaus durch die gematik bestätigt werden.

Der Betrieb der Dienste der Anwendungsinfrastruktur erfolgt durch den jeweiligen Anbieter, § 307 Abs. 4 S. 1 SGB V.

4.5.2 Fachanwendung E-Rezept

Aus Anwendungs- und Nutzerperspektive umfasst die Fachanwendung E-Rezept im Wesentlichen die E-Rezept-App, den E-Rezept-Fachdienst, den Identitätsdienst, das Apothekenverzeichnis sowie die Schnittstellen der IT-Systeme der verordnenden und abgebenden Leistungserbringer (Ärzte, Zahnärzte und Apotheker).

4.5.2.1 E-Rezept-App

Die E-Rezept-App ermöglicht Nutzern den Zugriff und die Verwaltung von E-Rezepten auf mobilen Endgeräten. Im Zusammenspiel mit anderen Bestandteilen der Fachanwendung E-Rezept – dem E-Rezept-Fachdienst, dem Identitätsdienst und dem Apothekenverzeichnis – versetzt sie Nutzer in die Lage, E-Rezepte einzuscannen oder papierlos zu empfangen, elektronisch (online oder vor Ort) bei einer Apotheke einzulösen, eine Apotheke zu suchen und mit Apotheken zu kommunizieren. Der Import von E-Rezepten durch Scan und das Einlösen vor Ort in der Apotheke stehen als Funktion auch dann zur Verfügung, wenn die E-Rezept-App ohne Verbindung zu den anderen Komponenten genutzt wird. **Anbieter der E-Rezept-App ist die gematik.**

4.5.2.2 E-Rezept-Fachdienst

Der Fachdienst ist ein zentrales Serversystem in der Anwendungsinfrastruktur zur Ausführung der Fachanwendung E-Rezept. Er setzt die E-Rezept-Workflows um, speichert also beispielsweise die E-Rezepte des Versicherten, protokolliert die Zugriffe auf das E-Rezept und verwaltet die entsprechenden Statusübergänge; außerdem ermöglicht der Fachdienst den Nachrichtenaustausch zwischen Apothekern und Versicherten. **Anbieter des E-Rezept-Fachdienstes ist die IBM Deutschland GmbH.**

4.5.2.3 Identitätsdienst

Um die Berechtigung von Zugriffen auf Daten zu überprüfen, die im E-Rezept-Fachdienst gespeichert sind, sehen die Spezifikationen der gematik die Verwendung eines Identitätsdienstes vor. Der Identitätsdienst fungiert als Identity Provider (IDP) für den E-Rezept-Fachdienst und überprüft und bestätigt gegenüber dem E-Rezept-Fachdienst die Identität und Zugangsberechtigung von Personen und Geräten, die versuchen, auf Daten im E-Rezept-Fachdienst zuzugreifen.

Zur Verbesserung des Bedienkomforts bietet die App dem Nutzer nach erfolgreicher Authentifizierung die Option „Zugangsdaten speichern“ zum lokalen Speichern der für den Zugang zum E-Rezept-Fachdienst benötigten Daten an, sofern das Betriebssystem des Endgeräts des Nutzers über eine Vorrichtung verfügt, mit dem Daten auf dem Endgerät in einem speziellen Bereich sicher gespeichert werden können (Secure Module). Wird diese Funktion gewählt, erzeugt die App eine Geräteidentität, die durch den Identitätsdienst verwaltet wird. **Anbieter des IDP-Dienstes ist die Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH.**

4.5.2.4 Schnittstellen der IT-Systeme der verordnenden und abgebenden Leistungserbringer

Zu den IT-Systemen der verordnenden und abgebenden Leistungserbringer zählen Apotheken- und Praxisverwaltungssoftware (AVS bzw. PVS) sowie Krankenhausinformationssysteme (KIS). Diese Systeme dienen den jeweiligen Leistungserbringern zu Verwaltungszwecken sowie zur Primärdokumentation in ihrer alleinigen Verantwortung. Über die Schnittstellen der PVS und KIS können E-Rezepte elektronisch auf dem E-Rezept-Fachdienst von Ärzten und Zahnärzten eingestellt und von Apotheken mittels AVS abgerufen werden.

4.5.2.5 Apothekenverzeichnis

Die Apothekensuche in der E-Rezept-App nutzt die Datenbank des Apothekenverzeichnisses. Das Apothekenverzeichnis ergänzt die Apothekenbasisdaten des elektronischen Verzeichnisdienstes der TI (§ 313 SGB V) um weitere Inhalte.

Die Apothekenbasisdaten des zentralen Verzeichnisdienstes werden durch die Apothekenkammern gepflegt. Zu diesen Daten gehören z. B. Adressierungsinformationen innerhalb der TI, Basis-Kontaktdaten und Anschrift.

Die ergänzenden Inhalte des Apothekenverzeichnisses werden von den Apotheken oder deren Dienstleistern selbst eingepflegt. Hierbei handelt es sich z. B. um Öffnungszeiten, weitere Kontaktdaten, angebotene Dienstleistungen oder technische Informationen.

Der Deutsche Apothekerverband e.V. (DAV) betreibt das Apothekenverzeichnis im Auftrag der gematik (§ 311 Abs. 5 SGB V). Dabei setzt der DAV die Netzgesellschaft Deutscher Apotheker mbH (NGDA) als Subunternehmer ein.

4.5.3 Betriebssystemdienste

Jede App ist zwingend auf die Funktionalitäten und Konnektivitäten des Smartphones sowie auf Betriebssystemfunktionen angewiesen. Diese werden durch das Betriebssystem als standardisierte Dienste über lokale oder an Server-Endpunkten bereitgestellte Schnittstellen (API) bereitgestellt.[29] Dabei handelt es sich einerseits um technisch zwingende Betriebssystemdienste in dem Sinne, dass keine App auf ihre Nutzung verzichten kann, da andernfalls selbst grundlegende Funktionen jeder App (z. B. Speichern von Daten, Anzeige von Inhalten, Einbindung von Schaltflächen) nicht bereitgestellt werden können (essentielle Betriebssystemdienste). Teilweise handelt es sich auch um Betriebssystemdienste, mit denen Funktionen bereitgestellt werden, die grundsätzlich auch mit selbst entwickelten oder Diensten von anderen Anbietern realisiert werden könnten oder unter Inkaufnahme insbesondere von Komfort- oder Sicherheitsnachteilen verzichtbar wären, weil sie für die Funktionsfähigkeit der Kernfunktionen der jeweiligen App nicht benötigt werden (nicht-essentielle Betriebssystemdienste). Dazu zählen im Fall der E-Rezept-App die Standard-Betriebssystemdienste für Push-Mitteilungen Firebase Cloud Messaging (FCM), Huawei Pushkit und Apple Push Notification (APN) sowie die Integritätsprüfungs-Dienste Google SafetyNet Attestation, Huawei Safety Detect SysIntegrity und Apple DeviceCheck. Im Fall der Android- und der EMUI-Version der App wird zudem ein spezieller Betriebssystemdienst für das Scannen von Barcodes genutzt (Google ML Kit/Huawei ML Kit).

29 Für die Nutzung einiger Betriebssystemdienste kann es außerdem erforderlich sein, dass bestimmte Softwaremodule wie Programmbibliotheken oder SDK in die App integriert werden.

4.6 Akteure und betroffene Personen

Verschiedene Akteure sind auf unterschiedliche Art und Weise mit der E-Rezept-Anwendung befasst oder von ihrer Umsetzung betroffen. Akteure und betroffene Personen zählen damit gleichermaßen zum Kontext des Prüfgegenstandes.

4.6.1 gematik

Die gematik ist eine Betriebsorganisation der Spitzenorganisationen des deutschen Gesundheitswesens, die sich mehrheitlich in der Hand des Bundes befindet. Sie wurde 2005 als „gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH" gegründet, um die Einführung, Pflege und Weiterentwicklung der elektronischen Gesundheitskarte zu betreiben und zu begleiten. Ihre Geschäftsanteile sind immer wieder neu verteilt worden[30] und entfallen derzeit zu 51% auf die Bundesrepublik Deutschland, vertreten durch das BMG, zu 22,05% auf den GKV-Spitzenverband und zu 24,5% auf die anderen in § 306 Abs. 1 S. 1 SGB V genannten und in § 310 Abs. 3 SGB V vorgesehenen Organisationen[31], § 310 Abs. 2 und Abs. 3 SGB V. Die Finanzierung der gematik ist ebenfalls gesetzlich geregelt. Der GKV-Spitzenverband finanziert die Arbeit der gematik jährlich zu 93% mit einem Betrag in Höhe von 1,50 Euro[32] je Mitglied der Gesetzlichen Krankenversicherung, § 316 Abs. 1 S. 1 SGB V. Der Verband der Privaten Krankenversicherung trägt die übrigen 7% der Finanzierung.

Nach § 311 Abs. 1 Nr. 1 und 2 SGB V hat die gematik die Aufgabe, die TI aufzubauen und auszubauen, die Rahmenbedingungen für Betriebsleistungen und die Auftragsvergabe an Anbieter solcher Leistungen festzulegen.[33] Nach § 311 Abs. 1 Nr. 10 und § 360 Abs. 10 ist die gematik außerdem verpflichtet, die Komponenten der TI, die den Zugriff der Versicherten auf die elektronische ärztliche Verordnung nach § 334 Abs. 1 S. 2 Nr. 6 (nach Maßgabe des § 360 Abs. 10 SGB V) ermöglichen, als Dienstleistung von allgemeinem wirtschaftlichem Interesse zu entwickeln und zur Verfügung zu stellen.[34]

Diese Doppelstellung der gematik als Hersteller und Anbieter auf der einen und als spezifizierende Stelle der E-Rezept-Komponenten auf der anderen Seite könnte möglicherweise den Eindruck der Befangenheit erwecken.[35] Um diesem potentiellen Risiko wirksam zu begegnen, wurde die Entwicklung des E-Rezepts von vornherein einer umfassenden unabhängigen Kontrolle unterstellt. Die gematik hat relevante Festlegungen, Maßnahmen und Beschlüsse im Einvernehmen oder im Benehmen mit dem BSI oder dem BfDI zu treffen bzw. dem BSI oder dem BfDI Informationen zu übermitteln, vgl. §§ 311 Abs. 2 S. 1, Abs. 6 S. 1; 312 Abs. 1 Nr. 14, Abs. 9; 315 Abs. 2; 323 Abs. 2 S. 9; 325 Abs. 3 S. 2, 3 und 5, Abs. 4 S. 2, Abs. 5 S. 2, Abs. 6; 327 Abs. 2 S. 2, 4 und 6; 331 Abs. 1, Abs. 3 S. 2, Abs. 5 S. 2; 340 Abs. 8 S. 2; 360 Abs. 10 S. 5 ff SGB V und unterliegt darüber hinaus noch weiteren, umfassenden Informations- und Rechenschaftspflichten. Die gematik hat unter anderem das BSI über Gefahren, Maßnahmen der Gefahrenabwehr, gemeldete oder sonst bedeutende Störungen, erkannte Sicherheitsmängel sowie über die Erfüllung der Anforderungen an die Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der TI zu informieren, §§ 329 Abs. 1 S. 2, Abs. 4, 330 Abs. 3 S. 1 SGB V. Auf Verlangen hat sie dem BSI die in § 333 Abs. 1 SGB V genannten Unterlagen und Informationen vorzulegen. Ergibt eine Bewertung dieser Informationen Sicherheitsmängel, so kann das BSI der gematik verbindliche Anweisungen zur Beseitigung der festgestellten Sicherheitsmängel erteilen, § 333 Abs. 2 SGB V.

30 Vgl. oben 4.2

31 Bundesärztekammer (2,45%), Bundeszahnärztekammer (2,45%), Deutsche Apothekerverband (3,92%), Deutsche Krankenhausgesellschaft (5,88%), Kassenzahnärztliche Bundesvereinigung (7,35%) und der Verband der Privaten Krankenversicherung (2,45%, vgl. https://www.gematik.de/ueber-uns/struktur).

32 Das Bundesministerium für Gesundheit kann diesen Betrag entsprechend dem Mittelbedarf der gematik durch Rechtsverordnung anpassen, § 316 Abs. 1 S. 2 SGB V.

33 Zu den weiteren Aufgaben der gematik, siehe oben 4.4.

34 Zur Qualifikation der E-Rezept-App als (dezentrale) Komponente, siehe unten 7.2.3.1.1.

35 Vgl. BfDI, Tätigkeitsbericht 2020, S. 39.

Im Falle des E-Rezepts hat die gematik die Sicherheit, Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der von ihr entwickelten und zur Verfügung gestellten Komponenten und Dienste außerdem durch ein externes Sicherheitsgutachten nachzuweisen, § 360 Abs. 10 S. 3 und 4 SGB V. Die gematik legt im Einvernehmen mit dem BSI ein Prüfverfahren für das Sicherheitsgutachten fest. Das BSI prüft und bestätigt dieses Gutachten anschließend, § 360 Abs. 10 S. 5 und 6 SGB V. Erst mit Bestätigung des BSI dürfen die Komponenten und Dienste durch die gematik zur Verfügung gestellt werden, § 360 Abs. 10 S. 7 SGB V.

Im Juni 2021 erfolgte die Erstellung des vorbezeichneten Gutachtens mit dem Ergebnis:

„Die Produktgutachter sind der Auffassung, dass das eRp-FdV[36] und die normativen Festlegungen, beziehungsweise Anforderungen zur Telematikinfrastruktur (im Folgenden „TI“ genannt) des deutschen Gesundheitswesens für den Online-Produktivbetrieb, nach reiflicher Begutachtung und Bewertung den sicherheitstechnischen sowie datenschutzrechtlichen Anforderungen der gematik entsprechen und somit geeignet sind, Teil der TI des Produkttyp eRp-FdV einschließlich der durch ihn bereitgestellten Schnittstellen zu werden. Einer kontrollierten Inbetriebnahme in den Produktionsbetrieb steht aus Sicht der Gutachter nichts im Wege.“[37]

4.6.2 Gesellschafter der gematik

Die Gesellschafter der gematik – mit Ausnahme des Verbandes der Privaten Krankenversicherungen (PKV) – sind gemäß § 306 Abs. 1 SGB V gleichermaßen mit der Schaffung der TI im Allgemeinen betraut.

4.6.2.1 Bundesministerium für Gesundheit (BMG)

Das BMG ist eine oberste Bundesbehörde. Es ist dem Bundesminister für Gesundheit unterstellt, der seinerseits auf Vorschlag des Bundeskanzlers vom Bundespräsidenten ernannt wird und als Bundesminister Teil der Bundesregierung ist, Art. 62, 64 Abs. 1 GG. Im Zusammenhang mit der Digitalisierung des Gesundheitswesens im Allgemeinen und der E-Rezept-Anwendung im Besonderen erfüllt das BMG verschiedene Aufgaben. Insbesondere schafft das BMG für die Bundesrepublik Deutschland – zusammen mit den übrigen Gesellschaftern der gematik gemäß § 306 Abs. 1 S. 1 SGB V – die TI und nimmt diese Aufgabe durch die gematik wahr.

4.6.2.2 Spitzenverband Bund der Gesetzlichen Krankenkassen (GKV-Spitzenverband)

Der GKV-Spitzenverband ist die zentrale Interessenvertretung der Gesetzlichen Kranken- und Pflegekassen in Deutschland – alle gesetzlichen Krankenkassen sind von Gesetzes wegen Mitglieder im GKV-Spitzenverband, § 217a Abs. 1 SGB V. Die Aufgaben des GKV-Spitzenverbandes sind in § 217f SGB V allgemein geregelt. Außerdem handelt der GKV-Spitzenverband den Ausgleich und die Abrechnung der Ausstattungs- und Betriebskosten mit verschiedenen Akteuren im Gesundheitswesen aus, die diesen Akteuren mit Festlegung, Erprobung, Einführung und Betrieb der TI entstehen, § 376ff. SGB V.

4.6.2.3 Kassenärztliche Bundesvereinigung (KBV)

Die KBV ist der Dachverband der einzelnen Kassenärztlichen Vereinigungen. Sie nimmt die Interessen der Ärzte und Psychotherapeuten wahr, stellt die ambulante ärztliche Versorgung aller gesetzlich Versicherten in Deutschland sicher und setzt sich für ihre Verbesserung ein.[38]

36 Bezeichnung für die E-Rezept-App.

37 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, Produktgutachten eRezept-Frontend des Versicherten, S. 6.

38 Vgl. https://www.kbv.de/html/434.php (zuletzt abgerufen am 15.12.2022)

4.6.2.4 Deutsche Krankenhausgesellschaft (DKG)

Die DKG ist der Dachverband der deutschen Krankenhausträger. Sie vertritt die Interessen der 12 Spitzenverbände der Krankenhausenträger und der 16 Landeskrankenhausgesellschaften. Gemeinsam mit dem GKV-Spitzenverband regelt sie die Höhe und Abrechnung des sogenannten Telematikzuschlags, sprich des Ausgleichs der Ausstattungs- und Betriebskosten, die den Krankenhäusern bei Festlegung, Erprobung, Einführung und Betrieb der TI entstehen, § 377 Abs. 3 S. 1 SGB V.

4.6.2.5 Deutscher Apothekerverband (DAV)

Der DAV ist die Interessenvertretung der Apothekenleiter. Er vertritt primär die kaufmännischen Interessen des Apothekerberufs.[39]

4.6.2.6 Bundesärztekammer (BÄK)

Die BÄK ist die Spitzenorganisation der ärztlichen Selbstverwaltung. Sie dient dem ständigen Erfahrungsaustausch unter den 17 deutschen Ärztekammern und der gegenseitigen Abstimmung ihrer Ziele und Tätigkeiten, §§ 1 Abs. 1, 2 Abs. 1 der Satzung.

4.6.2.7 Bundeszahnärztekammer (BZÄK)

Die BZÄK ist die Berufsvertretung aller Zahnärzte in Deutschland. Sie setzt sich zusammen aus den 17 Zahnärztekammern der Länder und vertritt die gesundheits- und professionspolitischen Interessen des zahnärztlichen Berufsstandes, §§ 1 Nr. 1, 2 der Satzung.

4.6.2.8 Verband der Privaten Krankenversicherungen (PKV)

Der PKV ist die Interessenvertretung der Privaten Kranken- und Pflegeversicherer. Der Verband setzt sich aus 42 ordentlichen und zehn außerordentlichen[40] Mitgliedern zusammen. Der PKV ist am 3. April 2020 erneut Gesellschafter der gematik geworden.[41]

4.6.3 Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das BSI ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene, § 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Zu seinen Aufgaben gehört insbesondere die Untersuchung von Sicherheitsrisiken bei Anwendungen der Informationstechnik, die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und die Erteilung von Sicherheitszertifikaten. Außerdem prüft und bestätigt es die Konformität von informationstechnischen Systemen und Komponenten mit Technischen Richtlinien des Bundesamtes (§ 3 Abs. 1 S. 2 Nr. 3, Alt. 1, Nr. 5 und 6 BSIG).

Das BSI ist eine unabhängige Kontrollinstanz im Zusammenhang mit der Entwicklung und dem Betrieb der E-Rezept-Anwendung. An vielen Stellen überträgt das SGB V dem BSI die letztverantwortliche Überprüfung der Sicherheit des Prüfgegenstands. Insbesondere muss mit dem BSI Einvernehmen über ein Prüfverfahren für das Sicherheitsgutachten hergestellt werden, mit dem die gematik die Sicherheit, Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der von ihr entwickelten und zur Verfügung gestellten Komponenten und Dienste nachweist; anschließend prüft und bestätigt das BSI dieses Gutachten, § 360 Abs. 10 S. 5 und 6 SGB V. Die Sicherheit von Komponenten und Diensten der TI wird durch eine Sicherheitszertifizierung nach den Vorgaben des BSI oder eine andere, gleichwertige Form nachgewiesen, § 325 Abs. 3, S. 2 und 3 SGB V.

39 Sein berufspolitisches und pharmazeutisches Pendant ist die Bundesapothekerkammer. Die 17 Landesapothekerkammern und die 17 Landesapothekerverbände sind zusammengeschlossen in der Bundesvereinigung Deutscher Apothekerverbände e. V.

40 Außerordentliche Mitglieder bieten keine Krankenvollversicherungen, sondern nur Krankenzusatzversicherungen an.

41 gematik, Pressemitteilung vom 3. April 2020.

Umgekehrt ist die gematik verpflichtet, das BSI unverzüglich über Gefahren, die von Komponenten und Diensten der TI für die Funktionsfähigkeit oder Sicherheit dieser ausgehen sowie über die zur Abwehr getroffenen Maßnahmen zu informieren, § 329 Abs. 1 SGB V. Ebenso ist das BSI verpflichtet, über die nach § 329 Abs. 2 SGB V gemeldeten oder darüberhinausgehenden bedeutenden Störungen, die zu beträchtlichen Auswirkungen auf die Sicherheit oder Funktionsfähigkeit der TI führen können oder bereits geführt haben zu informieren, § 329 Abs. 4 SGB V. Außerdem hat die gematik das BSI über erkannte Sicherheitsmängel zu informieren und die Erfüllung der Anforderungen an die Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der TI nachzuweisen, § 330 Abs. 3 S. 1 SGB V. Auf Verlangen legt die gematik dem BSI Unterlagen über bestimmte Zulassungen, Bestätigungen und Aufstellungen vor, § 333 Abs. 1 SGB V. Ergibt eine Bewertung dieser Informationen Sicherheitsmängel, so kann das BSI der gematik verbindliche Anweisungen zur Beseitigung der festgestellten Sicherheitsmängel erteilen, § 333 Abs. 2 SGB V. Schließlich regelt das SGB V diverse Mitwirkungspflichten des BSI. So dürfen bestimmte Handlungen nur im Einvernehmen oder im Benehmen mit dem BSI vorgenommen werden; insbesondere bestimmt es gemeinsam mit der gematik solche Festlegungen und Maßnahmen, die Fragen der Datensicherheit berühren, erteilt befristete Genehmigungen zur Aufrechterhaltung der Sicherheit und regelt das Zulassungsverfahren für Komponenten und Dienste der TI sowie für Hersteller oder Anbieter solcher Komponenten, §§ 311 Abs. 2 S. 1, 325 Abs. 4 S. 2, Abs. 5 S. 2 SGB V. Es legt Authentisierungsverfahren für Leistungserbringer fest, für die ein solches noch nicht besteht, und reguliert die Einzelheiten der Nutzung bestimmter TI-Komponenten zu Prüfzwecken, §§ 327 Abs. 6, 331 Abs. 5 S. 2 SGB V. Im Benehmen mit der gematik bestimmt das BSI zudem die Details unterschiedlicher Bestätigungs- und Zulassungsverfahren sowie die erforderlichen Maßnahmen zur Überwachung des Betriebes der Komponenten und Dienste der TI und solcher Komponenten und Dienste, die die TI nutzen, aber außerhalb der TI betrieben werden, §§ 311 Abs. 9, 325 Abs. 4 S. 5, 327 Abs. 4 S. 2, 331 Abs. 1 SGB V.

4.6.4 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)

Der BfDI ist eine oberste Bundesbehörde, der die datenschutzrechtliche Aufsicht über alle öffentlichen Stellen des Bundes, über bestimmte Träger der sozialen Sicherung und – in gewissem Umfang – über Telekommunikations- und Postdienstunternehmen obliegt, § 8 Abs. 1 S. 1, § 9 Abs. 1 Bundesdatenschutzgesetz (BDSG). Der BfDI wird von der Bundesregierung vorgeschlagen und vom Deutschen Bundestag für fünf Jahre gewählt, § 11 Abs. 1 S. 1, Abs. 3 BDSG. Er ist bei Erfüllung seiner Aufgaben und bei der Ausübung seiner Befugnisse völlig unabhängig, § 10 BDSG. Zu seinen gesetzlichen Aufgaben gehören insbesondere die Überwachung, Untersuchung und Durchsetzung rechtlicher Bestimmungen zum Datenschutz, die Aufklärung und Sensibilisierung der Öffentlichkeit für Risiken, Garantien, Rechte und Pflichten im Zusammenhang mit der Verarbeitung personenbezogener Daten sowie die Beratung öffentlicher Einrichtungen und Gremien zu datenschutzrechtlichen Fragen, vgl. § 14 Abs. 1 S. 1 Nr. 1, 2, 3, 4 und 8 BDSG.

Im Zusammenhang mit der Entwicklung der E-Rezept-Anwendung kommt dem BfDI ebenfalls die Rolle einer unabhängigen Kontrollinstanz zu. Er überprüft die technische und organisatorische Umsetzung der E-Rezept-Anwendung in erster Linie hinsichtlich ihrer Vereinbarkeit mit datenschutzrechtlichen Bestimmungen. Zugleich wirkt der BfDI proaktiv auf den Gang des Entwicklungsverfahrens ein, beispielsweise im Rahmen von Abstimmungsprozessen mit den übrigen Akteuren oder durch gezielte Stellungnahmen. Bestimmte Handlungen dürfen nur in Abstimmung, im Einvernehmen oder im Benehmen mit dem BfDI vorgenommen werden. Insbesondere legt der BfDI in Abstimmung mit der gematik sichere Verfahren zur Übermittlung medizinischer Daten fest, bestimmt gemeinsam mit der gematik die Festlegungen und Maßnahmen zur Schaffung der TI, die Fragen des Datenschutzes berühren und die erforderlichen Voraussetzungen für die Nutzung weiterer Anwendungen im Sinne des § 306 Abs. 1 S. 2 Nr. 2 lit. a SGB V sowie die Einzelheiten der Nutzung bestimmter TI-Komponenten zu Prüfzwecken, §§ 310 Abs. 6 S. 1, 311 Abs. 2 S. 1, 327 Abs. 2, 331 Abs. 5 S. 2 SGB V. Im Einvernehmen mit dem BfDI legt der GKV-Spitzenverband bestimmte Zugriffsmodalitäten auf Daten in Anwendungen nach § 334 Abs. 1 S. 2 Nr. 1, 4, 6 und 7 fest, § 336 Abs. 7 SGB V, und erstellt geeignetes Informationsmaterial zur Unterstützung der Krankenkassen, §§ 343 Abs. 2, 358 Abs. 10 SGB V.

Der BfDI ist Mitglied im Beirat der gematik, § 317 Abs. 1 S. 3 Nr. 8 SGB V. Ihm ist im Zusammenhang mit der Schaffung der TI verschiedentlich Gelegenheit zur Stellungnahme zu geben, etwa wenn ein Beschluss der gematik Belange des Datenschutzes berührt oder wenn das BMG eine Vereinbarung im Sinne des § 369 SGB V oder eine Richtlinie im Sinne des § 383 SGB V überprüft, §§ 315 Abs. 2, 369 Abs. 2, 383, Abs. 3 S. 3 SGB V. Außerdem sind dem BfDI Protokolle über Zugriffe der gematik auf Komponenten zur Identifikation und Authentifizierung jährlich oder auf Anforderung vorzulegen, § 331 Abs. 5 SGB V.

4.6.5 Externe Auditoren, Prüfer oder Gutachter

Externe Stellen wie beispielsweise Auditoren, Prüfer oder Gutachter sind sowohl fakultativ als auch obligatorisch an der Entwicklung der E-Rezept-Anwendung zu beteiligen.

Betreibt die gematik Komponenten und Dienste selbst, so muss die Sicherheit dieser Komponenten und Dienste durch ein externes Sicherheitsgutachten nachgewiesen werden, § 323 Abs. 2 S. 5 SGB V. Die Festlegung der Prüfverfahren für das externe Sicherheitsgutachten erfolgt in diesem Fall durch das BSI, die Auswahl des Sicherheitsgutachters im Rahmen dieses Prüfverfahrens durch die gematik, § 323 Abs. 2 S. 6 und 7 SGB V. Für die Komponenten der E-Rezept-Anwendung einschließlich der E-Rezept-App ergibt sich diese Anforderung aus § 360 Abs. 10 S. 3 SGB V. Allerdings legt die gematik Prüfverfahren und Auswahl des Sicherheitsgutachters in diesem Fall im Einvernehmen mit dem BSI fest, § 360 Abs. 10 S. 5 SGB V. Von einer weiteren Spezifizierung der Anforderungen an die be-

gutachtende Stelle wurde im Laufe des Gesetzgebungsverfahrens ausdrücklich Abstand genommen.[42]

Mindestens alle zwei Jahre hat die gematik geeignete Nachweise über die Erfüllung der Anforderungen an die Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der TI zu erbringen, § 330 Abs. 2 S. 1 SGB V.

Diese Nachweise können jeweils insbesondere durch Audits, Prüfungen oder Zertifizierungen erfolgen, die von geeigneten und unabhängigen externen Stellen durchgeführt werden, § 330 Abs. 2 S. 2 SGBV. Aus der Begründung des Patientendaten-Schutz-Gesetzes ergibt sich, dass diese Stellen entweder vom BSI bestätigt oder zertifiziert oder von der Deutschen Akkreditierungsstelle GmbH akkreditiert werden müssen.[43]

4.6.6 Anbieter von Diensten der Anwendungsinfrastruktur

Die TI umfasst neben der zentralen Infrastruktur eine dezentrale Infrastruktur sowie eine Anwendungsinfrastruktur.[44] Diese Anwendungsinfrastruktur besteht aus Fachdiensten und Fachanwendungen, die durch den jeweiligen Anbieter betrieben werden, § 307 Abs. 4 S. 1 SGB V.

Die für die E-Rezept-Anwendung relevanten Anbieter sind

- der Anbieter des E-Rezept-Fachdienstes,
- der Anbieter des Identitätsdienstes und
- der Anbieter des Apothekenverzeichnisses.

4.6.7 Technische Dienstleister

Die gematik bedient sich zur Durchführung der optionalen App-Nutzungsanalyse eines Analytics-Dienstleisters mit Sitz in Deutschland. Der Dienstleister stellt ein Software Development Kit (SDK) für die App sowie eine Web-Anwendung im Software-as-a-Service-Modell für die Auswertung der Analysedaten zur Verfügung. Die entsprechenden Datenverarbeitungen werden unter Ziffer 5.10 aufgeführt.

Die für das E-Rezept relevanten Anbieter von Diensten der Anwendungsinfrastruktur (vgl. 4.6.6) setzen teilweise ebenfalls technische Dienstleister ein. Dabei müssen sie die für den jeweiligen Dienst geltenden Vorgaben in den Spezifikationsdokumenten der gematik beachten.

4.6.8 Krankenkassen

Die Krankenkassen stellen den bei ihnen Versicherten eine NFC-fähige elektronische Gesundheitskarte und die zugehörige PIN sowie eine ePA-App zur Verfügung, die jeweils für die Authentifizierung gegenüber dem Identitätsdienst der E-Rezept-Anwendung genutzt werden können. Sie rechnen die eingelösten E-Rezepte mit den Apotheken ab und finanzieren die Ausstattungs- und Betriebskosten, die im Zusammenhang mit der Festlegung, Erprobung und Einführung sowie dem Betrieb der TI entstehen, §§ 376 ff. SGB V. Beschlüsse, die die gematik zu den Regelungen, dem Aufbau und dem Betrieb der TI trifft, sind für die Krankenkassen und ihre Verbände verbindlich, § 315 Abs. 1 S. 1 SGB V.

42 In der Entwurfsfassung verlangte der damalige § 360 Abs. 5 S. 7 SGB V noch, dass die begutachtende Stelle "für Zertifizierungen zusätzlich nach § 39 des [BDSG] akkreditiert und zugelassen sein" müsse. Dies wurde jedoch im finalen Entwurf mit der Begründung gestrichen, eine solche Stelle sei bislang nicht eingerichtet; daher bedeute das Festhalten an diesem Erfordernis "ein nicht absehbares Risiko für Verzögerungen". Zudem werde die Einhaltung der erforderlichen sicherheitstechnischen Anforderungen "bereits durch den Nachweis mittels eines externen Sicherheitsgutachtens und die gemeinsame Abstimmung mit dem [BSI] über die Prüfverfahren und die Auswahl des Sicherheitsgutachters gewährleistet" (BT-Drs. 19/20708, S. 175).

43 BT-Drs. 19/18793, S. 107.

44 Siehe oben 4.5.1.

4.6.9 Leistungserbringer

Leistungserbringer erbringen Leistungen des Gesundheitswesens für Versicherte. Nach § 339 SGB V dürfen sie auf Versichertendaten in Anwendungen der TI zugreifen. Nach § 360 SGB V sind die Leistungserbringer zur Nutzung der E-Rezept-Anwendung verpflichtet. Die Zugriffsrechte der Leistungserbringer auf E-Rezepte im E-Rezept-Fachdienst ergeben sich aus § 361 SGB V.

4.6.9.1 Apotheken

Versicherte und in bestimmten Fällen auch Ärzte können Apotheken über die E-Rezept-Anwendung E-Rezepte übermitteln, dort die Vorrätigkeit eines Medikaments abfragen, Medikamente bestellen oder einsehen, ob ein bestelltes Medikament abgeholt werden kann. Über den E-Rezept-Token erhalten Apotheker Zugriff auf die elektronisch signierte Verordnung eines Arztes.

4.6.9.2 Ärzte/Zahnärzte

Ärzte/Zahnärzte stellen E-Rezepte auf dem E-Rezept-Fachdienst aus. Dazu nutzen sie ihr an den E-Rezept-Fachdienst angebundenes PVS. Die E-Rezepte müssen mit einer qualifizierten elektronischen Signatur (QES) unterzeichnet werden, damit sie dem Versicherten bereitgestellt werden. Ärzte/Zahnärzte sind verpflichtet, den Versicherten auf Wunsch den ausgedruckten Rezeptcode zur Verfügung zu stellen.

4.6.10 Deutscher Bundestag

Der Deutsche Bundestag ist die Gesamtheit der nach Art. 38 Abs. 1 S. 1 GG gewählten Abgeordneten. Im Jahr 2019 hat er der gematik aufgetragen, die Voraussetzungen zu schaffen, ärztliche Verordnungen für apothekenpflichtige Arzneimittel in elektronischer Form übermitteln zu können, Nr. 16 Art. 12 des Gesetzes für mehr Sicherheit in der Arzneimittelversorgung. Mit dem PDSG wurden Aufgaben, Aufträge und Pflichten der gematik dann neu gefasst und im SGB V verankert. Im DVPMG wurden weitere Leistungserbringergruppen sukzessive zum Anschluss an die TI verpflichtet und der gesetzlich vorgegebene Leistungsumfang erweitert.

4.6.11 Organe und Organisationen der Europäischen Union (EU)

Verschiedene Organe und Organisationen der Europäischen Union befassen sich auf unterschiedlichen Ebenen und auf unterschiedliche Art und Weise mit der Digitalisierung des Gesundheitswesens. Art. 168 AEUV stellt zwar einerseits klar, dass Gesundheitspolitik grundsätzlich Sache der einzelnen Mitgliedsstaaten ist und die EU diese Gesundheitspolitik allenfalls ergänzen soll. Der Artikel weist jedoch andererseits auch darauf hin, dass die Mitgliedstaaten ihre Gesundheitspolitiken untereinander im Benehmen mit der EU-Kommission koordinieren (sollen). Um diese Koordination zu fördern, wurde Anfang 2011 die Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung verabschiedet. Mit dieser Richtlinie wurde ein eigenes Netzwerk für elektronische Gesundheitsdienste (eHealth-Netzwerk) ins Leben gerufen, das auf freiwilliger Basis die Schaffung nachhaltiger, wirtschaftlicher und sozialer Gesundheitssysteme und -dienste voranbringen, entsprechende Leitlinien erarbeiten und die Mitgliedsstaaten bei ihrer Umsetzung unterstützen soll. Flankiert wurde dieses Netzwerk von mehreren sogenannten gemeinsamen Aktionen (engl. Joint Actions). Im Jahr 2012 wurde außerdem eine eHealth-Interessengruppe (eHealth stakeholder group, eHSG) gegründet, die sich aus verschiedenen Dachverbänden und Interessengruppen zusammensetzt und die EU-Kommission zur Digitalisierung des Gesundheitswesens berät. Ebenfalls im Jahr 2012 veröffentlichte die Europäische Kommission einen Aktionsplan für die Jahre 2012-2020 (European Union eHealth Action Plan), der insbesondere das Ziel ausgab, eine breitere Interoperabilität elektronischer

Gesundheitsdienste herzustellen. Dieser Aktionsplan wurde inzwischen um eine Mitteilung der Kommission über die Ermöglichung der digitalen Transformation von Gesundheit und Pflege im digitalen Binnenmarkt die aufgeklärte Mitwirkung der Bürger und den Aufbau einer gesünderen Gesellschaft (COM/2018/233 final) sowie eine Absichtsbekundung zur Schaffung eines europäischen Gesundheitsdatenraumes (European Health Data Space, EHDS) und der entsprechenden Infrastruktur (MyHealth@EU; 2020) ergänzt. In den beiden Folgejahren 2021 und 2022 wurde je eine gemeinsame Aktion zur näheren Ausgestaltung eines einheitlichen europäischen Standards für den Austausch von Gesundheitsdaten (European Electronic Health Record exchange Formats, EHRxF; X-eHealth) und des europäischen Gesundheitsdatenraums (Towards the European Health Data Space, TEHDAS) eingeleitet. Die Absichtsbekundung vom Sommer 2020 wurde Mitte 2022 zu einem Vorschlag für eine Verordnung über den Europäischen Gesundheitsdatenraum konkretisiert. Dort wird die Erwartung formuliert, dass das E-Rezept und die elektronische Patientenkurzakte in den meisten Mitgliedsstaaten bis 2025 eingeführt werden sollen.

4.6.12[45] Anbieter, Betreiber und Hersteller von Smartphones, mobilen Betriebssystemen, Betriebssystemdiensten und Online-Diensten

Apple, Google und Huawei treten im Zusammenhang mit der E-Rezept-Anwendung in unterschiedlichen Rollen auf: als Hersteller von Smartphones und mobilen Betriebssystemen, von Betriebssystemdiensten oder als Anbieter von Online-Diensten (z. B. App-Stores).

4.6.13 Entwicklercommunity

Die gematik hat den Quellcode der E-Rezept-App unter der European Union Public Licence (EUPL) sowie Referenzimplementierungen des E-Rezept-Fachdienstes und des Identitätsdienstes veröffentlicht. Mit dieser Maßnahme soll das Vertrauen in das E-Rezept gestärkt und Fachleuten die Möglichkeit zur Identifikation von potentiellen Sicherheitsmängeln gegeben werden. Durch die Veröffentlichung des Quellcodes soll die Entwicklercommunity kontinuierlich in die weitere Verbesserung der Softwarekomponenten integriert werden.

4.6.14 Betroffene Personen

Die von der E-Rezept-Anwendung betroffenen Personen im Sinne des Art. 4 Nr. 1 DSGVO sind in erster Linie die Versicherten und Nutzer der E-Rezept-App.

Eine weitere Gruppe betroffener Personen stellen die an die E-Rezept-Anwendung angebundenen Leistungserbringer dar.[46]

45 Wenn im Folgenden im Zusammenhang mit den aus Endgeräten, Betriebssystemen, Apps und Online-Diensten bestehenden mobilen Ökosystemen von „Anbietern“, „Betreibern“ oder „Herstellern“ die Rede ist, ist damit in der Regel der gleiche Akteur in seiner im jeweiligen Kontext maßgeblichen Funktion gemeint. Im Falle von Apple fungiert der Betreiber des App-Stores nicht nur als Hersteller des Betriebssystems, sondern auch als Hersteller des Smartphones.

46 Die Datenschutzrisiken für Leistungserbringer im Zusammenhang mit der Nutzung der E-Rezept-Anwendung sind nicht Gegenstand dieser DSFA.

5 Beschreibung der E-Rezept-App (Prüfgegenstand)

Die nachfolgend beschriebenen Verarbeitungstätigkeiten und Verarbeitungszwecke bilden den Prüfgegenstand. Die Beschreibung der einzelnen Verarbeitungstätigkeiten folgt grundsätzlich dem für die Vorbereitungsphase der DSFA gewählten Drei-Ebenen-Modell (Geschäfts-/Sachebene, Anwendungsebene, Infrastrukturebene), wobei in der nachfolgenden Darstellung aus Gründen der Übersichtlichkeit die Anwendungs- und Infrastrukturebene zusammen abgehandelt werden.

Bei der Beschreibung des Prüfgegenstands hat sich das DSFA-Team grundsätzlich an den von der gematik spezifizierten Anwendungsfällen orientiert. Für die gesetzlich geforderte Analyse der mit der Verarbeitung einhergehenden Risiken für die Rechte und Freiheiten der betroffenen Personen wurden die Anwendungsfälle der gematik um datenschutzrelevante Details der konkret geplanten Umsetzung ergänzt und als Verarbeitungstätigkeiten interpretiert. Hierbei entstehen Verarbeitungstätigkeiten durch Bündelung mehrerer Verarbeitungsvorgänge zu jeweils einem Verarbeitungszweck. Eine Verarbeitungstätigkeit umfasst in der Regel die zu einer bestimmten Funktionalität oder Anwendungsphase zugehörigen Verarbeitungsvorgänge.

5.1 Zweck der Verarbeitung

Vor dem Hintergrund der gesetzlichen Aufträge der gematik (siehe 4.4) besteht der Zweck der prüfgegenständlichen Verarbeitungsvorgänge darin, den Versicherten nach §§ 312 Abs. 1 Nr. 16, 360 Abs. 10 S. 1 SGB V eine Komponente für den elektronischen Zugriff auf die E-Rezept-Anwendung nach Maßgabe der gesetzlichen Vorgaben zur Verfügung zu stellen.

Aus den gesetzlichen Vorgaben und teilweise ergänzend den Gesetzgebungsmaterialien lässt sich entnehmen, dass die den Versicherten von der gematik zur Verfügung zu stellende Zugriffskomponente insbesondere über folgende Eigenschaften bzw. Funktionalitäten verfügen muss oder kann:

- Die Zugriffskomponente muss den Versicherten die sichere elektronische Einlösung ihrer E-Rezepte in einer Apotheke ermöglichen (§ 360 Abs. 10 SGB V).
- Die Zugriffskomponente muss den Versicherten die Eingabe der für den Zugriff auf ihre E-Rezepte erforderlichen Zugangsdaten ermöglichen, auch wenn die Zugangsdaten in Papierform bereitgestellt werden (§ 360 Abs. 9 S. 1 SGB V).[47]
- Die Interoperabilität der Zugriffskomponente muss gewährleistet sein (§ 360 Abs. 10 S. 3 SGB V).
- Die Zugriffskomponente muss den Versicherten einen barrierefreien Zugriff auf ihre Daten ermöglichen (§§ 311 Abs. 4 S. 1, 336 Abs. 1 S. 1 SGB V).
- Die Zugriffskomponente darf den Zugriff der Versicherten erst nach ihrer Authentifizierung mit einem geeigneten technischen Verfahren, das zur Authentifizierung einen hohen Sicherheitsstandard gewährleistet, ermöglichen (§ 336 Abs. 4 SGB V).
- Die Zugriffskomponente muss den Zugriff der Versicherten mittels der eGK oder ihrer digitalen Identität ermöglichen (§ 336 Abs. 1 SGB V).
- Die Zugriffskomponente muss auf die Informationen des Nationalen Gesundheitsportals nach § 395 SGB V zugreifen können und den Versicherten diese Informationen mit Daten, die in ihrem E-Rezept gespeichert sind, verknüpft anbieten können (§ 360 Abs. 12 Nr. 1 SGB V).
- Die Zugriffskomponente muss so gestaltet sein, dass sie die Interessen der Patienten sowie den Datenschutz wahrt (§ 311 Abs. 4 SGB V).
- Die Zugriffskomponente kann den Versicherten das Auslesen ihrer Protokolldaten gemäß § 309 Abs. 1 SGB V und der Fachdaten ermöglichen, sofern ein technisches Verfahren vorzusehen wird, das zur Authentifizierung einen hohen Sicherheitsstandard gewährleistet (§ 312 Abs. 6 DSGVO).
- Die Sicherheit, Verfügbarkeit und Nutzbarkeit der von den Nutzern auf ihren eigenen Endgeräten betriebenen Zugriffskomponente muss von der gematik überwacht und gewährleistet werden können (§ 331 Abs. 1 SGB V).
- Die Zugriffskomponente muss bis zum 1. Januar 2024 eine Funktion zur Übermittlung von E-Rezepten an die nationale eHealth-Kontaktstelle bereitstellen, damit Versicherte nach vorheriger Einwilligung in die Nutzung dieses Übermittlungsverfahrens ihre E-Rezepte bei Leistungserbringern in anderen EU-Mitgliedstaaten einlösen können (§ 360 Abs. 12 Nr. 2 SGB V).

5.2 Eingrenzung des Prüfgegenstands

Der Prüfgegenstand umfasst die nachstehenden Anwendungsaspekte bzw. Verarbeitungstätigkeiten im Zusammenhang mit der App, soweit diese den gesetzlichen Aufgaben-, Auftrags- und Pflichtenkreis der gematik betreffen und insoweit von ihr gestaltend beeinflusst werden können:

- Installation und Deinstallation der App,
- Start und Einrichtung der App,
- Anmeldung am E-Rezept-Fachdienst,
- E-Rezepte einlösen,

47 Vgl. Gesetzesbegründung in BT-Drs. 19/18793, S. 128. Dass für den Zugriff auf E-Rezepte im E-Rezept-Fachdienst „Zugangsdaten" benötigt werden, wird von den gesetzlichen Regelungen nicht ausdrücklich festgelegt, sondern von § 360 Abs. 9 SGB V vorausgesetzt.

- Apothekensuche und -bestimmung,
- Mitteilungsfunktion,
- E-Rezepte verwalten und teilen,
- Nutzungsanalyse.

Zur Klarstellung werden nachfolgend einzelne Verarbeitungsvorgänge und Sachverhalte genannt, die nicht vom Prüfgegenstand umfasst sind:

- Verarbeitungsvorgänge im Verantwortungsbereich der Leistungserbringer, insbesondere die Übermittlung und der Abruf von E-Rezepten durch Leistungserbringer,
- Verarbeitungsvorgänge bei der Nutzung der Desktop-Anwendung des E-Rezepts durch Versicherte,
- Verarbeitungsvorgänge im Verantwortungsbereich des Betreibers des Nationalen Gesundheitsportals,
- Verarbeitungsvorgänge durch Betreiber von App-Stores,[48]
- Verarbeitungsvorgänge auf Seiten der mobilen Betriebssysteme, die zwingend mit der technischen Ausführung einer App einhergehen.

Zur besseren Nachvollziehbarkeit werden die Umstände beschrieben, die für die Bewertung der spezifischen datenschutzrechtlich maßgeblichen Merkmale des Prüfgegenstands relevant sein können. Dies erfordert teilweise auch, dass Verarbeitungsvorgänge beschrieben werden, die zwar im Zusammenhang mit der Nutzung der E-Rezept-App stehen, jedoch außerhalb der datenschutzrechtlichen Verantwortlichkeit der gematik liegen (z. B. die Nutzung von Diensten der Hersteller der mobilen Betriebssysteme). Diese Verarbeitungsvorgänge sind nicht vom Prüfgegenstand umfasst. Soweit erforderlich werden sie jedoch im Rahmen der Risikoanalyse berücksichtigt, worauf ggf. hingewiesen und erläutert wird, welche Auswirkungen diese Aspekte auf das Ergebnis der Risikoanalyse haben.

5.3 Verarbeitungstätigkeit 1: Installation und Deinstallation der App

Vor der Nutzung der App hat der Nutzer einige vorbereitende Handlungen durchzuführen. Hierbei werden Daten des Nutzers teilweise durch den Betreiber der gewählten Vertriebsplattform (App-Store) und den Hersteller des mobilen Betriebssystems seines Endgeräts verarbeitet.

Zunächst muss die App auf das Smartphone des Nutzers heruntergeladen und installiert werden. Hierzu muss der Nutzer regelmäßig ein bestehendes Benutzerkonto für den von ihm genutzten App-Store verwenden. Zurzeit vertreibt die gematik die App über den Apple App Store, den Google Play Store und die Huawei App Gallery. Im Rahmen des Downloads und der Installation der App werden vom Betreiber des jeweiligen App-Stores Login-, Nutzungs- und Zugriffsdaten des Nutzers bzw. Inhabers des genutzten Benutzerkontos erfasst und für verschiedene Zwecke verarbeitet.

Der Nutzer hat mit dem jeweiligen App-Store-Betreiber, der zugleich auch der Hersteller des genutzten Betriebssystems oder mit diesem konzernverbunden ist, verschiedene Nutzungs- und Lizenzvereinbarungen über das jeweilige Betriebssystem, die Betriebssystemdienste und die Benutzerkonten, die für die Nutzung von zentralen Betriebssystemfunktionen und des App-Stores notwendig sind (z. B. Google-Konto), abzuschließen, um die für den Betrieb der Software oder die Nutzung der Dienste erforderlichen Rechte zu erhalten. Der Nutzer wird dabei vom jeweiligen Anbieter oder Hersteller über das vertragliche Leistungs- und Pflichtenprogramm und seine Datenverarbeitungspraktiken informiert und erteilt ggf. die vom Anbieter für notwendig erachteten Einwilligungen für bestimmte Verarbeitungen. Entsprechendes gilt für den Erwerb von Nutzungsrechten an Drittanbieter-Apps in den App-Stores.

Die Hersteller der Betriebssysteme legen in ihren Lizenzbedingungen diverse Befugnisse fest, die auch die Nutzung der Betriebssystemdienste durch Drittanbieter-Apps betreffen können. Dazu gehört regelmäßig die Verarbeitung bestimmter personenbezogener Daten, insbesondere der Geräte- und Nutzungsdaten sowie die Konto-ID des Benutzerkontos. Da-

48 Soweit zu Verarbeitungstätigkeit 1 (Installation und Deinstallation der App) in allgemeiner Form auf Verarbeitungsvorgänge der App-Store-Betreiber eingegangen wird, dient dies der Beschreibung des bei der datenschutzrechtlichen Bewertung zu berücksichtigenden Nutzungsverhältnisses zwischen dem Nutzer und dem jeweiligen Betreiber.

bei behalten sich die Hersteller die Verarbeitung von Nutzungsdaten, die bei der Nutzung von Betriebssystemdiensten durch Apps anfallen (auch sogenannte „Telemetriedaten“) in aller Regel vor und lassen sich gewisse Befugnisse einräumen, um Betriebssystemfunktionen und -dienste im Rahmen von Softwareaktualisierungen verändern oder entfernen zu dürfen, die Nutzung von Betriebssystemfunktionen und -diensten von der Durchführung von Updates oder der Verwendung bestimmter Gerätemodelle abhängig zu machen oder um das Gerät des Nutzers auf potentielle Sicherheitsrisiken hin zu überprüfen. Schließlich behalten sich die Hersteller üblicherweise vor, eine vom Nutzer installierte Drittanbieter-App in bestimmten Fällen (z. B. aus Sicherheitsgründen) zu löschen.

Für technisch versiertere Nutzer, die ein alternatives Betriebssystem ohne Bindung an Google oder Huawei verwenden, besteht die Möglichkeit, die App über das GitHub-Repository der gematik im apk-Format zu beziehen. Auch Nutzer mit einem „gebundenen“ Android- oder EMUI-Betriebssystem, die den entsprechenden App-Store nicht nutzen möchten, können die App auf diese Weise installieren, sofern sie in den Betriebssystemeinstellungen die Installation aus „unbekannten Quellen“ freigegeben haben.

Die App speichert alle lokal von ihr verarbeiteten Daten ausschließlich im von ihr verwalteten Speicherbereich. Wenn der Nutzer die App auf die vom Hersteller des Betriebssystems vorgesehene Weise löscht, werden somit auch alle von der App lokal gespeicherten Daten gelöscht.

5.4 Verarbeitungstätigkeit 2: Start und Einrichtung der App

5.4.1 Nutzerperspektive

Beim initialen und bei jedem weiterem Startvorgang der App erfolgt eine Prüfung auf Anzeichen einer Modifikation des Smartphones bzw. des Betriebssystems. Diese Prüfung dient dem Zweck, unwissende Nutzer vor dem Einsatz der App in kompromittierten Umgebungen zu warnen. Warnkriterium ist dabei, ob Nutzungsbeschränkungen, die vom Hersteller des Betriebssystems oder Smartphones serienmäßig eingerichtet sind, auf vom Hersteller nicht-autorisiertem Weg entfernt wurden (sogenanntes Rooting oder Jailbreaking). Wenn eine Modifikation des Betriebssystems erkannt wird, wird dem Nutzer in der App eine Warnung angezeigt. Möchte der Nutzer die App unter Inkaufnahme der Risiken infolge der Modifikation des Betriebssystems dennoch verwenden, muss er in der App bestätigen, dass er die Warnung zur Kenntnis genommen hat. Die Warnung erscheint bei jedem Start der App erneut, solange die Modifikation fortbesteht. Die Nutzung der App wird durch die erkannte Modifikation von Seiten der App nicht gezielt beschränkt, so dass Funktionsbeeinträchtigungen infolge des Rootings bzw. Jailbreakings nicht ausgeschlossen werden können.

Zur Absicherung des Zugriffs auf die App wird im Anschluss an die Root-Erkennung die Authentifizierung des Nutzers gegenüber der App (im Folgenden auch als „lokale Authentifizierung“ bezeichnet) abgefragt. Dem Nutzer werden im Rahmen des Onboardings die auf seinem Smartphone verfügbaren lokalen Authentifizierungsverfahren angezeigt und erläutert, wobei das sicherste verfügbare Verfahren standardmäßig vorausgewählt ist. Der Nutzer kann diesen Schritt auch überspringen, da die Nutzung der lokalen Authentifizierungsfunktion in dieser Anwendungsphase optional ist.

Zur lokalen Authentifizierung werden dem Nutzer ggf. die bereits von ihm eingerichteten betriebssystemseitigen biometrischen Authentifizierungsverfahren (z. B. Face ID oder „Entsperren per Fingerabdruck“) sowie die von der App verwaltete Absicherung mittels eines Kennworts angeboten. Wählt der Nutzer zur Absicherung das Kennwortverfahren, so werden ihm zwei Eingabefelder angezeigt (Kennwort und Kennwortwiederholung), in die er ein Kennwort seiner Wahl eingeben kann. Ggf. auf dem Endgerät eingerichtete Kennwortmanager werden unterstützt. Ein Indikatorbalken zeigt den Grad der Sicherheit des eingegebenen Kennworts an.

Falls ein aus technischer Sicht vorhandener, vom Nutzer aber noch nicht eingerichteter oder aktivierter biometrischer Authentifizierungsdienst genutzt werden könnte (z. B. weil noch keine Fingerabdrücke hinterlegt wurden), wird der Nutzer von der App darüber informiert, dass die Einrichtung nicht vollständig ist und das Verfahren daher aktuell nicht genutzt werden kann. Der Nutzer kann den lokalen biometrischen Authentifizierungsdienst in den Betriebssystemeinstellungen dann zunächst einrichten und später die Einrichtung der App fortsetzen oder in der App sofort das Kennwortverfahren auswählen. Nach der Einrichtung der lokalen Authentifizierung ist die App bei jedem künftigen Start gesperrt und fordert den Nutzer auf, sich mit dem zuvor gewählten lokalen Authentifizierungsverfahren zu authentifizieren. Ist die Authentifizierung nicht erfolgreich, wird der fehlgeschlagene Versuch in der App angezeigt und gezählt. Der Nutzer kann die Authentifizierung erneut und beliebig oft starten. Bei erfolgreicher Authentifizierung wird der Nutzer auf den Hauptbildschirm der App geleitet und die von der App gespeicherten Daten werden angezeigt. Ggf. sieht der Nutzer einen gHinweis, dass es erfolglose Anmeldeversuche gab.

Im Rahmen des Onboardings wird der Nutzer auf die verlinkten Nutzungsbedingungen und Datenschutzhinweise der gematik für die E-Rezept-App hingewiesen.

Im Zuge des Onboardings wird in der App ein Profil angelegt. Dieses dient der vereinfachten lokalen Verwaltung der E-Rezepte. Der Nutzer kann mehrere Profile anlegen, was ihm die Möglichkeit gibt, als Vertreter (bspw. für Familienangehörige) die E-Rezepte von anderen Personen in seiner App zu verwalten. Er kann an jeder Stelle der App zwischen Profilen umschalten, und ggf. als Vertreter agieren. Für die Einrichtung eines Profils ist lediglich erforderlich, dass der Nutzer einen sogenannten „Profilnamen“ seiner Wahl eingibt. Es ist nicht notwendig, dass dieser Profilname mit dem Namen auf der eGK des Nutzers übereinstimmt. Wenn der Nutzer sich mit einem Authentifizierungsmittel am Fachdienst anmeldet (siehe Ziffer 5.5), und das Authentifizierungsmittel diese Funktion erlaubt, wird der Profilname durch die App aktualisiert auf den Namen des Versicherten. Der Name des Profils kann im Nachgang in der App jederzeit beliebig oft geändert werden. Anders als die Authentifizierungsdaten für die Anmeldung am E-Rezept-Fachdienst genügt für den Zugriff auf die eingerichteten Profile die Eingabe des lokalen Authentifizierungsmittels, sofern dieses eingerichtet worden ist. Das Eingabefeld für den Profilnamen ist so konfiguriert, dass es der entsprechenden Funktion des Betriebssystems erlaubt, ein automatisches Ausfüllen der Profilnamen zu unterstützen (sofern der Nutzer diese Funktion des Betriebssystems aktiviert hat).

5.4.2 Anwendungs-/Infrastrukturebene

Die App-seitigen Verarbeitungsvorgänge laufen in dieser Anwendungsphase lokal ab. Die Konfigurationseinstellungen und Profildaten des Nutzers werden daher nur auf dem Smartphone gespeichert und nicht an einen Server übermittelt.

Für die Jailbreak-Erkennung unter iOS stellt Apple den Entwicklern von Apps keine spezielle Sicherheitsfunktionen oder Betriebssystemdienste zur Verfügung. Daher ist die App so programmiert, dass sie nach jedem Start auf dem iPhone des Nutzers nach Dateien von Apps sucht, die typischerweise nur auf gejailbreakten iPhones installiert sind (z. B. Cydia, FakeCarrier, Icy und SBSettings). Dabei werden die Inhalte der gefundenen Dateien von der App nicht untersucht.

Für die Root-Erkennung unter Android wird der Betriebssystemdienst SafetyNet Attestation von Google genutzt, der Bestandteil der vom Nutzer bereits verwendeten Google Play Services ist. Dabei greift die App auf die lokal bereitgestellte SafetyNet Attestation API zu und übergibt ihr eine Zufallszahl (Nonce), die den angestoßenen Attestationsvorgang identifiziert. Der SafetyNet-Attestation-Dienst wertet sodann die Ausführungsumgebung auf dem Smartphone aus und übermittelt das Ergebnis an den Server-Endpunkt des SafetyNet-Attestation-Servers. Der SafetyNet-Attestation-Server sendet daraufhin eine signierte Attestation mit dem Bewertungsergebnis an das Betriebssystem zurück, das dieses dann an die App weitergibt. Das Bewertungsergebnis enthält lediglich eine allgemeine Angabe zur Geräteintegrität („True“ oder „False“). Die App verarbeitet die erhaltene Attestation lediglich für die Entscheidung über die Anzeige des Sicherheitshinweise beim Start der App. Diese Verarbeitung erfolgt lokal anhand von hartkodierten Kriterien; der auf dem SafetyNet-Attestation-Server bereitgestellte Verifikationsdienst zur Prüfung der Echtheit der an die App weitergegebene Attestation wird von der App nicht verwendet.

Für die Root-Erkennung unter Huawei EMUI wird der Betriebssystemdienst Safety Detect SysIntegrity von Huawei genutzt, der mit dem Betriebssystem ausgeliefert wird. Die Funktionsweise entspricht derjenigen der Google SafetyNet Attestation. Ein Verifikations-

dienst zur Echtheitsprüfung der Attestation wird nicht genutzt und von Huawei derzeit auch nicht angeboten.

Das vom Nutzer zur Kennwort-basierten Authentifizierung eigegebene App-Kennwort wird mit der in der App enthaltenen quelloffenen Bibliothek ZXCVBN[49] lokal auf seine Komplexität hin geprüft. Typische und weit verbreitete Kennwortmuster (z. B. Datumsangaben) und potentiell unsichere Kennworte (z. B. „password“ oder „1234“) werden dabei erkannt und infolgedessen von der App nicht als Kennwort akzeptiert. Das Kennwort wird von der App verschlüsselt gespeichert.

Wählt der Nutzer zur lokalen Authentifizierung ein biometrisches Verfahren, so werden die zugehörigen Betriebssystemdienste aufgefordert, die gewählte biometrische Authentifizierung durchzuführen und dieses Authentifizierungsmittel wird anstatt des Kennworts für den Zugriffsschutz lokal hinterlegt. Die biometrische Authentifizierung erfolgt durch Fingerabdrücke oder Gesichtserkennung. Die App erhält vom Betriebssystem dabei nur das Ergebnis der biometrischen Authentifizierung im Sinne der Angabe, dass die Authentifizierung erfolgreich war bzw. fehlgeschlagen ist.

5.5 Verarbeitungstätigkeit 3: Anmeldung am E-Rezept-Fachdienst

5.5.1 Nutzerperspektive

Um über die App auf die Fachdaten im E-Rezept-Fachdienst zugreifen zu können, muss sich der Nutzer bei diesem anmelden. Die Anmeldung am E-Rezept-Fachdienst setzt das Vorhandensein von gültigen Zugangsschlüsseln (auch Token genannt, siehe 5.11.2) voraus, die erst nach der Authentifizierung des Nutzers gegenüber dem Identitätsdienst an die App ausgegeben und von dieser bei der Anmeldung gegenüber dem E-Rezept-Fachdienst vorgezeigt werden müssen.

Der Authentifizierungsprozess kann vom Nutzer über einen Button im Profilbereich initiiert werden. Der Authentifizierungsprozess wird auch initiiert, wenn der Nutzer eine Funktion aufruft, für die die Anmeldung am E-Rezept-Fachdienst zwingend erforderlich ist, beispielsweise wenn er auf dem Hauptbildschirm die Rezeptanzeige aktualisiert oder er ein nur lokal gespeichertes E-Rezept elektronisch einer Apotheke zuweisen will.

Nach der Initiierung des Authentifizierungsprozesses muss der Nutzer zunächst eine Authentifizierungsmethode für die Anmeldung am E-Rezept-Fachdienst auszuwählen. Dabei kann der Nutzer zwischen der Authentifizierung mit einer NFC-fähigen eGK und der Authentifizierung mit der ePA-App seiner Krankenkasse wählen.

Wählt der Nutzer die Authentifizierung mit einer NFC-fähigen eGK, verfügt aber noch nicht über eine solche, wird er aufgefordert, bei seiner Krankenkasse eine neue eGK zu bestellen. Hierfür kann der Nutzer in einer Liste seine Krankenkasse auswählen. Abhängig von der Krankenkasse werden dem Nutzer sodann die Kontaktdaten seiner Krankenkasse angezeigt, darunter Telefonnummern, Webseiten und E-Mail-Adressen. Die Kontaktaufnahme des Nutzers zur Krankenkasse unter Verwendung dieser Daten erfolgt außerhalb der App.

Verfügt der Nutzer bereits über eine geeignete eGK, gibt er in der App die Card Access Number (CAN) und PIN ein. Anschließend wird der NFC-Betriebssystemdienst gestartet und der Nutzer liest über das In-App-Frontend des NFC-Betriebssystemdienstes seine eGK aus. War die Authentifizierung gegenüber dem Identitätsdienst erfolgreich, bietet die App die Option „Zugangsdaten speichern“ an, sofern das Betriebssystem des Endgeräts des Nutzers über eine Vorrichtung verfügt, mit dem Daten auf dem Endgerät in einem speziellen Bereich sicher gespeichert werden können (Secure Module). Nachdem sich der Nutzer erfolgreich authentifiziert hat, wird die App automatisch am E-Rezept-Fachdienst angemeldet. Wird diese Funktion gewählt, erzeugt die App eine Geräteidentität, die durch den zentralen IDP verwaltet wird. Dabei werden Gerätespezifische Informationen an den IDP übertragen (Gerätetyp, Betriebssystemversion). Der IDP kann

49 Testen kann man dies unter https://lowe.github.io/tryzxcvbn/ (zuletzt aufgerufen am 15.12.2022).

Geräteidentitäten invalidieren. Wenn der Nutzer die Option „Zugangsdaten speichern“ nicht nutzt, muss er sich nach Ablauf seiner Zugangstoken erneut am E-Rezept-Fachdienst anmelden.

Wenn sich der Nutzer für die Anmeldung mit der ePA-App entscheidet, muss er zunächst seine Krankenkasse aus einer Liste auswählen. Nachdem der Nutzer seine Auswahl getroffen hat, öffnet sich die ePA-App der jeweiligen Krankenkasse. Ist diese noch nicht installiert, wird eine Webseite des Identitätsdienstes im Standard-Webbrowser geöffnet, auf welcher Links zum Download der jeweiligen ePA-App in den verschiedenen App-Stores bereitgestellt werden. Wird eine bereits installierte ePA-App aufgerufen, so wird die E-Rezept-App durch das Betriebssystem in den Hintergrund verschoben und in den Status „Anzeige des Hauptbildschirms“ versetzt. Ist die Validierung erfolgreich, ruft die ePA-App wieder die E-Rezept-App auf, die sich dann automatisch am E-Rezept-Fachdienst anmeldet.

5.5.2 Anwendungs-/Infrastrukturebene

5.5.2.1 Authentifizierungsarchitektur

Die Authentifizierungsspezifikationen für das Anmeldeverfahren basieren auf dem OpenID-Connect-Authentifizierungsprotokoll und dem OAuth-2.0-Autorisierungsprotokoll mit dem Grant Type „Authorization Code“ und der Erweiterung PCKE. Wenn die Authentifizierung erfolgreich ist, erhält die E-Rezept-App vom Identitätsdienst drei Zugangsschlüssel (Access-Token, ID-Token und SSO-Token).

Die OAuth-2.0-Rollen (OpenID-Connect-Rollen) der am Authentifizierungsprozess beteiligten Akteure und Dienste sind wie folgt festgelegt:

- Nutzer: Resource Owner (End User)
- E-Rezept-Fachdienst: Resource Server
- Identitätsdienst: Authorization Server (OpenID Provider)
- E-Rezept-App-Installation des Nutzers: Client (Relying Party)

Grundsätzliche Funktionsweise:

Der Resource Server verwaltet die geschützten Ressourcen (hier: Fachdaten) des Resource Owners und darf nur die von diesem autorisierten Zugriffe durch bestimmte Clients (hier: E-Rezept-App-Installation des Nutzers) erlauben. Zum Nachweis seiner Autorisierung muss der Client den Access-Token vorweisen, der von einer vertrauenswürdigen Stelle, nämlich dem Authorization Server (hier: Identitätsdienst), im Auftrag des Ressource Owners ausgestellt wurde. Um die Ausstellung des Access-Tokens für den Resource Server für einen bestimmten Client zu beauftragen, muss sich der Resource Owner gegenüber dem Authorization Server authentifizieren. Hierzu erzeugt der Client das PKCS-Secret, indem ein Zufallswert (code_verifier) generiert und daraus ein SHA256-Hashwert (code_challenge) berechnet wird. Die Autorisierungsanfrage des Clients an den Authorization Server enthält die code_challenge, die Angabe des zur Berechnung der code_challenge verwendeten Hashverfahren, eine zufällige Client-ID zur eindeutigen Bezeichnung des Clients und einen weiteren Zufallswert (State-Parameter). Der Authorization Server speichert diese Daten unter einer zufälligen Session-ID in der Datei „Challenge“. Dann stellt der Identitätsdienst die für die Anmeldung am Resource Server benötigten Identitätsdaten (Claims) zusammen und überträgt die Challenge und die benötigten Claims als Challenge-Token an den Client.

Nach erfolgter Authentifizierung des Resource Owners durch den Authorization Server (hier z. B. mit der eGK) erhält der Client vom Authorization Server den Authorization-Code zusammen mit dem unveränderten State-Parameter und der Client-ID sowie ein SSO-Token zurück. Mit dem SSO-Token kann der Client später – nach Ablauf der Gültigkeit des (noch fehlenden) Access-Tokens – einen neuen Access-Token beim Identitätsdienst anfordern, ohne dass eine erneute Authentifizierung unter aktiver Mitwirkung des Ressource Owners durchgeführt werden muss. Der Client prüft, ob der State-Parameter und die Client-ID mit den in der Autorisierungsanfrage enthaltenen Werten identisch sind. Ist dies der Fall, fordert der Client mit dem Authorization-Code beim Authorization Server den Access-Token an. Neben dem Authorization-Code enthält diese Autorisierungsanfrage auch die Client-ID sowie das PKCS-Secret (code_verifier).

5.5.2.2 Ablauf der Authentifizierung per eGK

Verfügt der Nutzer über eine NFC-fähige eGK, läuft das Authentifizierungsverfahren wie folgt ab:

1. Die App generiert einen Zufallswert (code_verifier), berechnet daraus einen SHA256-Hashwert (code_challenge) und sendet diesen mit der Autorisierungsanfrage an den Identitätsdienst.

2. Der Identitätsdienst beantwortet die Autorisierungsanfrage mit einem Challenge-Token und den für die Anmeldung am E-Rezept-Fachdienst erforderlichen Attribute (sog. Claims) in Form der Datei „USER_CONSENT“. Die erforderlichen Claims sind:

> Vorname
> Nachname
> Krankenkasse (IK-Nummer)
> Krankenversicherungsnummer (KVNR)

3. Nach Erhalt des Challenge-Tokens und der Datei USER_CONSENT startet die E-Rezept-App den bebilderten und mit erläuternden Hinweisen gestalteten eGK-Scanprozess. Hierbei wird der Nutzer zunächst um die Eingabe der auf seiner eGK aufgedruckten CAN zur Freigabe der NFC-Schnittstelle der eGK sowie seiner PIN gebeten. Die Eingabe von CAN und PIN erfolgt in der App, die diese sodann an die Schnittstelle des betriebssystemseitigen NFC-Scanners weitergibt.

4. Der NFC-Scanner liest nach Eingabe der CAN und PIN das Authentisierungszertifikat der eGK (C.CH.AUT) aus. Der Challenge-Token wird mit dem Authentifizierungszertifikat signiert und mit dem öffentlichen Schlüssel des Identitätsdienstes (PuK_IDP_ENC) von der App verschlüsselt an den Identitätsdienst zurückgesendet.

5. Der Identitätsdienst validiert den zurückerhaltenen Challenge-Token mittels des Authentifizierungszertifikats. Anschließend erzeugt und übermittelt der Identitätsdienst den mit seinem privaten Schlüssel (PrK_IDP_SIG) signierten Authorization-Code und den SSO-Token an die App.

6. Die App erzeugt sodann einen zufälligen 256bit-AES-Schlüssel („Token-Key“), verknüpft ihn mit dem eingangs erzeugten code_verifier zum „key_verifier“ und sendet diesen zusammen mit dem Authorization-Code unter erneuter Nutzung des öffentlichen Schlüssels des Identitätsdienstes (PuK_IDP_ENC) verschlüsselt an den Identitätsdienst zurück.

7. Der Identitätsdienst entschlüsselt und validiert den key_verifier, entnimmt den darin enthaltenen code_verifier und gleicht diesen mit der im Authorization-Code enthaltenen code_challenge ab.

8. Der Identitätsdienst erzeugt den Access-Token und den ID-Token, signiert sie jeweils mit seinem privaten Schlüssel (PrK_IDP_SIG) und verschlüsselt sie mit dem Token-Key (siehe Schritt 6), welchen er dem key_verifier entnimmt. Anschließend übermittelt der Identitätsdienst die verschlüsselten Access- und ID-Token an die App. Der ID-Token enthält die vom E-Rezept-Fachdienst verlangten Claims, die aus dem Authentifizierungszertifikat entnommen werden.

9. Die App entschlüsselt Access- und ID-Token jeweils mit dem Token-Key und validiert die jeweiligen Token-Signaturen anhand des öffentlichen Schlüssels des Identitätsdienstes (PuK_IDP_SIG).

10. Die App übermittelt den Access-Token verschlüsselt an den E-Rezept-Fachdienst.

11. Der E-Rezept-Fachdienst entschlüsselt und validiert den Access-Token mit dem öffentlichen Schlüssel des Identitätsdienstes (PuK_IDP_SIG).

12. Der E-Rezept-Fachdienst ruft die Claims aus dem Access-Token ab und gibt bei positiver Validierung den Zugriff der E-Rezept-App auf die Rezeptdaten frei.

Die SSO-Token für den Identitätsdienst sind 12 Stunden gültig, die Access-Token 5 Minuten und ID-Token 24 Stunden. Vor Anfragen an IDP und E-Rezept-Server ermittelt die App zunächst die Gültigkeit vorhandener Token und löscht ungültige. Bei Ablauf des Access-Tokens wird unter Vorlage des SSO-Tokens vom Identitätsdienst ein neuer Zugriffs-Token angefordert. Bei Ungültigkeit des SSO-Tokens wird eine Neuauthentifizierung des Nutzers initiiert. Zugriffe auf Identitätsdienst und E-Rezept-Fachdienst werden bei Ungültigkeit abgelehnt.

5.5.2.3 Authentifizierung per ePA-App

Das Authentifizierungsverfahren bei der Anmeldung per ePA-App läuft wie folgt ab:

1. Die App lädt vom Identitätsdienst eine aktuelle Liste der Krankenkassen, die eine unterstützte ePA-App anbieten. In der Liste ist jeder unterstützten ePA-App ein spezifischer Identifier zugewiesen.

2. Der Nutzer wählt in der E-Rezept-App seine Krankenkasse aus der Liste aus.

3. Die App generiert einen Zufallswert (code_verifier), berechnet daraus einen SHA256-Hashwert (code_challenge) und sendet diesen mit der Autorisierungsanfrage und dem Identifier der ePA-App der ausgewählten Krankenkasse an den Identitätsdienst.

4. Der Identitätsdienst beantwortet die Autorisierungsanfrage mit einem Redirect an den Autorisierungs-Endpunkt des sektoralen Identitätsdienstes[50] der ausgewählten ePA-App, der anhand des in der Autorisierungsanfrage enthaltenen ePA-App-Identifiers zugeordnet wird. Der Redirect enthält neben der Autorisierungsanfrage auch die für die Anmeldung am E-Rezept-Fachdienst benötigten Attribute sowie die URL einer auf dem Identitätsdienst gehosteten Krankenkassen-spezifischen Webseite mit Links zu der jeweiligen ePA-App in den verschiedenen App-Stores.

5. Die E-Rezept-App öffnet über einen im Redirect enthaltenen App-Link (Android) bzw. Universal Link (iOS) den Authentifizierungs-Screen der ePA-App und übergibt ihr die vom Identitätsdienst umgeleitete Autorisierungsanfrage. Die E-Rezept-App wird dadurch durch das Betriebssystem in den Hintergrund verschoben und in den Zustand „Zeige den Home-Screen an“ versetzt. Ist die ePA-App der Krankenkasse noch nicht installiert, führt dies zum Aufruf der im Redirect enthaltenen URL (siehe Schritt 4).

6. Die ePA-App leitet den Redirect an ihren sektoralen Identitätsdienst weiter.

7. Der sektorale Identitätsdienst identifiziert den Nutzer anhand der im Redirect verlangten Attribute.[51]

8. Der Nutzer erteilt in der ePA-App seine ausdrückliche Zustimmung zur Weitergabe der vom Identitätsdienst verlangten Attribute an die E-Rezept-App.[52]

9. Der sektorale Identitätsdienst erstellt einen Authorization-Code für den Identitätsdienst (authorization_code_idp) und übermittelt diesen mit einem Redirect zur Authentifizierungsfunktion der E-Rezept-App an die ePA-App.

10. Die ePA-App öffnet die E-Rezept-App und übergibt ihr den Authorization-Code.

11. Die E-Rezept-App leitet den Authorization-Code an den Identitätsdienst weiter.

12. Der Identitätsdienst übermittelt den Authorization-Code an den sektoralen Identitätsdienst.

13. Der sektorale Identitätsdienst beantwortet die Autorisierungsanfrage (siehe Schritt 3) mit einem ID-Token (id_token_idp).

14. Der Identitätsdienst prüft den ID-Token und erzeugt, basierend auf den darin enthaltenen Identitätsdaten (Claims) einen eigenen Authorization-Code.

50 Als „sektoraler“ Identitätsdienst wird ein von einzelnen Leistungserbringerkategorien (z. B. Ärzteschaft) oder Krankenkassen (sogenannte „Sektoren“) in der Telematikinfrastruktur bereitgestellter Identitätsdienst bezeichnet, der nach Durchführung einer Authentifizierung Identitätsinformationen über bestimmte Nutzerkategorien (z. B. Versicherte) für verschiedene Fachdienste bereitstellen kann.

51 Gemäß § 336 Abs. 4 SGB V muss die Identifikation „mittels eines geeigneten technischen Verfahrens, das zur Authentifizierung einen hohen Sicherheitsstandard gewährleistet“, durchgeführt werden. Die konkreten Festlegungen zu diesen Verfahren werden durch die jeweilige Krankenkasse getroffen und sind nicht Gegenstand dieser DSFA.

52 Die konkrete Ausgestaltung des Zustimmungsverfahrens liegt im Verantwortungsbereich der Krankenkasse und ist nicht Gegenstand dieser DSFA.

15. Der Identitätsdienst beantwortet die Autorisierungsanfrage der E-Rezept-App mit dem Authorization-Code sowie dem SSO-Token.

16. Die weiteren Schritte entsprechen den Schritten 6 bis 11 bei Anmeldung mit der eGK.

5.5.2.4 Zugangsdaten speichern

Der Prozess zur Registrierung eines alternativen Authentifizierungsschlüssel sieht folgende Schritte vor:

1. Die App erzeugt über die Betriebssystems-APIs in der Secure Enclave das Schlüsselpaar PrK_SE_AUT/PuK_SE_AUT sowie einen zufälligen Key-Identifier zur Kennzeichnung der beiden Schlüssel.

2. Die App signiert mithilfe des privaten Authentisierungsschlüssels PrK.CH.AUT der eGK die folgenden Daten, die zusammen die sog. Pairing-Daten bilden:

> den öffentlichen Schlüssel PuK_SE_AUT und die zur Anwendung des Schlüssels zu verwendenden Algorithmen,

> die folgenden Daten aus dem Authentifizierungszertifikat C.CH.AUT der eGK:

  > der öffentliche Schlüssel (PUK_CH_AUT) und die zur Anwendung des Schlüssels zu verwendenden Algorithmen
  > die Seriennummer,
  > das Gültigkeitsende,
  > die Informationen zum Aussteller,
  > den vom Hersteller vergebenen Namen des vom Nutzer verwendeten Geräts,
  > den Key-Identifier des Schlüsselpaars Prk_SE_AUT/PuK_SE_AUT.

3. Zur Registrierung werden folgende Daten verschlüsselt an den Pairing-Endpunkt des Identitätsdienstes übermittelt (sog. Registrierungsdaten, siehe Ziffer 5.11.4):

> den Access-Token,

> die soeben produzierten Pairing-Daten,

> das Authentisierungszertifikat C.CH.AUT der eGK,

> den vom Benutzer vergebenen Namen für sein Gerät,

> zum Zeitpunkt der Authentisierung erhobene Geräteinformationen bestehend aus:
  > Herstellername,
  > Produktname,
  > Modell,
  > Betriebssystem und Version des Betriebssystems.

Die Verschlüsselung basiert auf Schlüsseln, die über das Discovery Document des IDP- Dienstes publiziert werden.

Die Aufnahme des vom Hersteller vergebenen Namen des Geräts („Produktname“) in die signierten Pairing-Daten dient dem Nutzer in Kombination mit dem von ihm vergebenen Namen des Geräts der Nachvollziehbarkeit der Zuordnung des Pairings zu einem Gerät bei einer Geräte-übergreifenden Verwaltung seiner Pairing-Daten (siehe 5.9.1.4). Es wird hierbei angenommen, dass der Produktnamen über den gesamten Lebenszyklus des Geräts hinweg konstant bleibt (auch über Betriebssystem-Updates hinaus).

4. Der Pairing-Endpunkt des Identitätsdienstes prüft darauf hin:

> den Access-Token auf Gültigkeit,

> ob anhand der Claims des Access-Token die Authentifizierung auf Basis der eGK nachzuvollziehen ist,

> ob die übermittelten Geräteinformationen sich nicht auf der Block-Liste befinden,

> das übermittelte Authentifizierungszertifikats auf Gültigkeit,

> die Integrität der übermittelten Pairing-Daten mithilfe des öffentlichen Schlüssels aus dem Authentifizierungszertifikat C.CH.AUT,

> ob die im Access-Token vorhandene idNummer identisch mit der des übermittelten Zertifikats C.CH.AUT ist,

> ob die in den Pairing-Daten vorhandenen Angaben zu Seriennummer, Gültigkeitsende und Aussteller identisch zu denen des übermittelten Zertifikats C.CH.AUT sind und ob der in den Pairing-Daten vorhandene öffentliche Schlüssel einschließlich der Angaben zu den Algorithmen identisch zu dem in dem Zertifikat C.CH.AUT ist.

5. Bei Fehlschlag einer dieser Prüfungen wird der Registrierungsprozess abgebrochen. Bei Erfolg aller dieser Prüfungen werden die folgenden Registrierungsdaten am Pairing-Endpunkt für die weitere Verwendung im Zuge der Authentifizierung hinterlegt:

- die übertragenen Pairing-Daten einschließlich der Signaturdaten,
- den Zeitpunkt der Anlage,
- den vom Nutzer vergebenen Namen für sein Gerät,
- die idNummer und den übertragenen Key-Identifier.

Das Authentifizierungszertifikat C.CH.AUT wird hierbei nicht gespeichert. Die Kombination von idNummer und Key-Identifier dient zur Referenzierung der verbundenen Geräte (siehe 5.9.1.4).

Die nun verbundene App speichert lokal das Authentifizierungszertifikat C.CH.AUT, die Key-Identifier, und den vom Nutzer vergebenen Namen des Geräts als lokale Registrierungsdaten.

5.6 Verarbeitungstätigkeit 4: E-Rezepte einlösen

5.6.1 Nutzerperspektive

Der Nutzer kann seine E-Rezepte in der Apotheke vor Ort elektronisch einlösen, indem er den in der App gespeicherten Rezeptcode auf dem Bildschirm anzeigt und dann der Apotheke zum Scannen vorlegt. Daneben kann der Nutzer einen in der App gespeicherten Rezeptcode über die App elektronisch einer beliebigen Apotheke zur Einlösung zuweisen, um das Medikament später abzuholen oder liefern zu lassen.

5.6.1.1 Vor-Ort-Einlösung

Für die Einlösung von E-Rezepten in der Apotheke vor Ort muss der Nutzer den Rezeptcode in der App erfasst haben, um ihn anzeigen können. Es gibt zwei Möglichkeiten, den Rezeptcode in der App zu erfassen:

- Einscannen des (ausgedruckten) Rezeptcodes mit der Kamera;
- Abrufen des Rezeptcodes vom E-Rezept-Fachdienst.

Für das Einscannen des Rezeptcodes mit der Kamera muss der Nutzer der App die Systemberechtigung für den Kamerazugriff erteilen. Sobald der Rezeptcode erfasst wurde, kann der Nutzer den Rezeptcode in der App speichern und in der Rezeptübersicht anzeigen lassen. Die weiteren mit dem ausgedruckten Rezeptcode verbundenen Angaben (z. B. Versichertenstammdaten, Arztstempel, Medikamentenbezeichnung) werden in der App nicht erfasst und können somit auch nicht angezeigt werden. Der Nutzer erhält über sein Betriebssystem akustisch, optisch und haptisch Feedback über erfasste Rezeptcodes. Nach erfolgter Vor-Ort-Einlösung in der Apotheke kann der Nutzer den Rezeptcode in der App als eingelöst markieren. Gespeicherte Rezeptcodes können durch den Nutzer jederzeit gelöscht werden.

Zum Abrufen der Rezeptcodes direkt vom E-Rezept-Fachdienst muss sich der Nutzer am E-Rezept-Fachdienst anmelden. Nach erfolgter Anmeldung lädt die App automatisch alle im E-Rezept-Fachdienst gespeicherten E-Rezepte des Nutzers (einschließlich deren Rezeptcodes) herunter und speichert diese als lokale Kopie.

Der Nutzer kann die Rezeptcodes in der Apotheke vor Ort somit auch ohne aktive Internetverbindung vorzeigen.

Wenn der Nutzer einen Rezeptcode mit der Kamera eingescannt hat, ohne am E-Rezept-Fachdienst angemeldet zu sein, speichert die App zunächst nur den Rezeptcode (s. o.). Meldet sich der Nutzer später am E-Rezept-Fachdienst an, so dass alle im E-Rezept-Fachdienst gespeicherten E-Rezepte heruntergeladen und als lokale Kopie gespeichert werden, werden die zu dem eingescannten Rezeptcode lokal gespeicherten Informationen durch die vom E-Rezept-Fachdienst zu dem betreffenden E-Rezept heruntergeladenen ersetzt. Sollte der Nutzer den betreffenden Rezeptcode in der App also bereits gelöscht oder (irrtümlich) als eingelöst markiert haben, wird das zugehörige E-Rezept (einschließlich des Rezeptcodes und Rezeptstatus), solange es auf dem E-Rezept-Fachdienst gespeichert ist, erneut bzw. mit dem tatsächlichen Status in der App gespeichert.

5.6.1.2 Elektronische Einlösung

Zum Starten des elektronischen Einlöseprozesses für die direkte Zuweisung eines Rezeptcodes vom E-Rezept-Fachdienst zu einer Apotheke muss der Nutzer am E-Rezept-Fachdienst angemeldet sein. Es stehen folgende Optionen für die (Fern-)Einlösung und Medikamentenbereitstellung zur Auswahl:

- Reservieren zur Abholung,
- Lieferung per Botendienst anfragen und
- per Versand liefern.

Über die Apothekensuche kann der Nutzer gezielt eine Apotheke suchen, die die vom Nutzer gewünschte Option anbietet. Alternativ kann der Nutzer auch nach Apotheken, die bestimmte Kriterien erfüllen (z. B. Apotheken in der Umgebung), suchen und sich dann anzeigen lassen, welche Bereitstellungsoptionen diese anbieten. Dabei kann der Nutzer im Fall von Sammelrezepten die Einlösung auch auf einzelne Rezeptcodes des Sammelrezepts beschränken, so dass die einzelnen E-Rezepte auf unterschiedliche Art bzw. bei verschiedenen Apotheken eingelöst werden können.

Nachdem ein E-Rezept bei einer Apotheke per App eingelöst worden ist, wird der Status des E-Rezepts in der Rezeptübersicht entsprechend laufend aktualisiert, solange der Nutzer am E-Rezept-Fachdienst angemeldet ist. In den ersten fünf Minuten nach einer Einlösung wird der Status auf „in Einlösung“ gesetzt, so dass eine erneute Einlösung zunächst nicht mehr möglich ist. Bestätigt die ausgewählte Apotheke in dieser Zeit die Einlösung nicht oder lehnt sie die Einlösung ab, wechselt der Status wieder auf „einlösbar“.

Wählt der Nutzer die Botendienstlieferung, muss er eine Telefonnummer zur Ermöglichung der Kommunikation des Boten mit dem Nutzer angeben. Zudem kann er eine von seiner im E-Rezept genannten Anschrift abweichende Lieferadresse angeben. Die Angaben des Nutzers werden gespeichert, sodass sie bei weiteren Botendienstlieferungen bei Bedarf nicht erneut eingegeben werden müssen; der Nutzer kann seine gespeicherten Angaben bei Bedarf jederzeit löschen.

Die Versandoption steht nur bei Wahl einer Versandapotheke zur Verfügung. Der Nutzer muss in der App die zu versendenden Medikamente sowie seine Lieferanschrift eingeben. Die App schlägt dem Nutzer die im E-Rezept enthaltene Anschrift als Lieferanschrift vor, der Nutzer kann jedoch auch eine abweichende Lieferanschrift angeben. Vor der verbindlichen Bestellung bei der ausgewählten Versandapotheke zeigt die App dem Nutzer in einer Übersicht nochmals die Lieferadresse sowie die zu versendenden Medikamente an. Ist der Nutzer einverstanden, kann er die Bestellung final aufgeben. Falls die gewählte Apotheke zum Abschluss der Bestellung weitere Interaktion erfordert, erhält der Nutzer eine Mitteilung in die E-Rezept App übermittelt. Diese Mitteilung enthält einen Bestellungs-individuellen Link, der als „Warenkorb öffnen“ angezeigt wird. Der Link ist als externer Verweis gekennzeichnet und leitet den Nutzer in die reguläre Warenkorbansicht des Onlineshops der ausgewählten Versandapotheke, wobei der Warenkorbinhalt und das Feld zur Angabe der Lieferanschrift bereits mit den Nutzereingaben aus der App vorausgefüllt sind. Der Nutzer kann seine Bestellung außerhalb der App im Onlineshop der Versandapotheke nun wie ein regulärer (Gast-)Nutzer des Onlineshops fortsetzen und bei Bedarf auch weitere Produkte in den Warenkorb legen. Der weitere Bestellprozess für die Bezahlung und Bestellung richtet sich nach den Vorgaben der Versandapotheke.

Nachdem die ausgewählte Apotheke die elektronische Einlösung bestätigt hat, wird das betreffende E-Rezept in der Bestellübersicht der App angezeigt.

5.6.2 Anwendungs-/Infrastrukturebene

Zum Einscannen von Rezeptcodes nutzt die App den für die Kamera zuständigen Betriebssystemdienst. Hat der Nutzer die Systemberechtigung für die Kamerafunktion noch nicht freigegeben, stellt die App einen entsprechenden Permission-Request an das Betriebssystem.

Bei der Nutzung der Kamerafunktion wird das Kamerabild während der Aufnahme und Weiterleitung an die App durch den für die Kamera zuständigen Betriebssystemdienst kurzzeitig lokal verarbeitet.

Im Fall des Android- und des EMUI-Betriebssystems wird das Kamerabild durch den Barcodescanner-Betriebssystemdienst (Google ML Kit/Huawei ML Kit) analysiert. Google behält sich in den vom Nutzer zu bestätigenden Nutzungsbedingungen und Datenschutzhinweisen vor, die dabei anfallenden Nutzungsdaten („Angaben zur Gerätenutzung“) auszuwerten und zur Optimierung und Fehlerbehebung des verwendeten SDK zu verwenden. Die inhaltliche Verarbeitung des Rezeptcodes, d. h. das Auslesen des Rezeptcodes aus dem Kamerabild und die Weitergabe an die App, erfolgt jedoch ebenso wie im Fall der iOS-Version der App ausschließlich lokal und ohne Speicherung des Rezeptcodes im vom Betriebssystem verwalteten Speicher.

Die individuellen Bestelldaten (ggf. abweichende Lieferadressen und Kontaktrufnummern) werden von der App lokal verschlüsselt gespeichert und nur im Rahmen von Bestellungen über den Mitteilungsdienst des E-Rezept-Fachdienstes an die Apotheke weitergeleitet. Solange der Nutzer die individuellen Bestelldaten nicht löscht, werden sie bei weiteren Bestellungen mit der gleichen Lieferoption genutzt, um die entsprechenden Felder vorauszufüllen. Die Rezeptcodes der eingelösten E-Rezepte werden sowie die weiteren Bestelldaten (z. B. gewählte Lieferoption) ebenfalls nur über den Mitteilungsdienst an den E-Rezept-Fachdienst übermittelt, der sie dann für die vom Nutzer ausgewählte Apotheke freigibt.

Löst der Nutzer ein E-Rezept bei einer Versandapotheke ein, stellt die Versandapotheke über den Mitteilungsdienst des E-Rezept-Fachdienstes eine individuelle URL zur Verfügung, die direkt in die vorausgefüllte Warenkorbansicht ihres Webshops führt. Die App empfängt die Warenkorb-URL vom Mittteilungsdienst des E-Rezept-Fachdienstes und bindet den Warenkorb in der Einlöseansicht der App als externen Link ein.

Mit der Einlösung eines E-Rezepts bei einer Apotheke wird ein Hintergrundprozess ausgelöst, wodurch die App laufend beim E-Rezept-Fachdienst Statusänderungen und neue Mitteilungen in Bezug auf das eingelöste E-Rezept abfragt und diese ggf. in der App anzeigt.

Gleichzeitig wird ein Hintergrundprozess ausgelöst, wodurch die App während der Anmeldedauer am E-Rezept-Fachdienst fortlaufend beim E-Rezept-Server nach aktualisierten Fachdaten (Mitteilungen, Statusänderungen, Protokolleinträge, Abgabeinformationen usw.) in Bezug auf die eingelösten Rezeptcodes anfragt.

5.7 Verarbeitungstätigkeit 5: Apothekensuche und -bestimmung

5.7.1 Nutzerperspektive

Im Menüpunkt „Apotheken“ oder im Rahmen der elektronischen Einlösung wird dem Nutzer ein Bildschirm für die Suche nach Apotheken angezeigt, mit einem Freitext-Eingabebereich für den Namen oder die Adresse von Apotheken. Wählt der Nutzer die Umkreissuche, folgt der Permission-Request des Betriebssystems. Die Apothekensuche verfügt über eine Filterfunktion, so dass die vom Nutzer eingegebenen Suchkriterien (Öffnungszeiten, E-Rezept-Anbindung, Lieferoptionen) bei der Suche berücksichtigt werden können.

5.7.2 Anwendungs-/Infrastrukturebene

Für die Apothekensuche nutzt die App das Apothekenverzeichnis. Die Sucheingaben bzw. Filterkriterien werden verschlüsselt an den Server-Endpunkt des Apothekenverzeichnisses übermittelt und mit der Apothekendatenbank abgeglichen. Der Abgleich mit dem Apothekenverzeichnis erfolgt mit einer gewissen Fehlertoleranz, so dass typische Eingabefehler berücksichtigt werden. Es werden bis zu 50 Ergebnisse verschlüsselt an die App zurückgeliefert. Bei der Umkreissuche auf Basis des vom Betriebssystem ermittelten Standorts wird als Sucheingabe der geographische Standort des Smartphones an das Apothekenverzeichnis übermittelt.

Die Daten des zentralen Verzeichnisdienstes werden durch die Apothekenkammern gepflegt. Zu diesen Daten gehören z. B. Adressierungsinformationen innerhalb der TI, Basis-Kontaktdaten und Anschrift.

Die ergänzenden Inhalte des Apothekenverzeichnisses werden von den Apotheken oder deren Dienstleistern selbst eingepflegt. Hierbei handelt es sich z. B. um Öffnungszeiten, weitere Kontaktdaten, angebotene Dienstleistungen oder technische Informationen.

5.8 Verarbeitungstätigkeit 6: Mitteilungsfunktion

5.8.1 Nutzerperspektive

Im Rahmen der elektronischen Einlösung gibt die App dem Nutzer die Möglichkeit, über die Mitteilungsfunktion mit der ausgewählten Apotheke zu kommunizieren. Hat der Nutzer eine elektronische Einlösung vorgenommen, kann er in der App Mitteilungen an die ausgewählte Apotheke senden oder von dieser empfangen. Alle Mitteilungen sind stets an ein bestimmtes E-Rezept bzw. eine Rezeptcode-Zuweisung an die betreffende Apotheke gekoppelt, so dass Kontaktaufnahmen aus anderen Anlässen nicht möglich sind. Ist der Nutzer am E-Rezept-Fachdienst angemeldet, wird er in der App durch rote Badges am Menüpunkt „Mitteilungen“ über neue Mitteilungen informiert.

5.8.2 Anwendungs-/Infrastrukturebene

Die Kommunikation mit Apotheken erfolgt verschlüsselt über den Mitteilungsdienst des E-Rezept-Fachdienstes. Die Speicherdauer von Mitteilungen auf dem E-Rezept-Fachdienst entspricht der Speicherdauer des betreffenden E-Rezepts. Die Fortsetzung einer begonnenen Kommunikation ist nur möglich, solange das betreffende E-Rezept den Status „einlösbar“ hat.

Der E-Rezept-Fachdienst protokolliert die Sendezeit, die Empfangszeit sowie die Abrufzeiten der Mitteilungen sowie den Lesestatus. Außerdem zählt der E-Rezept-Fachdienst die Anzahl der auf eine Task-ID bezogenen Mitteilungen, damit die zulässige Mitteilungszahl (10 Mitteilungen pro E-Rezept) eingehalten wird. Zum Inhalt von Mitteilungen: siehe unten 5.11.8.10.

5.9 Verarbeitungstätigkeit 7: Verwaltung von Fach-/Zugangsdaten

5.9.1 Nutzerperspektive

Wenn der Nutzer am E-Rezept-Fachdienst angemeldet ist, kann er mit den nachfolgend beschriebenen Funktionen neben seinen E-Rezepten auch auf weitere im E-Rezept-Fachdienst und Identitätsdienst gespeicherte Daten zugreifen und diese in einem gewissen Umfang verwalten.

5.9.1.1 E-Rezepte verwalten

Der Nutzer kann nach der Anmeldung am E-Rezept-Fachdienst im Rahmen seiner Zugriffsberechtigung alle aktuell im E-Rezept-Fachdienst gespeicherten E-Rezepte sowie die zugehörigen Task-IDs, AccessCodes, Rezeptcodes und Rezeptstatus abrufen und als lokale Kopie in der App speichern und einsehen. Die Detailansicht eines heruntergeladenen E-Rezepts enthält einen Link zum Nationalen Gesundheitsportal sowie in bestimmten Fällen allgemeine Hinweise und Warnungen, etwa zu demnächst ablaufenden E-Rezepten oder zur Austauschbarkeit des verordneten Medikaments (Generika). Solange der Nutzer am E-Rezept-Fachdienst angemeldet ist, werden die heruntergeladenen Daten regelmäßig im Hintergrund mit den auf dem E-Rezept-Fachdienst gespeicherten Daten abgeglichen und ggf. aktualisiert. Ist der Nutzer nicht mehr am E-Rezept-Server angemeldet, bleiben die zuletzt heruntergeladenen Kopien in der App gespeichert; in der App wird dann eine Mitteilung angezeigt, dass die angezeigten Daten möglicherweise nicht aktuell sind.

Der Nutzer kann lokale Kopien von E-Rezepten jederzeit löschen, auch wenn die App nicht am E-Rezept-Fachdienst angemeldet ist. Ist die App angemeldet, können per App auch die auf dem E-Rezept-Fachdienst

gespeicherten E-Rezepte gelöscht werden, solange sie nicht den Rezeptstatus „in Abgabe (gesperrt)“ haben. Vor jeder Löschaktion zeigt die App eine Warnung an, die den Nutzer auf die Unwiderruflichkeit der Löschung hinweist. Erst nach Bestätigung dieser Warnung durch den Nutzer erfolgt die Löschung.

5.9.1.2 E-Rezepte teilen

Der Nutzer kann die lokale Kopie eines E-Rezept-Tokens bzw. den Rezeptcode eines E-Rezepts mit dem Rezeptstatus „einlösbar“ per App mit einer anderen App teilen. Wenn der Nutzer den Teilen-Button betätigt, öffnet sich das In-App-Sharesheet des Betriebssystems. Darüber kann der Nutzer einen Link mit einer App oder einem in der Nähe befindlichen Gerät per WiFi oder Bluetooth teilen (z. B. per AirDrop (iOS) oder Nearby Share (Android, EMUI)). Der Link verweist auf eine Landingpage mit der URL https://www.das-e-rezept-fuer-deutschland.de/prescription und enthält einen URL-Parameter mit dem E-Rezept-Token des geteilten E-Rezepts. Sofern der Nutzer als Ziel eine App auswählt, die Bilddateien entgegennehmen kann (z. B. eine E-Mail- oder Messenger-App), enthalten die geteilten Informationen auch das E-Rezept-Logo und den DataMatrix-Code des geteilten E-Rezepts (Rezeptcode). Wenn der Empfänger des Links nun die Landingpage in seinem mobilen Webbrowser aufruft und er bereits die E-Rezept-App installiert hat, wird diese automatisch geöffnet und der E-Rezept-Token als Rezeptcode gespeichert. Der Empfänger kann den gespeicherten Rezeptcode dann in der Apotheke zur Einlösung vorzeigen. Ist die E-Rezept-App noch nicht installiert, leitet die Landingpage den Empfänger in den jeweiligen App-Store auf die Seite der E-Rezept-App, so dass er die App einfach installieren kann. Wenn der Empfänger nach der Installation der App erneut den Link aufruft, wird der Rezeptcode in der App gespeichert.

Eine weitere Möglichkeit zum Teilen von E-Rezepten besteht darin, den E-Rezept-Token direkt über den E-Rezept-Fachdienst mit einem anderen Versicherten zu teilen, der ebenfalls die App nutzt und am E-Rezept-Fachdienst angemeldet ist. Hierzu muss der Nutzer im Sharesheet als Ziel-App die (eigene) E-Rezept-App auswählen. In der App öffnet sich dann ein Eingabedialog, mit dem die KVNR des Empfängers abgefragt wird. Die zuletzt genutzten KVNR werden in der App gespeichert und können um einen Namen ergänzt werden (im Sinne eines KVNR-Adressbuchs). Nach dem Teilen erscheint in den Mitteilungen eine Bestätigung, dass das E-Rezept für den angegebenen Empfänger bzw. die angegebene KVNR auf dem E-Rezept-Fachdienst freigegeben wurde.

5.9.1.3 Zugriffsprotokolle einsehen

Die App kann genutzt werden, um die vom E-Rezept-Fachdienst verwalteten Protokolldaten zu Zugriffen auf Fachdaten einzusehen. Die Anzeige der Protokolleinträge in der App enthält jeweils folgende Angaben:

- Bezeichnung des E-Rezepts (z. B. Medikamentenname),
- Name und Rolle des Zugreifenden,
- Zeitpunkt des Zugriffs und
- Art und Ergebnis des Zugriffs (z. B. dass ein E-Rezept bereitgestellt oder gelöscht worden ist oder dass der Zugriff verweigert wurde).

Die App zeigt zudem das Abrufdatum des in der App angezeigten Zugriffsprotokolls an (Datum und Uhrzeit), so dass der Nutzer die Aktualität der Informationen beurteilen kann. Es werden stets alle auf dem E-Rezept-Fachdienst gespeicherten Protokolleinträge geladen. Aufgrund der gesetzlich angeordneten dreijährigen Speicherfrist (§ 309 Abs. 1 SGB V) kann der Nutzer die Protokolleinträge auf dem E-Rezept-Fachdienst nicht per App löschen lassen.

5.9.1.4 Geräteregistrierungen verwalten

Die App kann nach der Anmeldung am Fachdienst genutzt werden, um die vom Identitätsdienst verwalteten Daten zu den „verbundenen Geräten“ einzusehen. Verbundene Geräte sind solche, die vom Nutzer (oder einer anderen Person) in der Vergangenheit zur Anmeldung am E-Rezept-Fachdienst mit den Authentifizierungsdaten des Nutzers verwendet worden sind, wobei auf dem verwendeten Gerät bzw. in der auf diesem installierten E-Rezept-App die Option „Zugangsdaten speichern“ aktiviert wurde. Zur einfachen Erkennbarkeit der verbundenen Geräte werden sie in der App jeweils mit folgenden Informationen dargestellt:

- Name des Produkts (z. B. „iPhone 13“),
- Seriennummer, Aussteller und Gültigkeitsende des bei der Geräteregistrierung verwendeten eGK-Zertifikats (C.CH.AUT),
- Registrierungszeitpunkt und
- Gerätename (z. B. „iPhone von Felix“).

Falls der Nutzer die Verbindung eines angezeigten verbundenen Geräts aufheben möchte, kann er den Identitätsdienst über die App mit der Deaktivierung der Verbindung beauftragen. Die Deaktivierung führt dazu, dass sich das betreffende Gerät mit den auf diesem gespeicherten Registrierungsdaten innerhalb einer Stunde nicht mehr am E-Rezept-Fachdienst anmelden kann bzw. eine aktive Anmeldung beendet wird. Nach dem Erhalt der Deaktivierungsanfrage wird dem Nutzer die Antwort des Identitätsdienstes mit Informationen zum Ergebnis der Deaktivierungsanfrage angezeigt (z. B. ob die Deaktivierung durchgeführt werden konnte und wann mit dem Wirksamwerden der Deaktivierung zu rechnen ist).

5.9.2 Anwendungs-/Infrastrukturebene

5.9.2.1 E-Rezepte verwalten

Jedes vom E-Rezept-Fachdienst heruntergeladene E-Rezept wird von der App entschlüsselt und validiert, bevor es lokal gespeichert werden kann. Die Verwaltung von E-Rezepten auf dem E-Rezept-Fachdienst über die App ist nur für den Versicherten als Nutzer, nicht aber für Vertreter als Nutzer möglich. Wenn der Nutzer auf dem E-Rezept-Fachdienst ein E-Rezept löscht und angemeldet ist, wird auch eine etwaig gespeicherte lokale Kopie gelöscht. Der Lösch-Request an den E-Rezept-Fachdienst enthält den aktuellen Access-Token des Nutzers sowie die Task-ID und den AccessCode des zu löschenden Rezepts.

5.9.2.2 E-Rezepte teilen

Zum Teilen eines E-Rezepts mit anderen Apps oder Geräten nutzt die App den regulären Sharesheet-Betriebssystemdienst. Die Landingpage enthält Links zu den App-Store-Seiten der E-Rezept-App sowie Steuerungsinformationen (z. B. zur Anzeige sogenannter smarter Banner), mit denen der mobile Webbrowser den Installationsstatus der App feststellen und den Nutzer ggf. an die App bzw. auf die App-Store-Seite der App weiterleiten kann.

Beim Teilen eines E-Rezepts über die E-Rezept-App wird die eingegebene KVNR und ggf. der Name des Empfängers lokal gespeichert. Eine Übermittlung dieser Daten erfolgt nicht.

5.9.2.3 Zugriffsprotokolle einsehen

5.9.2.4 Geräteregistrierungen verwalten

Damit die App zum Abrufen und Anzeigen der Liste der verbundenen Geräte verwendet werden kann, muss sie dem Identitätsdienst einen gültigen Access-Token vorlegen. Nachdem der Identitätsdienst den vorgelegten Access-Token validiert hat, entnimmt er die im Access-Token enthaltene KVNR unter stellt eine Liste aller mit dieser KVNR verbundenen Geräteregistrierungen zusammen. Die Liste enthält für jede Geräteregistrierung auch den im Rahmen der Registrierung des jeweiligen Geräts verwendeten Key-Identifier.

Wenn der Nutzer in der App die Verbindung eines Geräts deaktiviert, wird ein Deaktivierungs-Request mit dem Access-Token und dem Key-Identifier des zu trennenden Geräts an den Identitätsdienst gesendet. Der Identitätsdienst validiert den Access-Token und deaktiviert schließlich die zu deaktivieren Geräte, wobei erneut die im Access-Token enthaltene KVNR und die genannten Key-Identifier als Referenzmerkmale genutzt werden.

Der Identitätsdienst beantwortet den Deaktivierungs-Request mit einem Statuscode, der dem Nutzer in der App in verständlicher Form angezeigt wird (etwa ob die Deaktivierung durchgeführt wurde bzw. in welcher Frist dies geschieht oder ob technische Fehler eine Deaktivierung verhindern).

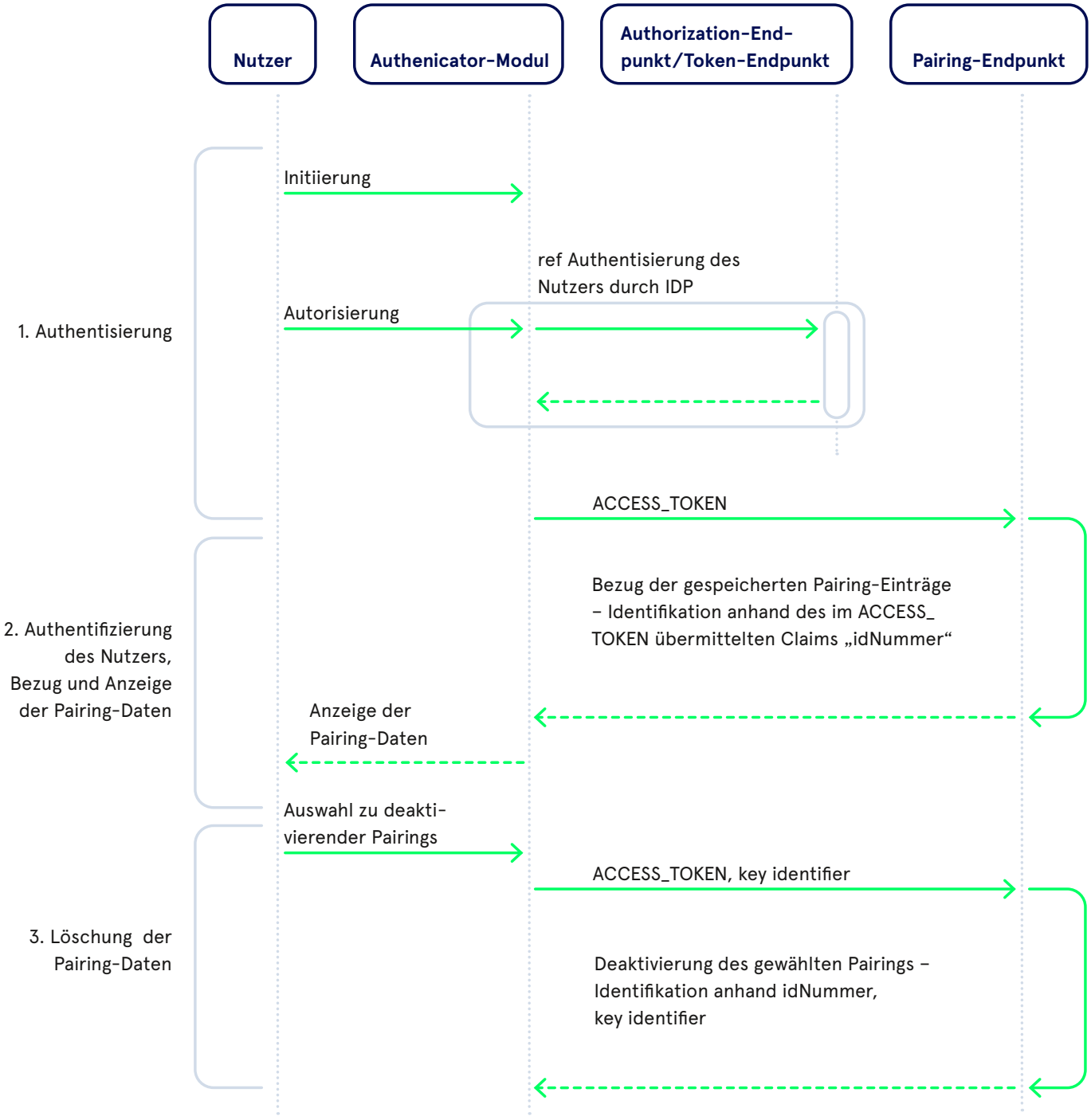


Abbildung 1: Ablauf der De-Registrierung

5.10 Verarbeitungstätigkeit 8: Nutzungsanalyse[53]

5.10.1 Nutzerperspektive

Der Nutzer kann in den App-Einstellungen mit einem Umschalter die Nutzungsanalyse aktivieren. Standardmäßig ist die Nutzungsanalyse deaktiviert (Opt-in-Prinzip). Der Umschalter wird flankiert von einem Datenschutzhinweis, mit dem der Nutzer in knapper Form über die Zwecke der Nutzungsanalyse (Verbesserung des Nutzungserlebnisses, Fehleranalyse nach Abstürzen) informiert wird. Wenn der Nutzer den Umschalter aktiviert, wird das Einstellungsmenü von einer zweiten Informationsebene mit einer Dialogbox überlagert. Die Dialogbox enthält nähere Informationen zur Datenverarbeitung und verweist ergänzend auf die verlinkte Datenschutzerklärung der App. Dabei werden dem Nutzer auch die jederzeitige Deaktivierbarkeit der Nutzungsanalyse sowie die Identität und Kontaktdaten des Analytics-Dienstleisters mitgeteilt. Der Nutzer kann die Nutzungsanalyse nun jeweils per Button erlauben oder ablehnen. Erlaubt der Nutzer die Nutzungsanalyse, schließt sich die Dialogbox und der Umschalter für die Nutzungsanalyse wird aktiviert. Lehnt der Nutzer die Nutzungsanalyse ab oder schließt er die Dialogbox mit der Fenster-Schließen-Schaltfläche (Kreuz-Symbol), bleibt der Umschalter für die Nutzungsanalyse deaktiviert.

5.10.2 Anwendungs-/Infrastrukturebene

Die App enthält das Software Development Kit (SDK) des von der gematik beauftragten Dienstleisters für App-Analyselösungen. Der Dienstleister soll standardisierte Analytics-Dienstleistungen, wobei die gematik zugestimmt hat, dass der Analytics-Dienstleister die IT-Infrastruktur von Amazon Webservices (AWS) als Auftragsverarbeiter nutzt, sofern diese Verarbeitung ausschließlich auf Servern in der EU-Region stattfindet.

Das Analyseverfahren ist als reines Session-Tracking konfiguriert, sodass jeweils nur das Nutzungsverhalten während einer Session zusammenhängend analysiert werden kann. Eine Session beginnt mit dem Öffnen der App. Sie endet, wenn der Nutzer die App schließt oder andernfalls nach 30-minütiger Inaktivität (z. B. nachdem die App in den Hintergrundbetrieb gelegt oder das Smartphone während einer laufenden Session gesperrt wurde). Bei aktivierter Nutzungsanalyse ruft das SDK bei jedem App-Start die aktuelle Konfigurationsdatei für das SDK vom Server des Dienstleisters ab (sofern eine Internetverbindung besteht) und generiert eine neue zufällige Session-ID und löscht gleichzeitig die alte Session-ID. Der Abruf der aktuellen Konfigurationsdatei ermöglicht, dass die technischen Details des Analyseverfahrens angepasst werden können, ohne dass ein neues App-Release bereitgestellt werden muss. Zur Analyse werden folgende Daten erfasst:

- Angezeigter Screen
- Betätigte Screen-Elemente
- Verweildauer zwischen Nutzerinteraktionen und ähnliche
- Programmfehler und Abstürze

Die Datenerfassung beschränkt sich auf allgemeine Gerätedaten und Nutzungsdaten zu Events (welche Screens werden angezeigt, welche Buttons werden betätigt, Dauer der Session, Fehlermeldungen), mit denen das Gerätemodell, die Betriebssystemumgebung und der User Flow des Nutzers sowie eventuelle Programmfehler bzw. App-Abstürze während der jeweiligen Session nachvollzogen werden können. Es werden im Rahmen der Nutzungsanalyse keine Geräte- oder Nutzungsdaten erhoben, die Rückschlüsse auf die Identität des Nutzers oder den Inhalt von E-Rezepten zulassen (z. B. Name des Geräts[54], Geräte-IDs, Screen-Inhalte oder Eingaben in der App).

Die getrackten Eventdaten werden von der App jeweils temporär lokal gespeichert. Sobald 50 Events angefallen sind oder bei Ende der Session werden die einzelnen Event-Datensätze in einer Batchdatei zusammengefasst und diese zusammen mit der Session-ID an den API-Endpunkt des Analysedienstes übertragen. Die lokalen Eventdaten bzw. die Batchdatei werden anschließend gelöscht.

53 Im Prüfungszeitraum verfügte die E-Rezept-App nicht über eine Trackingfunktion für die Nutzungsanalyse. Es ist geplant, diese mit einem der nächsten Releases einzuführen. Die nachfolgende Beschreibung legt die aktuelle Umsetzungsplanung zugrunde.

54 Gemeint ist der vom Nutzer vergebene Gerätename, der häufig Hinweise auf den Namen des Nutzers enthält („Susanne Musterfraus iPhone“).

Die API-Endpunkte für den Abruf der Konfigurationsdatei und die Entgegennahme der Batches werden jeweils auf einem vorgeschalteten Server, der als Load Balancer fungiert, bereitgestellt. Unmittelbar nach Beendigung des jeweiligen Übertragungsvorgangs und somit vor der Weiterleitung an den Analyseserver des Dienstleisters löscht der Load Balancer die Zugriffsdaten mit der IP-Adresse des Nutzers aus seinem Arbeitsspeicher, so dass die Session-ID als einziges Zuordnungsmerkmal der erhaltenen Analysedaten verbleibt. Ein Logging oder eine Sicherung der auf dem Load Balancer anfallenden Daten erfolgt nicht.

Die empfangenen Batches werden vom Load Balancer zwischengespeichert und nach Ende der jeweiligen Session an den Analyseserver weitergeleitet und von diesem anhand der Session-ID aggregiert und für die Analyse aufbereitet. Die zuständigen Mitarbeiter der gematik können die aufbereiteten Analysedaten über ein zugangsgeschütztes Web-Frontend einsehen. Die aggregierten und aufbereiteten Daten enthalten weder Session-IDs noch sonstige Angaben, die Rückschlüsse auf einzelne Personen zulassen. Zugriffsmöglichkeit auf die aggregierten Daten besteht auf technischer Ebene auch für die Administratoren. Auf explizite Anfrage der gematik hin, erhalten auch die Datenanalysten des Analytics-Dienstleisters Zugriff auf die Daten, um Supportanliegen zu bearbeiten oder die gematik bei der Auswertung zu unterstützen. Deaktiviert der Nutzer die Nutzungsanalyse in den App-Einstellungen, werden sofort alle vom SDK erzeugten und lokal gespeicherten Daten (Event-Datensätze, Session-ID) gelöscht. Außerdem wird die Erzeugung weiterer Daten beendet. Solange die Nutzungsanalyse deaktiviert ist, erfolgt auch kein Abruf der Konfigurationsdatei beim App-Start. Der Analytics-Dienstleister nutzt für den Betrieb des Load Balancers, des Analyseservers sowie zur Datensicherung der Daten auf dem Analyseserver die Infrastruktur von AWS in den AWS-Regionen Irland und Stockholm. Jeder Datenverkehr zwischen der App und den API-Endpunkten des Load Balancers sowie zwischen den AWS-Servern erfolgt jeweils über eine TLS-verschlüsselte HTTPS-Verbindung. Die Datensicherungsdaten werden jeweils nach 13 Monaten automatisch gelöscht.

5.11 Datenarten

Die verschiedenen Datenarten, die im Rahmen des Prüfgegenstands verarbeitet werden, werden den nachfolgend beschriebenen Kategorien zugeordnet. Die Kategorien umfassen jeweils verschiede Datentypen, die durch gemeinsame thematische bzw. inhaltliche Merkmale gekennzeichnet sind. Kriterien der Zuordnung sind insbesondere die jeweils betroffenen Personen und die primären Verwendungszwecke der Daten.[55] Die verwendeten Kategorien sind nicht gänzlich trennscharf, so dass einzelne Datenarten begrifflich unter mehrere Kategorien fallen können, je nachdem, welchem Zweck sie konkret dienen.

5.11.1 Authentifizierungsdaten

Authentifizierungsdaten werden im Rahmen der Überprüfung der Zugriffsberechtigung für den E-Rezept-Fachdienst und bei Nutzung der Option zur lokalen Speicherung der Zugangsdaten für den E-Rezept-Fachdienst mittels des betriebssystemseitigen Entsperrmechanismus verarbeitet. Da die Anmeldung am E-Rezept-Fachdienst nur nach erfolgreicher Überprüfung der Zugriffsberechtigung des Zugreifenden erfolgen darf, muss sich der Zugreifende zunächst gegenüber dem Identitätsdienst authentifizieren. Dabei fallen je nach genutztem Verfahren unterschiedliche Authentifizierungsdaten an.

Bei der Authentisierung mit der eGK umfassen die Authentifizierungsdaten insbesondere die Daten im Authentifizierungszertifikat (C.CH.AUT) sowie die PIN und CAN der eGK. Bei Nutzung des systemseitigen lokalen Authentifizierungs- bzw. Entsperrmechanismus für die Speicherung der Zugangsdaten umfassen die Authentifizierungsdaten auch jene Daten, die der Entsperrmechanismus benötigt, beispielsweise den Geräte-Zugangscode (PIN, Passwort) oder biometrische Daten (Fingerabdruck, Gesichtsdaten).

55 Die nachfolgende Kategorisierung dient der funktionalen Beschreibung und Systematisierung der verarbeiteten Daten. Die datenschutzrechtliche Frage des Personenbezugs und der Zugehörigkeit zu einer besonderen Kategorie personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO wird in Abschnitt 7.1.1behandelt.

5.11.2 Zugangsschlüssel (Token)

Der Identitätsdienst stellt der App nach erfolgreicher Authentifizierung entsprechend dem OpenID-Connect-Identitätsprotokoll drei Token aus, mit denen sich der Nutzer am E-Rezept-Fachdienst anmelden und auf die für ihn zugänglichen Fachdaten zugreifen kann:

- ID-Token (auch als AuthN-Token bezeichnet),
- Access-Token und
- SSO-Token

Der ID-Token enthält die bestätigten Identitätsdaten des Nutzers, die der E-Rezept-Fachdienst für die Autorisierung des Zugriffs benötigt. Er wird vom Identitätsdienst an die App ausgegeben. Die App nutzt den ID-Token, um lokal die Identität des Nutzers zu bestätigen. Der ID-Token ist gerätegebunden, d. h. er kann nur auf einem bestimmten Smartphone genutzt werden. Er hat eine Gültigkeit von maximal 24 Stunden.

Der Access-Token enthält die Zugriffsberechtigung (im Sinne von Zugangsdaten) für die für den jeweiligen Nutzer zugänglichen Fachdaten auf dem E-Rezept-Fachdienst. Der Access-Token wird vom Identitätsdienst zusammen mit dem ID-Token an die App ausgegeben. Er ist nicht gerätegebunden, d. h. jeder, der im Besitz des Access-Tokens ist, kann diesen nutzen. Er hat eine kurze Gültigkeitsdauer von fünf Minuten.

Der SSO-Token enthält die Berechtigung zum Erhalt eines neuen Access-Token, ohne dass eine neue Authentifizierung am Identitätsdienst durchgeführt werden muss. Die Gültigkeitsdauer des SSO-Tokens beträgt 12 Stunden.

5.11.3 Gerätedaten

Die App erhebt zu verschiedenen Zwecken Informationen über das Smartphone. Gerätedaten umfassen beispielsweise:

- Name des Herstellers (z. B. „Apple“),
- Name des Produkts (z. B. „iPhone 13“),
- Name des Modells (z. B. „A2633“),
- Name und Version des Betriebssystems 8 (z. B. „iOS 16.1“) und
- Informationen zur Geräteintegrität (Attestationsergebnis).

Der Inhalt des Attestationsergebnisses hängt vom Betriebssystem des Nutzers bzw. dem jeweils verwendeten Integritätsprüfungs-Dienst ab.

5.11.4 Registrierungsdaten (Zugangsdaten)

Wenn der Nutzer ein alternatives Authentifizierungsmittel einrichtet, d. h., wenn er in der App die Option „Zugangsdaten speichern“ aktiviert, kann der bei der Anmeldung verwendete Authentifizierungsfaktor eGK bzw. ePA-App durch die Registrierungsdaten ersetzt werden, die beim Identitätsdienst gespeichert und verwaltet werden. Die Registrierungsdaten umfassen (siehe ausführlich 5.5.2.4):

- die Pairing-Daten einschließlich der Signaturdaten,
- den Zeitpunkt der Registrierung,
- den vom Nutzer vergebenen Namen für sein Gerät,
- die idNummer und den übertragenen Key-Identifier.

Die registrierte App speichert lokal das eGK-Authentifizierungszertifikat (C.CH.AUT), die Key-Identifier, und den vom Nutzer vergebenen Namen des Geräts als lokale Registrierungsdaten.

5.11.5 Sucheingaben

Bei der Nutzung der Apothekensuche werden die Sucheingaben des Nutzers verarbeitet. Die Sucheingaben enthalten regelmäßig Standortinformationen (z. B. Straßenname, Postleitzahl, Ort) und/oder Namen von Apotheken.

Wenn der Nutzer der App die Berechtigung für die Nutzung des Ortungsdienstes seines Betriebssystems[56] erteilt, werden die vom Betriebssystem an die App weitergegebenen geographischen Koordinaten des aktuellen Standorts als Sucheingabe verwendet.

5.11.6 Nutzungsdaten

Nutzungsdaten sind standardisierte technische Information, die innerhalb der App durch ihre Nutzung und die konkrete Interaktion des Nutzers mit der App anfallen, beispielsweise das Betätigen von Schaltflächen, die Dauer und den Umfang der Nutzung einer bestimmten App-Funktion oder die Reihenfolge des Aufrufs bestimmter App-Inhalte oder -Funktionen.

5.11.7 Profil- und Konfigurationsdaten

Profildaten sind Angaben des Nutzers bei der Einrichtung eines lokalen Nutzerprofils in der App. Ein Nutzerprofil enthält einen frei wählbaren Namen. Optional kann der Nutzer ein Bild in seinem Profil hinterlegen.

Weitere Konfigurationsdaten enthalten Informationen über die lokalen Einstellungen der App, beispielsweise ob der Nutzer die optionale Nutzungsanalyse oder die Speicherung der Zugangsdaten aktiviert und welche Spracheinstellung er vorgenommen hat.

5.11.8 Fachdaten

Der Begriff der Fachdaten beschreibt als Oberbegriff verschiedene anwendungsspezifische Daten der E-Rezept-App. Sie umfassen in erster Linie das konkrete „eigentliche“ E-Rezept, aber auch weitere mit diesem konkreten E-Rezept zusammenhängende Daten.

5.11.8.1 E-Rezept

Ein „E-Rezept“ ist auf technischer Ebene ein vom Verordnenden mit seiner QES signierter Verordnungsdatensatz.

Der Verordnungsdatensatz wird auf dem Primärsystem des Verordnenden erstellt und enthält den „eigentlichen“ Inhalt des E-Rezepts. Die Inhalte bzw. Datenfelder des Verordnungsdatensatzes werden durch Muster e16A der Anlage 2b zum Bundesmantelvertrag der Ärzte und der zugehörigen „Technischen Anlage zur elektronischen Arzneimittelverordnung“ der KBV definiert und entsprechen inhaltlich dem bisherigen (rosafarbenen) Muster 16. Zusätzlich enthält der Verordnungsdatensatz die Rezept-ID[57] sowie zusätzliche Datenfelder für Mehrfachverordnungen gemäß § 31 Abs. 1b SGB V. Bei einer Einzelverordnung sind diese zusätzlichen Datenfelder leer.

56 Ortungsdienste sind Betriebssystemdienste, die anhand der vom Smartphone empfangenen Funksignale beispielsweise von GSM-Funkzellen, GPS-Satelliten und umliegenden WLAN-Zugangspunkten den Standort des Smartphones ermitteln und für andere Betriebssystemdienste und vom Nutzer freigegebene Drittanbieter-Apps bereitstellen.

57 In den KBV-Spezifikationen wird die Rezept-ID teilweise als Dokumenten-ID bezeichnet.

Diese zusätzlichen Datenfelder müssen nur im Fall einer Mehrfachverordnung Angaben dazu enthalten, dass es sich bei dem jeweiligen E-Rezept um eine Teilverordnung handelt und um die wievielte Teilverordnung einer Mehrfachverordnung es sich handelt (z. B. 1 von 3).[58] Daneben stehen Datenfelder zur Angabe von Beginn und Ende der Einlösefrist zur Verfügung.

5.11.8.2 Rezept-ID

Die Rezept-ID ist ein vom E-Rezept-Fachdienst verwendeter Identifikator zur eindeutigen Zuordnung eines Verordnungsdatensatzes[59], eines Dispensierdatensatzes und einer Quittung zu einem E-Rezept. Die Spezifikationen legen fest, dass die Rezept-ID für die Dauer von mindestens 11 Jahren eindeutig ist.

Der formale Aufbau einer Rezept-ID folgt der Struktur *aaa.bbb.bbb.bbb.bbb.cc*.

Dabei gibt aaa als alphanummerischer Wert den vom Verordnenden festgelegten Rezepttyp (dazu sogleich) und *bbb.bbb.bbb.bbb* die vom E-Rezept-Fachdienst festgelegte laufende Rezeptnummer an. Der Wert cc stellt die vom E-Rezept-Fachdienst per Modulo 97 gemäß ISO 7064 generierte Prüfziffer dar.

Mit dem Rezepttyp wird nicht direkt der verwendeten digitale KBV-Vordruck, sondern der sogenannte Workflow-Typ angegeben. Der Workflow-Typ bestimmt, welche technischen und fachlichen Prozesse und Parameter bei der weiteren Verarbeitung des jeweiligen E-Rezepts einzuhalten sind. Die Angabe des Workflow-Typs lässt eindeutig auf den verwendeten digitalen Vordruck schließen, weil dieser für die Festlegung der einzuhaltenden Workflows maßgeblich ist.

Um besonderen Versorgungsituationen Rechnung zu tragen, können für E-Rezepte auf Basis des gleichen digitalen Vordrucks mehrere Workflow-Typen definiert werden. So kann beispielsweise für E-Rezepte zur Arzneimittelversorgung durch krankenhausversorgende Apotheken und Krankenhausapotheken im Rahmen von § 14 Abs. 7 und 8 Apothekengesetz (ApoG) auf Grundlage des KBV-Vordrucks e16A ein spezifischer Workflow-Typ definiert werden, der ausnahmsweise dem Verordnenden selbst die Einlösung in der Krankenhausapotheke ermöglicht und den E-Rezept-Fachdienst oder die App anweist, dem Versicherten keine Mitteilungen über Statusänderungen in Bezug auf das vom Verordnenden eingelöste E-Rezept anzuzeigen.

5.11.8.3 Task-ID

Beim Erstellen eines E-Rezepts wird auf dem E-Rezept-Fachdienst ein E-Rezept-spezifischer Prozess initiiert (sogenannter Task), der den gesamten Lebenszyklus des E-Rezepts abbildet. Die Task-ID ist der vom E-Rezept-Fachdienst verwendete eindeutige Identifikator für den Task und die diesbezüglichen Einzelprozesse in Bezug auf ein bestimmtes E-Rezept bzw. den Task.

5.11.8.4 Dispensierdatensatz

Bei der Arzneimittelabgabe erstellt die Apotheke einen sogenannten Dispensierdatensatz, mit dem sie das bei Einlösung eines E-Rezepts konkrete abgegebene Arzneimittel im E-Rezept-Fachdienst dokumentiert. Der Dispensierdatensatz enthält die Task-ID und die Rezept-ID sowie optionale Felder zur Dokumentation der Chargennummer. Die Inhalte bzw. Datenfelder des Dispensierdatensatzes werden vom DAV und dem GK-Spitzenverband festgelegt. Der Dispensierdatensatz wird zusammen mit dem E-Rezept und der Quittung für die Abrechnung verwendet.

5.11.8.5 Protokolldaten

Zu jedem E-Rezept wird auf dem E-Rezept-Fachdienst ein Protokolldatensatz geführt. Dieser dokumentiert für den Versicherten alle Zugriffe, Statusänderungen (z. B. Gültigkeits- und Einlösestatus) und die (ggf. automatische) Löschung in Bezug auf ein bestimmtes E-Rezept. Konkret enthalten die Protokolldaten die folgenden Angaben:

- Task-ID,
- Rezept-ID,
- Name/Rolle des Zugreifenden (z. B. Arzt, Zahnarzt, Apotheke, E-Rezept-Fachdienst),
- Zeitpunkt des Zugriffs,
- Art und Ergebnis des Zugriffs (z. B. dass ein E-Rezept bereitgestellt oder gelöscht worden ist) und
- Beschreibung des Vorgangs.

58 Gemäß § 31 Abs. 1b SGB V sind Mehrfachverordnungen „besonders zu kennzeichnen“.

59 Der Verordnungsdatensatz enthält den Inhalt eines E-Rezepts, siehe 5.11.8.1.

Nach den Spezifikationen muss die Beschreibung des Vorgangs durch einen „lesbaren Text in einfacher Sprache (deutsch und englisch)“ erfolgen, der mindestens den Namen des Zugreifenden, den Zweck und das Ergebnis der Operation umfasst, damit Versicherte ohne technisches Vorwissen den Inhalt des Zugriffsprotokolls einfach verstehen können.

5.11.8.6 Rezeptstatus

Jedes E-Rezept durchläuft in seinem Lebenszyklus bis zu fünf spezifizierte Status:

- **initialisiert:** Der Verordnungsdatensatz wurde vom Leistungserbringer angelegt, aber noch nicht signiert.
- **offen:** Nachdem der Leistungserbringer den Verordnungsdatensatz signiert hat (d. h. es handelt sich nun um ein E-Rezept), wechselt der Status auf „offen“.
- **in Abgabe (gesperrt):** Während Zugriffen einer Apotheke auf das E-Rezept und nach erfolgter Einlösung wechselt der Status auf „in Abgabe (gesperrt)“.
- **quittiert:** Bei Initialisierung des Abrechnungsprozesses wechselt der Status auf „quittiert“.
- **gelöscht:** Das E-Rezept wurde vom Versicherten in der App oder von einem zugriffsberechtigten Leistungserbringer auf dem E-Rezept-Fachdienst zur Löschung gekennzeichnet.[60] Eine Löschung ist nur durch den Versicherten selbst möglich.

Der aktuelle Rezeptstatus wird auf dem E-Rezept-Fachdienst Zustand des das E-Rezept repräsentierenden Tasks verwaltet.

5.11.8.7 AccessCode

Der AccessCode ist eine vom E-Rezept-Fachdienst generierte und hexadezimal kodierte 256-Bit-Zufallszahl mit einer Mindestentropie von 120 Bit. Er wird auf dem E-Rezept-Fachdienst beim Anlegen eines Verordnungsdatensatzes erzeugt und mit der Task-ID des E-Rezepts verknüpft. Jede Person außer dem Versicherten, die auf ein E-Rezept auf dem E-Rezept-Fachdienst zugreifen will, muss den AccessCode kennen.

5.11.8.8 Quittung

Die Quittung ist ein durch den E-Rezept-Fachdienst erstellter und signierter Datensatz, welcher der abgebenden Apotheke nach dem Statuswechsel des E-Rezepts auf „quittiert“ zu Abrechnungszwecken bereitgestellt wird. Die Quittung beinhalt das Datum des Statuswechsels auf „quittiert“ und die Rezept-ID.

5.11.8.9 E-Rezept-Token

Der E-Rezept-Token ist eine strukturierte Zeichenkette bestehend aus der Task-ID und dem AccessCode eines E-Rezepts. Um ein E-Rezept einlösen zu können, muss der zugehörige E-Rezept-Token bei der Apotheke vorliegen.

Beispiel eines E-Rezept-Tokens mit der Task-ID 4711 und dem AccessCode *„77bea0e13cc9c42ceec14aec3ddee2263325dc2c6c699db115f58fe423607ea“*: *Task/4711/$accept?ac=777bea0e13cc9c42ceec14aec3ddee2263325dc2c6c699db115f58fe423607ea*

5.11.8.10 Mitteilungen an/von Apotheken

Mitteilungen, die der Versicherte über die App an eine Apotheke sendet oder von diesen empfängt, enthalten jeweils folgende Angaben:

- Absender-ID,
- Empfänger-ID,
- Task-ID des betreffenden E-Rezepts und
- Nachrichteninhalt.

Als Absender-/Empfänger-ID des Versicherten dient seine KVNR und der Apotheke die Telematik-ID der jeweiligen Apotheke.

60 Der Status „gelöscht“ führt dazu, dass das betreffende E-Rezept nicht mehr angezeigt oder zugreifbar wird. Die physische Löschung des betreffenden Datensatzes auf den E-Rezept-Fachdienst erfolgt erst nach Ablauf der im Einzelfall geltenden Löschfrist, siehe hierzu7.4.1.

5.11.9 DataMatrix-Code (Rezeptcode)

Auf dem Rezeptausdruck und in der App wird das E-Rezept-Token als DataMatrix-Code gemäß ISO/IEC 16022:2006 dargestellt. Ein einzelner DataMatrix-Code kann bis zu vier E-Rezept-Token darstellen.

Gegenüber dem Versicherten wird der DataMatrix-Code zur besseren Verständlichkeit untechnischer als „Rezeptcode“ bezeichnet. Entsprechend wird ein DataMatrix-Code, der mehr als ein E-Rezept-Token darstellt, als „Sammel-Rezeptcode“ bezeichnet.

Abbildung 2: Ausdruck mit Rezeptcodes (Quelle: KBV)

5.11.10 Zugriffsdaten

Bei den HTTPS-Requests der App an die Server-Endpunkte des E-Rezept-Fachdienstes, des Identitätsdienstes, des Apotheken-Verzeichnisses sowie ggf. den Nutzungsanalysedienst fallen bei den jeweiligen Betreibern Zugriffsdaten an. Die Zugriffsdaten umfassen:

- IP-Adresse,
- Datum und Uhrzeit des Abrufs (Zeitstempel),
- Übertragene Datenmenge (bzw. Paketlänge) und
- Meldung, ob der Abruf erfolgreich war.

Die Zugriffsdaten fallen auch bei dem Telekommunikationsunternehmen an, welches den Internetzugang des Nutzers bereitstellt.[61]

5.11.11 Analysedaten

Die Kategorie der Analysedaten wird im Verwendungskontext der (optionalen) Nutzungsanalyse als Oberbegriff für die verarbeiteten Geräte-[62] und Nutzungsdaten[63] verwendet.

61 Verkehrsdaten im Sinne von § 3 Nr. 70 Telekommunikationsgesetz (TKG).

62 Siehe 5.11.3.

63 Siehe 5.11.6.

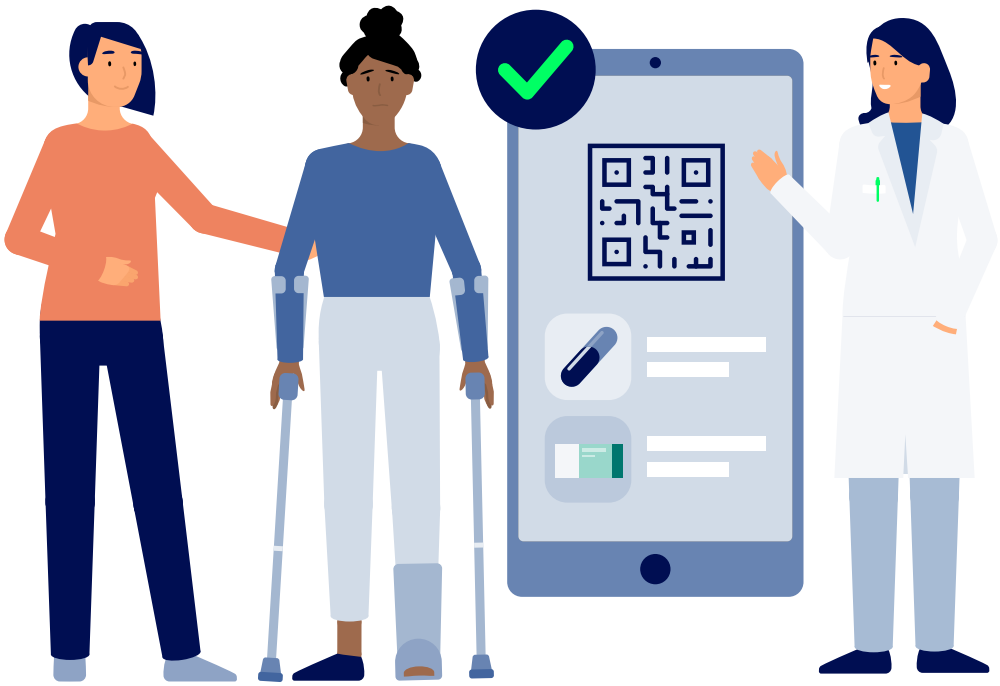
6 Einholung des Standpunktes der betroffenen Personen

Gemäß Art. 35 Abs. 9 DSGVO kann der Verantwortliche die Standpunkte der betroffenen Personen einholen, um deren Sichtweisen in Erfahrung zu bringen und somit möglicher Kritik frühzeitig zu begegnen und dadurch die Akzeptanz des in Rede stehenden Verfahrens zu fördern.

Da die betroffenen Personen alle Nutzer sind und daher ein sehr breites Spektrum der Bevölkerung umfassen, wurden und werden die Standpunkte der betroffenen Personen durch die Auswertung verschiedener Quellen eingeholt:

- Individuelles und öffentliches Feedback aus der Entwicklercommunity auf die Veröffentlichung von Quellcodes und Dokumenten (Datenschutzkonzepte usw.) auf der GitHub-Projektseite,
- Medienberichterstattung über die E-Rezept-App,
- Fachveröffentlichungen,
- Stellungnahmen von Datenschutzbehörden und Datenschutzgremien (z. B. EDPB) und
- Stellungnahmen von Verbänden und Interessensgruppen.

Den geäußerten Standpunkten wurde bei der Entwicklung der E-Rezept-App, soweit aus Sicht der Verantwortlichen zweckmäßig und möglich, Rechnung getragen.



7 Rechtsgrundlagen und Verantwortliche

Grundbedingung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten ist die Zulässigkeit der Verarbeitung. Die Zulässigkeit setzt voraus, dass der jeweilige Verantwortliche die gesamte von ihm verantwortete personenbezogene Verarbeitung grundsätzlich auf eine ausreichende Rechtsgrundlage gemäß Art. 6 Abs. 1 DSGVO stützen kann. Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss zusätzlich eine Rechtsgrundlage gemäß Art. 9 Abs. 2 DSGVO vorhanden sein.

Zur Identifikation und Bewertung der in Betracht kommenden Rechtsgrundlagen ist daher zunächst zu ermitteln, welche verarbeiteten Daten bzw. Datenkategorien im Rahmen des Prüfgegenstands einen Personenbezug aufweisen, von welchen Akteuren sie zu welchen Zwecken verarbeitet werden und wer jeweils als Verantwortlicher für diese Verarbeitungen anzusehen ist.

Soweit die Zulässigkeit der Verarbeitung personenbezogener Daten durch den verantwortlichen Akteur bejaht werden kann, d. h. wenn eine ausreichende Rechtsgrundlage zur Verfügung steht, sind im nächsten Schritt die weiteren Rechtsmäßigkeitsanforderungen an die betreffende Verarbeitung zu ermitteln und deren Einhaltung durch den oder die Verantwortlichen zu bewerten.

7.1 Verarbeitung personenbezogener Daten

In Art. 4 Nr. 1 DSGVO werden personenbezogenen Daten definiert als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Online-Kennung, einer Kennnummer, zu Standortdaten oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann. Direkt identifizierbar ist eine Person insbesondere durch ihren Namen und andere mit dem Namen verbundenen Informationen. Indirekt identifizierbar ist eine Person durch alle Daten, die ein Wiedererkennen ermöglichen, auch wenn die Daten auf Anhieb keinen Schluss auf eine bestimmte Person erlauben.[64] Dabei erkennt die DSGVO ausdrücklich an, dass Personen aufgrund der technologischen Entwicklungen zunehmend auch über „Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen [...] insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen“ identifizierbar werden können.[65]

Bei der Beurteilung, ob eine Person identifizierbar ist, sind alle Mittel zu berücksichtigen, die vernünftigerweise entweder von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden könnten, um die betreffende Person direkt oder indirekt zu identifizieren. Dies erfordert eine Berücksichtigung aller objektiven Faktoren, etwa den für eine Identifizierung notwendigen wirtschaftlichen und zeitlichen Aufwand.[66]

7.1.1 Bewertung des Personenbezugs der verarbeiteten Datenarten

Nachfolgend wird der Personenbezug der im Rahmen des Prüfgegenstands verarbeiteten Datenarten bewertet.

Da die Frage des Personenbezugs – ebenso wie die anschließende Frage der Verantwortlichkeit – im konkreten Verarbeitungskontext und insbesondere im Licht der an dem Verarbeitungsvorgang jeweils beteiligten Akteure beurteilt werden muss,[67] erfolgt die Darstellung aus Gründen der Übersichtlichkeit differenziert nach dem Ort der Verarbeitung. Hierzu wird begrifflich zum einen zwischen lokalen und andererseits nicht-lokalen Verarbeitungsvorgängen unterschieden. Lokale Verarbeitungsvorgänge sind solche, die innerhalb des von der E-Rezept-App kontrollierten Speicher- und Funktionsbereich auf dem Smartphone ablaufen. Zu den lokalen Verarbeitungsvorgängen zählen auch Zugriffe der E-Rezept-App auf lokale Schnittstellen und Dienste des Betriebssystems. Unter nicht-lokalen (Remote-)Verarbeitungsvorgängen werden demgegenüber Verarbeitungsvorgänge verstanden, die einen Zugriff auf einen Endpunkt im Internet beinhalten („online“). Im Fall der E-Rezept-App betreffen die Remote-Verarbeitungsvorgänge vor allem die Zugriffe auf den Apotheken-Verzeichnisdienst, den E-Rezept-Fachdienst, den Identitätsdienst, den Verzeichnisdienst und den Analysedienst.

64 Wolff/Brink/Schild, Beck OK Datenschutz, 41. Ed. (Stand: 01.08.22), Art. 4 Rn. 16, 17.

65 EG 30 DSGVO.

66 EG 26 DSGVO.

67 Siehe EG 26 S. 3 DSGVO: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.“; vgl. auch Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, 20. Juni 2007, WP 136, S. 15 ff, in deutscher Übersetzung abrufbar unter: https://www.lda.bayern.de/media/wp136_de.pdf (abgerufen am 15.12.2022).

7.1.1.1 Lokale Verarbeitung durch die App

Es wird angenommen, dass alle lokal von der App auf dem Smartphone des Nutzers verarbeiteten Datenarten grundsätzlich einen direkten Personenbezug aufweisen, da sie von jeder Person, die Zugang zu dem (entsperrten) Smartphone hat, anhand der auf einem Smartphone typischerweise gespeicherten Daten ohne weiteres der Person des Nutzers zugeordnet werden können. Die betroffene Person ist daher in erster Linie der Nutzer. Soweit der Nutzer die App zur Verwaltung eigener E-Rezepte verwendet, ist er nicht nur in der Rolle eines Nutzers, sondern auch in der Rolle eines Versicherten von der lokalen Verarbeitung durch die App betroffen. Sofern der Nutzer die App zur Verwaltung von E-Rezepten von Dritten verwendet, zählen auch diese in ihren Rollen als Versicherte zu den von der Verarbeitung betroffenen Personen.

Besondere Kategorien personenbezogener Daten:

Bei den lokal von der App verarbeiteten Fachdaten (z. B. gespeicherte E-Rezepte) sowie den in der App gespeicherten Rezeptcodes handelt es sich um Gesundheitsdaten des betroffenen Versicherten.

Biometrische Daten des Nutzers werden von der App nicht verarbeitet. Wenn der Nutzer zur lokalen Authentifizierung die biometrischen Authentifizierungsverfahren seines Betriebssystems nutzt (z. B. Face ID oder „Entsperren per Fingerabdruck"), werden auf dem Smartphone durch den zuständigen lokalen Betriebssystemdienst zwar biometrische Gesichts- oder Fingerabdruckdaten verarbeitet. Diese Verarbeitung findet jedoch durch das Betriebssystem statt. Die App erhält von dem Betriebssystem über eine lokale Schnittstelle lediglich das Authentifizierungsergebnis des durchgeführten biometrischen Authentifizierungsverfahrens in Form der sinngemäßen Angabe „Erfolgreich" oder „Fehlgeschlagen". Dieses Authentifizierungsergebnis enthält keine für die Einstufung als biometrische Daten vorausgesetzten Angaben zu physischen, physiologischen oder verhaltenstypischen Merkmalen des Nutzers.

7.1.1.2 Verarbeitung durch Betriebssystemdienste

Durch Schnittstellenzugriffe der App auf Betriebssystemdienste werden lokale Verarbeitungsvorgänge durch das Betriebssystem ausgelöst, um der App die im Einzelfall angeforderten Informationen (z. B. Standortdaten, Attestationsergebnisse oder gescannte Rezeptcodes) bereitzustellen. In einigen Fällen greifen die Betriebssystemdienste für die Bereitstellung ihrer Dienste über das Internet auf Server-Endpunkte von Backend-Systemen des jeweiligen Anbieters zurück. Für die durch die Betriebssystemdienste lokal oder remote verarbeiteten Nutzungsdaten ist grundsätzlich von einem Personenbezug zum Nutzer auszugehen.

Hinsichtlich der nur lokal verarbeiteten Nutzungsdaten folgt der Personenbezug jedenfalls aus den in Ziffer 7.1.1.1 bereits genannten Gründen.

Da die Installation der App und teilweise auch die Nutzung der Betriebssystemdienste regelmäßig[68] die Anmeldung im (Online-)Benutzerkonto bei dem jeweiligen App-Store-Anbieter erfordert, der zugleich auch als Anbieter der Betriebssystemdienste auftritt oder mit diesem konzernverbunden ist, ist davon auszugehen, dass der Anbieter auf technischer Ebene leicht eine Zuordnung der anfallenden Nutzungsdaten zu dem Benutzerkonto vornehmen kann, beispielsweise durch eine Analyse der vorhandenen Datensammlungen oder eine Modifikation der Betriebssystemdienste. Dabei ist zu berücksichtigen, dass die Anbieter von ihren technischen Möglichkeiten, große Mengen an personenbezogenen Daten über die Nutzer ihrer Betriebssysteme, Betriebssystemdienste und Onlinedienste zu erheben, erfahrungsgemäß umfassend Gebrauch machen, um neben fremdnützigen auch eigennützige Zwecke (z. B. Nutzungsanalysen auf der Basis von betriebssystemseitig erfassten Analysedaten) zu verfolgen. Auf Seiten des Anbieters ist daher in Bezug auf die durch Betriebssystemdienste verarbeiteten Nutzungsdaten von einer direkten Identifikationsmöglichkeit des Nutzers bzw. Inhabers des vom Nutzer verwendeten Benutzerkontos auszugehen.

Soweit die von der App verwendeten Betriebssystemdienste eine Remote-Verarbeitung im Backend des Anbieters umfassen, fallen bei dem Anbieter auch serverseitig zudem Zugriffsdaten über den jeweiligen Vorgang an. Die von einem Internet-Server verarbeiteten Zugriffsdaten umfassen technisch bedingt die IP-Adresse des zugreifenden Nutzers. Sofern es sich um eine statische IP-Adresse handelt, kann der Anbie-

68 Nutzer, die ein „alternatives" Android-Betriebssystem ohne Bindung an Google verwenden und/oder die Nutzung des Google Play Stores ablehnen, können die Android-Version der E-Rezept-App aus dem GitHub-Repository der gematik laden und auf ihrem Gerät installieren.

ter bzw. Betreiber des Servers die IP-Adresse anderen Zugriffen, bei denen die gleiche IP-Adresse genutzt wird, zuordnen. Bei den für mobile und private Internetzugänge üblichen dynamischen IP-Adressen verfügt prinzipiell nur der Internetzugangsanbieter des Nutzers über entsprechende Log-Dateien und Zuordnungsinformationen, die erkennen lassen, welchem Nutzer er zu welcher Zeit welche IP-Adresse zugeordnet hat. Wie der Europäische Gerichtshof (EuGH) festgestellt hat, ist die dynamische IP-Adresse daher für den Internetzugangsanbieter ein personenbezogenes Datum[69]. Später hat der EuGH klargestellt, dass ein Personenbezug auch für einen Online-Anbieter vorliegt, soweit ihm rechtliche Mittel zur Verfügung stehen, Daten, die eine Identifikation ermöglichen, vom Internetzugangsanbieter zu erhalten.[70]

Solange der Betreiber des Servers daher die IP-Adresse des Nutzers verarbeitet oder in der üblichen, mit Zeitstempeln versehenen Protokollierung in den Server-Logfiles speichert, ist der Personenbezug der Zugriffsdaten zu bejahen. Dabei ist zu berücksichtigen, dass die mobilen Betriebssysteme üblicherweise so konzipiert sind, dass zentrale Betriebssystemdienste und -funktionen nur mit einer dauerhaften Internetverbindung und Anmeldung im Online-Benutzerkonto des Anbieters zur Verfügung stehen. Insofern muss von einer dauerhaften Personenbezogenheit der Zugriffsdaten und somit auch von der damit durch den Anbieter verknüpften bzw. verknüpfbaren lokal und remote gespeicherten Nutzungsdaten des Nutzers bzw. des Kontoinhabers ausgegangen werden.[71]

Bei der Nutzung der vom Betriebssystem zur Verfügung gestellten Kamerafunktion zum Scannen von Rezeptcodes wird das Kamerabild während der Aufnahme und Weiterleitung an die App durch den für die Kamera zuständigen Betriebssystemdienst kurzzeitig lokal verarbeitet. Eine anschließende Speicherung oder Übermittlung des Rezeptcodes an einen Server-Endpunkt durch einen Betriebssystemdienst erfolgt nicht. Da der betroffene Inhaber des von der Kamera erfassten und auf dem Bildschirm wiedergegebenen Rezeptcodes dem Nutzer sowie etwaigen umstehenden Personen regelmäßig persönlich bekannt oder von diesem identifizierbar ist, insbesondere anhand der auf dem Rezeptausdruck enthaltenen Versichertendaten, ist von einem Personenbezug zum Versicherten auszugehen.

Im Fall des Android- und des EMUI-Betriebssystems wird das Kamerabild auch durch den Barcodescanner-Betriebssystemdienst (Google ML Kit/Huawei ML Kit) analysiert. Google behält sich in den vom Nutzer zu bestätigenden Nutzungsbedingungen und Datenschutzhinweisen vor, die dabei anfallenden Nutzungsdaten („Angaben zur Gerätenutzung“) auszuwerten, so dass hinsichtlich der ML-Kit-spezifischen lokalen Nutzungsdaten aus den bereits genannten Gründen von einem Personenbezug zum Nutzer bzw. Kontoinhaber auszugehen ist. Die inhaltliche Verarbeitung des Rezeptcodes, d. h. das Auslesen des Rezeptcodes aus dem Kamerabild und die Weitergabe an die App, erfolgt jedoch ebenso wie im Fall der iOS-Version der App lokal und ohne Speicherung des Rezeptcodes im vom Betriebssystem verwalteten Speicher. Personenbezogene Daten in Gestalt des Rezeptcodes werden daher auch durch die Betriebssystemdienste des Android-Betriebssystems nur für die Dauer des Scanvorgangs verarbeitet.

Besondere Kategorien personenbezogener Daten:

Bei den Rezeptcodes, die durch die für die Kamera zuständigen Betriebssystemdienste flüchtig lokal erfasst und direkt auf dem Bildschirm angezeigt werden, handelt es sich um Gesundheitsdaten des jeweiligen Versicherten.

Wenn der Nutzer zur lokalen Authentifizierung in der App die biometrischen Authentifizierungsverfahren des Betriebssystems nutzt (z. B. Face ID oder „Entsperren per Fingerabdruck“), werden auf dem Smartphone durch den zuständigen Betriebssystemdienst bereits gespeicherte sowie für den konkreten Authentifizierungsvorgang erhobene Gesichts- oder Fingerabdruckinformationen verarbeitet. Diese Informationen stellen biometrische Daten dar. Biometrische Daten werden in Art. 4 Nr. 14 DSGVO definiert als „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die eine eindeutige Identifizierung dieser ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten“. Diese Kriterien werden von den Gesichts- und Fingerabdruckinformationen, die von den von der App akzeptierten biometrischen Authentifizierungsverfahren verwendet werden, erfüllt. So werden bei der Verwendung von Gesichtsbildern als Authentifizierungsfaktor spezielle

69 EuGH, Urt. v. 19.10.2016, Rs. Breyer, C-582/14.

70 EuGH, Beschl. v. 6.12.2016, Rs. C-582/14.

71 Vgl. z. B. in der Google-Datenschutzerklärung: „Zu den von uns erhobenen Daten zählen eindeutige Kennungen, der Typ und die Einstellungen des Browsers, der Typ und die Einstellungen des Geräts, das Betriebssystem, Informationen zum Mobilfunknetz wie der Name des Mobilfunkanbieters und die Telefonnummer sowie die Versionsnummer der App. Wir erheben auch Daten über die Interaktion Ihrer Apps, Browser und Geräte mit unseren Diensten. Hierzu zählen u. a. die IP-Adresse, Absturzberichte, Systemaktivitäten sowie das Datum, die Uhrzeit und die Verweis-URL Ihrer Anfrage.“

biometrische Informationen genutzt, die zuvor durch ein mathematisches Verfahren aus mit 3D- oder Infrarotkameras erzeugten Gesichtsaufnahmen abgeleitet und als vom Betriebssystem als Referenzdaten auf dem Smartphone in der Secure Enclave gespeichert werden. Bei der Verwendung von Fingerabdruckinformationen werden die biometrischen Referenzdaten aus Aufnahmen der Fingerkuppe abgeleitet, die zuvor durch hochauflösende optische oder kapazitive Sensoren des Smartphones erzeugt werden. Bei jedem anschließenden Authentifizierungsvorgang werden auf die gleiche Weise erneut biometrische Gesichts- bzw. Fingerabdruckdaten erhoben und mit den biometrischen Referenzdaten abgeglichen.

Da die Anbieter von Betriebssystemdiensten mit einer Serverkomponente auch die Betreiber des App Stores sind, ist ihnen die Nutzung der App durch den Nutzer bereits bekannt. Allein die Kenntnis von der Installation der App lässt keine Rückschlüsse auf den Gesundheitszustand des betreffenden Nutzers zu. Anhand der Zugriffe der von der App genutzten Betriebssystemdienste auf Server-Endpunkte des jeweiligen Anbieters erfassten Nutzungs- und Zugriffsdaten könnte der Anbieter jedoch Rückschlüsse auf die Häufigkeit und den Umfang der App-Nutzung durch den Nutzer und dadurch mittelbar auf dessen allgemeinen Gesundheitszustand schließen (beispielsweise wenn Google oder Huawei als Anbieter des ML Kit durch das Tracking von Nutzungsdaten des Android- bzw. EMUI-Betriebssystems erfährt, dass der Nutzer mit der App regelmäßig zahlreiche Rezeptcodes einscannt).

Sofern der Nutzer seine Zugangsdaten lokal speichert und hierzu die betriebssystemseitigen biometrischen Authentifizierungsverfahren (z. B. Face ID oder „Entsperren per Fingerabdruck“) für die lokale Authentifizierung wählt, verarbeitet das Betriebssystem nach hier vertretener Auffassung biometrische Daten des Nutzers.

7.1.1.3 Verarbeitungsvorgänge des Apotheken-Verzeichnisdienstes

Bei bestimmungsgemäßer Verwendung der Apothekensuche stellen die jeweiligen Sucheingaben grundsätzlich keine personenbezogenen Daten des Nutzers bzw. des Versicherten dar. Lediglich bei den im Rahmen der Apothekensuche und -bestimmung fakultativ übermittelten Standortdaten handelt es um personenbezogene Daten des Nutzers.

Soweit sich aus den im Apotheken-Verzeichnisdienst eingetragenen Apothekendaten auf die Identität des Inhabers oder eines Mitarbeiters der betreffenden Apotheke schließen lässt (z. B. Apothekenname, E-Mail-Adresse), kann es sich ebenfalls um ein personenbezogenes Datum des betreffenden Apothekers handeln.

Die Zugriffsdaten, die bei den Suchanfragen der App auf dem Server des Apotheken-Verzeichnisdienst anfallen, enthalten die IP-Adressen der Nutzer und werden daher als personenbezogene Daten der Nutzer angesehen.

7.1.1.4 Verarbeitungsvorgänge des E-Rezept-Fachdienstes

Auch bei den Fach- und Zugriffsdaten auf dem E-Rezept-Fachdienst handelt es sich um personenbezogene Daten. Der Umstand, dass diese Daten für den Anbieter des E-Rezept-Fachdienst nicht einsehbar sind, ändert nichts an ihrem Personenbezug.

Bei Zugriffsdaten mit IP-Adressen handelt es sich für Anbieter von Online-Diensten regelmäßig um personenbezogene Daten, wenn sie über rechtliche Mittel verfügen, die es ihnen erlauben, ggf. auch mit Hilfe der zuständigen Behörde und dem Internetzugangsanbieter, die betreffende Person anhand der gespeicherten IP-Adressen bestimmen zu lassen. Da die IP-Adresse durch den Anbieter des E-Rezept-Fachdienst nur für die Dauer des Zugriffsvorgangs gespeichert und anschließend gelöscht wird, besteht der Personenbezug jedoch regelmäßig nur für wenige Minuten.

7.1.1.5 Verarbeitungsvorgänge des Identitätsdienstes

Bei den Zugriffs-, Authentifizierungs- und Registrierungsdaten, die im Identitätsdienst verarbeitet werden, handelt es sich um personenbezogene Daten. Allerdings wird das Authentifizierungszertifikat des Versicherten nur flüchtig verarbeitet, d. h. nicht dauerhaft gespeichert (vgl. Ziffer 5.5.2.2).

Da die IP-Adresse durch den Anbieter des E-Rezept-Fachdienst nur für die Dauer des Zugriffsvorgangs gespeichert und anschließend gelöscht wird, wird die Dauer des Personenbezugs der vom Identitätsdienst verarbeiteten Authentifizierungs- und Registrierungsdaten durch ihre Verbindung mit den Zugriffsdaten bei der Übermittlung nicht verlängert.

Die Authentifizierungsdaten werden gelöscht, sobald sich der Nutzer vom E-Rezept-Fachdienst abmeldet, so dass der unmittelbare Personenbezug dieser Daten nur für die Dauer der Anmeldung besteht.

Falls der Nutzer ein alternatives Authentifizierungsmittel registriert, werden die hierfür vom Identitätsdient gespeicherten Registrierungsdaten (vgl. Ziffer 5.5.2.4) gelöscht, sobald das alternative Authentifizierungsmittel de-registriert wird. Somit entfällt der Personenbezug der Registrierungsdaten mit der De-Registrierung.

7.1.1.6 Verarbeitungsvorgänge der Nutzungsanalyse

Die im Rahmen der Nutzungsanalyse verarbeiteten Analysedaten umfassen allgemeine Geräte- und Nutzungsdaten, die als solche keinen Personenbezug haben. Durch die kurzfristige Verbindung der Analysedaten mit der Session-ID und der IP-Adresse am Load Balancer entsteht jedoch ein kurzzeitiger Personenbezug.

Die Session-ID ermöglicht unmittelbar keinen Rückschluss auf den betreffenden Nutzer. Sie kann ausschließlich mit Zusatzkenntnissen, nämlich der auf dem Smartphone lokal gespeicherten Kopie der Session-ID oder IP-Adresse dem betreffenden Nutzer zugeordnet werden. Insoweit stellt die Session-ID ein (personenbezogenes) Pseudonym des Nutzers dar. Allerdings hat es allein der Nutzer in der Hand, die Identität seiner Session-ID gegenüber der gematik oder Dritten preiszugeben. Für die gematik oder den Dienstleister hat die an den Load Balancer übermittelte Session-ID als solche daher grundsätzlich keinen Personenbezug; einen solchen kann die gematik nur durch die Verknüpfung mit weiteren Informationen wie der auf dem Smartphone gespeicherten Session-ID oder der IP-Adresse des Nutzers herstellen.

Die vom Load Balancer verarbeitete IP-Adresse ist grundsätzlich als personenbezogenes Datum anzusehen. Bei den von den meisten Nutzern verwendeten dynamischen IP-Adressen verfügt prinzipiell nur der Internetzugangsanbieter des Nutzers über entsprechende Log-Dateien und Zuordnungsinformationen, die erkennen lassen, welchem Nutzer er zu welcher Zeit welche IP-Adresse zugeordnet hat. Wie der EuGH festgestellt hat, ist die dynamische IP-Adresse daher für den Internetzugangsanbieter ein personenbezogenes Datum.[72] Später hat der EuGH klargestellt, dass ein Personenbezug auch für einen Online-Anbieter vorliegt, soweit ihm rechtliche Mittel zustehen, Daten, die eine Identifikation ermöglichen, vom Internetzugangsanbieter zu erhalten.[73] Da der Load Balancer keine Protokollierung der IP-Adressen vornimmt und diese unmittelbar nach dem einzelnen Übermittlungsvorgang löscht, handelt es sich um eine zustandslose Verarbeitung der IP-Adresse. Nach Beendigung des Übermittlungsvorgangs kann anhand der vom Load Balancer gespeicherten Daten somit nicht mehr festgestellt werden, welche Daten zu welcher Zeit mit welcher (dynamischen oder statischen) IP-Adresse übermittelt worden sind. Eine Zuordnung der vom Load Balancer verarbeiteten IP-Adresse unter Verwendung der bei dem Internetzugangsanbieter gespeicherten Log-Dateien und sonstigen Nutzerdaten ist folglich ausgeschlossen.

Der Personenbezug der durch den Analysedienstleister verarbeiteten Daten hängt damit von der Dauer des Personenbezugs der Session-ID und der IP-Adresse ab. Entfällt der Personenbezug sowohl der Session-ID als auch der IP-Adresse oder werden diese Daten gelöscht oder anonymisiert, entfällt auch der Personenbezug der mit diesen Kennungen verknüpften allgemeinen Geräte- und Nutzungsdaten.

Hinsichtlich der durch den Analysedienst verarbeiteten Session-ID wird angenommen, dass der Personenbezug spätestens mit dem Löschen oder anderweitigem Wegfall der auf dem Smartphone des betroffenen Nutzers lokal gespeicherten Kopie wegfällt. Ab diesem Zeitpunkt steht weder dem Analysedienstleister noch Dritten eine Zuordnungsregel für die bei dem Analysedienst gespeicherte Session-ID mehr zur Verfügung. Dieser Fall tritt regelmäßig in den folgenden Situationen durch die automatische Löschung der lokal gespeicherten Kopie der Session-ID ein:

72 EuGH, Urt. v. 19.10.2016, Rs. Breyer, C-582/14.

73 EuGH, Beschl. v. 6.12.2016, Rs. C-582/14.

› Die Session des Nutzers ist beendet,

› der Nutzer deinstalliert die App oder

› der Nutzer deaktiviert die Nutzungsanalyse in den App-Einstellungen.

Der Personenbezug der durch den Load Balancer verarbeiteten IP-Adresse entfällt mangels dauerhafter Speicherung (etwa in Server-Logfiles) regelmäßig bereits unmittelbar nach Beendigung des jeweiligen Übermittlungsvorgangs, da sie sofort spurenlos aus dem Arbeitsspeicher des Load Balancer gelöscht wird.

Sofern im Laufe einer Session verschiedene IP-Adressen für mehrere Übermittlungsvorgänge unter der gleichen Session-ID an den Load Balancer verwendet werden, besteht allerdings die Möglichkeit, die früher übermittelten Session-Daten über die darin enthaltene Session-ID den später übermittelten Session-Daten mit der gleichen Session-ID zuzuordnen. Während der Bearbeitung des späteren Übermittlungsvorgangs, d. h. solange die aktuelle IP-Adresse dem Load Balancer bekannt ist, kann diese daher auch den früher übermittelten Session-Daten zugeordnet werden, obwohl die früher verwendete (gleiche oder andere) IP-Adresse dem Load Balancer nicht mehr bekannt ist.

Im Hinblick auf die Bewertung des Personenbezuges der durch den Analysedienstleister für die Nutzungsanalyse verarbeiteten Daten ist damit festzustellen, dass es sich für die Dauer der jeweiligen Session um personenbezogene Daten handelt. Spätestens mit dem Ende der jeweiligen Session können die unter der zugehörigen Session-ID bei dem Analysedienstleister gespeicherten Daten als anonymisiert angesehen werden.

7.2 Datenschutzrechtliche Verantwortlichkeiten

Die DSGVO weist unterschiedlichen natürlichen oder juristischen Personen, die an einer Datenverarbeitung beteiligt oder von einer Datenverarbeitung betroffen sind, verschiedene Rollen zu. Diese Rollen sind zum einen als funktionelle Konzepte zu verstehen. Sie zielen darauf ab, Verantwortlichkeiten in Bezug auf einen konkreten Verarbeitungsvorgang zuzuweisen. Zum anderen handelt es sich bei den Rollen um (europarechtliche) Konzepte sui generis. Das heißt, dass für die Auslegung der Rollenbegriffe im nationalen Recht – beispielsweise in § 307 SGB V – vorrangig die Wertungen der DSGVO maßgeblich sind.[74]

Die von der DSGVO vorgesehenen Rollen sind zum Teil exklusiv und zum Teil mit bestimmten normativen Vorgaben verknüpft. So muss der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO beispielsweise geeignete TOM umsetzen, um sicherzustellen, dass eine Verarbeitung, für die er die Verantwortung trägt, ordnungsgemäß erfolgt. Gleichzeitig kann, wer von einer Datenverarbeitung betroffen ist, für diese Verarbeitung selbst nicht verantwortlich sein.

Um die datenschutzrechtlichen Anforderungen an die Rechtmäßigkeit der einzelnen Verarbeitungstätigkeiten näher bestimmen zu können, wird das Rollenkonzept der DSGVO zunächst abstrakt beschrieben. Anschließend werden die gesetzlichen Vorgaben zur Bestimmung des Verantwortlichen eingeführt. In einem dritten Schritt wird dann der jeweils Verantwortliche für die einzelnen Verarbeitungskomplexe bestimmt, bevor die Rechtsgrundlage der Datenverarbeitung in einem vierten und letzten Schritt mit Blick auf den konkreten Verantwortlichen für eine bestimmte Verarbeitungstätigkeit diskutiert wird.

74 Vgl. EDPB, Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Version 2.0, S. 3 und 12, abrufbar unter: https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_de.pdf (zuletzt abgerufen am 15.12.2022).

7.2.1 Rollenkonzept der DSGVO

Die DSGVO spricht im Zusammenhang mit einem bestimmten Verarbeitungsvorgang alternativ von betroffenen Personen (Art. 4 Nr. 1 DSGVO)[75], Verantwortlichen (Art. 4 Nr. 7 DSGVO) und Auftragsverarbeitern (Art. 4 Nr. 8 DSGVO).[76]

Die Rolle des Verantwortlichen wird dabei besonders hervorgehoben. Er muss dafür Sorge tragen, dass die Vorschriften der DSGVO jederzeit eingehalten werden und nachweisen, dass personenbezogene Daten in seinem Verantwortungsbereich im Einklang mit den Bestimmungen der DSGVO verarbeitet werden. Er ist vorrangiger Adressat der Pflichten aus der DSGVO. Zu seinen zentralen Pflichten gehören die Gewährleistung der Datenschutzgrundsätze (Art. 5ff. DSGVO), der Betroffenenrechte (Art. 12ff. DSGVO) sowie von TOM, die sicherstellen, dass jegliche Verarbeitung im Einklang mit den anwendbaren Datenschutzvorschriften erfolgt (Art. 24f. DSGVO).

Auftragsverarbeiter ist demgegenüber jede Stelle, die personenbezogene Daten verarbeitet ohne Verantwortliche oder betroffene Person zu sein. Zu den Pflichten des Auftragsverarbeiters gehören insbesondere die Führung eines Verzeichnisses von Verarbeitungstätigkeiten (VVT), Art. 30 Abs. 2, und die Kooperation mit den Aufsichtsbehörden Art. 31 DSGVO.

7.2.2 Rechtsgrundlagen zur Bestimmung des Verantwortlichen

In Art. 4 Nr. 7 HS. 1 DSGVO ist die Rolle des Verantwortlichen legaldefiniert. Danach ist Verantwortlicher zunächst jede „natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

Allerdings ergibt sich aus der Formulierung des Art. 4 Nr. 7 HS. 2 DSGVO im Umkehrschluss, dass der Gesetzgeber die Zwecke und Mittel einer Verarbeitung im Rahmen seiner Gesetzgebungskompetenzen vorgeben kann:

„sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden“.

Macht der Gesetzgeber von dieser Öffnungsklausel Gebrauch, so besteht keine Entscheidungshoheit mehr bei der Stelle, die die Verarbeitung ausführt (und damit keine Verantwortlichkeit im Sinne des Art. 4 Nr. 7 DSGVO).

Im Fall der E-Rezept-App geht der Gesetzgeber davon aus, dass er mit den „gesetzlichen Vorgaben zur Struktur der Telematikinfrastruktur, den zweckgebundenen Anwendungen, Diensten und Komponenten sowie der Ermächtigung der Gesellschaft für Telematik zur Vorgabe von Spezifikationen für einzig zulässige Dienste und Komponenten [...] Zwecke und Mittel der Verarbeitung personenbezogener Daten vorgegeben“ hat. Ausweislich der Gesetzesbegründung hat er in § 307 SGB V eine „Klarstellung der Rolle der Beteiligten in den verschiedenen arbeitsteiligen Datenverarbeitungsprozessen der Telematikinfrastruktur [...] eine konkrete datenschutzrechtliche Verantwortlichkeitszuweisung im Sinne einer spezifizierenden Regelung nach Artikel 4 Nummer 7 Halbsatz 2 DSGVO auf Basis der in § 306 Absatz 2 [SGB V] normierten Mittel vorgenommen“.[77]

75 Die Rolle der betroffenen Personen wird oben unter 4.6.15 näher beschrieben.

76 Weitere in der DSGVO definierte Rollen sind der „Empfänger“ (Art. 4 Nr. 9 DSGVO) und der „Dritte“ (Art. 4 Nr. 10 DSGVO). Empfänger und Dritte sind Personen oder Stellen, denen im Rahmen eines bestimmten Verarbeitungsvorgangs durch einen Verantwortlichen (bzw. Auftragsverarbeiter) personenbezogene Daten offengelegt werden. Verarbeitet der Empfänger die erhaltenen Daten im anschließenden Verarbeitungsvorgang zu eigenen Zwecken, hat er im ersten Verarbeitungsvorgang die Rolle eines Dritten. Im anschließenden Verarbeitungsvorgang zu eigenen Zwecken ist der Dritte ein Verantwortlicher, vgl. EDPB, Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, S. 33 ff. Diese weiteren Rollen der DSGVO sind im Rahmen der hier untersuchten Verarbeitungsvorgänge nicht in erster Linie relevant, bilden aber den Kontext der Ausführungen zu Betroffenen, Verantwortlichen und Auftragsverarbeitern.

77 BT-Drs. 19/18793, S. 100f.

Die entsprechende Vorschrift lautet:

§ 307 Datenschutzrechtliche Verantwortlichkeiten

(1) Die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur nach § 306 Absatz 2 Nummer 1 liegt in der Verantwortung derjenigen, die diese Komponenten für die Zwecke der Authentifizierung und elektronischen Signatur sowie zur Verschlüsselung, Entschlüsselung und sicheren Verarbeitung von Daten in der zentralen Infrastruktur nutzen, soweit sie über die Mittel der Datenverarbeitung mitentscheiden. Die Verantwortlichkeit nach Satz 1 erstreckt sich insbesondere auf die ordnungsgemäße Inbetriebnahme, Wartung und Verwendung der Komponenten. Für die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur nach § 306 Absatz 2 Nummer 1 durch Verantwortliche nach Satz 1 erfolgt in der Anlage zu diesem Gesetz eine Datenschutz-Folgenabschätzung nach Artikel 35 Absatz 10 der Verordnung (EU) 2016/679. Soweit eine Datenschutz-Folgenabschätzung nach Satz 3 erfolgt, gilt für die Verantwortlichen nach Satz 1 Artikel 35 Absatz 1 bis 7 der Verordnung (EU) 2016/679 sowie § 38 Absatz 1 Satz 2 des Bundesdatenschutzgesetzes nicht.

(2) Der Betrieb der durch die Gesellschaft für Telematik spezifizierten und zugelassenen Zugangsdienste nach § 306 Absatz 2 Nummer 2 Buchstabe a liegt in der Verantwortung des jeweiligen Anbieters des Zugangsdienstes. Der Anbieter eines Zugangsdienstes darf personenbezogene Daten der Versicherten ausschließlich für Zwecke des Aufbaus und des Betriebs seines Zugangsdienstes verarbeiten. § 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes ist entsprechend anzuwenden.

(3) Die Gesellschaft für Telematik erteilt einen Auftrag nach § 323 Absatz 2 Satz 1 zum alleinverantwortlichen Betrieb des gesicherten Netzes nach § 306 Absatz 2 Nummer 2 Buchstabe b, einschließlich der für den Betrieb notwendigen Dienste. Der Anbieter des gesicherten Netzes ist innerhalb des gesicherten Netzes verantwortlich für die Übertragung von personenbezogenen Daten, insbesondere von Gesundheitsdaten der Versicherten, zwischen Leistungserbringern, Kostenträgern sowie Versicherten und für die Übertragung im Rahmen der Anwendungen der elektronischen Gesundheitskarte. Der Anbieter des gesicherten Netzes darf die Daten ausschließlich zum Zweck der Datenübertragung verarbeiten. § 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes ist entsprechend anzuwenden.

(4) Der Betrieb der Dienste der Anwendungsinfrastruktur nach § 306 Absatz 2 Nummer 3 erfolgt durch den jeweiligen Anbieter. Die Anbieter sind für die Verarbeitung personenbezogener Daten, insbesondere von Gesundheitsdaten der Versicherten, zum Zweck der Nutzung des jeweiligen Dienstes der Anwendungsinfrastruktur verantwortlich.

(5) Die Gesellschaft für Telematik ist Verantwortliche für die Verarbeitung personenbezogener Daten in der Telematikinfrastruktur, soweit sie im Rahmen ihrer Aufgaben nach § 311 Absatz 1 die Mittel der Datenverarbeitung bestimmt und insoweit keine Verantwortlichkeit nach den vorstehenden Absätzen begründet ist. Die Gesellschaft für Telematik richtet für die Betroffenen eine koordinierende Stelle ein. Die koordinierende Stelle erteilt den Betroffenen allgemeine Informationen zur Telematikinfrastruktur sowie Auskunft über Zuständigkeiten innerhalb der Telematikinfrastruktur, insbesondere zur datenschutzrechtlichen Verantwortlichkeit nach dieser Vorschrift.

7.2.3 Lokale Datenverarbeitung auf dem Smartphone

Als Verantwortliche für die lokalen Verarbeitungsvorgänge der E-Rezept-App kommen einerseits der technische Betreiber der jeweiligen E-Rezept-App-Installation, also der Nutzer, andererseits der Anbieter der E-Rezept-App, also die gematik, in Betracht.

7.2.3.1 Verantwortlichkeit der Nutzer

Eine datenschutzrechtliche Verantwortlichkeit der Nutzer kommt nur in bestimmten Fällen in Betracht. Da der Nutzer schon begrifflich nicht Verantwortlicher und Betroffener zugleich sein kann, ist eine Verantwortlichkeit nur dort möglich, wo der Nutzer die personenbezogenen Daten einer anderen Person verarbeitet. Gleichzeitig ist die Anwendung der DSGVO dort ausgeschlossen, wo Daten ausschließlich zu persönlichen oder familiären Zwecken verarbeitet werden, Art. 2 Abs. 2 lit. c DSGVO („Haushaltsausnahme“). Eine Verantwortlichkeit ist also dort ausgeschlossen, wo der Nutzer E-Rezepte für sich oder für Familienangehörige verarbeitet.

In allen übrigen Fällen, zum Beispiel, wenn der Nutzer ein E-Rezept für einen Bekannten oder im Rahmen von entgeltlich erbrachten Unterstützungsleistungen einlöst, kann sich eine Verantwortlichkeit des Nutzers aus Art. 4 Nr. 7 HS. 2 DSGVO i. V. m. § 307 Abs. 1 S. 1 SGB V und – soweit diese gesetzlich vorgesehene Verantwortlichkeitszuweisungen nicht greift – aus der allgemeinen Bestimmung des Art. 4 Nr. 7 H. 1 DSGVO ergeben.

7.2.3.1.1 Gesetzliche Zuweisung der Verantwortung, Art. 4 Nr. 7 HS. 2 DSGVO i. V. m. § 307 Abs. 1 S. 1 SGB V

Eine Verantwortlichkeit des Nutzers ergibt sich nicht aus Art. 4 Nr. 7 HS. 2 DSGVO i. V. m. § 307 Abs. 1 S. 1 SGB V.

Im Falle des Betriebs der E-Rezept-App durch den Nutzer ist der Anwendungsbereich des § 307 Abs. 1 S. 1 SGB V schon nicht eröffnet. Zwar stellt die E-Rezept-App eine „Komponente der dezentralen Infrastruktur nach § 306 Absatz 2 Nummer 1 [SGB V]“ dar.[78] Sie wird jedoch nicht im Sinne des § 306 Abs. 2 Nr. 1 bzw. § 307 Abs. 1 S. 1 SGB V „für die Zwecke der Authentifizierung und elektronischen Signatur sowie zur Verschlüsselung, Entschlüsselung und sicheren Verarbeitung von Daten in der zentralen Infrastruktur“ genutzt. Daher ist der Tatbestand des § 307 Abs. 1 S. 1 SGB V nicht erfüllt.

Für dieses Ergebnis sprechen insbesondere die Historie, eine Auseinandersetzung mit dem Wortlaut der Norm und die Gesetzessystematik:

Im Zusammenhang mit der TI werden Komponenten definiert als „dezentrale technische Systeme oder deren Bestandteile“, § 306 Abs. 4 S. 3 SGB V. Das Definiens „technische Systeme oder [...] Bestandteile“ eines technischen Systems umfasst sowohl nach allgemeinem Sprachgebrauch als auch nach der Intention des historischen Gesetzgebers Apps.[79] Naturgemäß erfüllt jede App, die eine Komponente im Sinne der TI darstellt, auch das von § 306 Abs. 4 S. 3 und § 307 Abs. 1 SGB V verlangte Merkmal der Dezentralität. Apps werden regelmäßig in der persönlichen Umgebung eines Nutzers – eben auf dem privaten Smartphone – betrieben. Die E-Rezept App ist damit als dezentrale Komponente einzustufen.[80]

Dieser Einstufung steht auch nicht der Wortlaut des § 306 Abs. 2 SGB V entgegen, der die dezentrale Infrastruktur (Nr. 1), die zentrale Infrastruktur (Nr. 2) und die Anwendungsinfrastruktur (Nr. 3) unterscheidet. Zwar spricht § 306 Abs. 2 Nr. 1 SGB V von Komponenten der dezentralen Infrastruktur, die für „Zwecke der Authentifizierung und elektronischen Signatur sowie zur Verschlüsselung, Entschlüsselung und sicheren Verarbeitung von Daten in der zentralen Infrastruktur“ genutzt werden. Allerdings ist zu beachten, dass § 306 SGB V zu einer Zeit erlassen wurde, als die heutige Anwendung des E-Rezepts nicht existierte und demzufolge auch vom Gesetzgeber nicht berücksichtigt werden konnte. Ausweislich der Gesetzesbegründung hatte der Gesetzgeber bei der Festlegung der dreiteiligen Infrastruktur durch § 306 SGB V nur solche dezentralen Komponenten im Sinn, die in der Umgebung der Leistungserbringer betrieben werden, wie zum Beispiel Kartenterminals, Konnektoren und elektronische Heilberufsausweise.[81] Dies zeigt sich auch daran, dass es gerade diese Komponenten sind, die die in § 306 Abs. 2 Nr. 1 SGB V genannte Authentifizierung, elektronische Signatur, Verschlüsselung und Entschlüsselung zur sicheren Verarbeitung von Daten in der zentralen Infrastruktur (Nr. 2) ermöglichen. Die E-Rezept-App ermöglicht zwar ebenfalls Authentifizierung, elektronische Signatur, Verschlüsselung und Entschlüsselung, allerdings nicht zur Verarbeitung in der zentralen Telematikinfrastruktur (Nr. 2), sondern zur Verarbeitung in der Anwendungsinfrastruktur (Nr. 3).[82] Daher ist davon auszugehen, dass die E-Rezept-App – obwohl sie im Wortsinne eine dezentrale Komponente der TI darstellt – nicht von der auf die Umgebung der Leistungserbringer zielenden Beschreibung der dezentralen Infrastruktur in § 306 Abs. 2 Nr. 1 SGB V umfasst ist. Da der Gesetzgeber zur Beschreibung des Anwendungsbereichs des § 307 Abs. 1 S. 1 SGB V den Wortlaut des § 306 Abs. 2 Nr. 1 SGB V weitestgehend übernimmt, ist anzunehmen, dass der Anwendungsbereich des § 307 Abs. 1 S. 1 SGB V auf die von § 306 Abs. 2 Nr. 1 SGB V adressierten Komponenten beschränkt sein soll.

78 Vgl. auch den Überblick zu möglichen Bedeutungen des Begriffs der „Komponente“ und im Ergebnis wohl ebenso bei BeckOK KHR/Dettling, SGB V § 306 Rn. 132–142. Dettling weist unter Bezugnahme auf die Gesetzesbegründung allerdings darauf hin, dass alle Komponenten der Telematikinfrastruktur gemäß § 325 Abs. 1 SGB V zulassungsbedürftig sind (Rn. 132), was gegen die Komponenteneigenschaft der E-Rezept-App spricht. Die gematik geht aufgrund ihrer ausnahmsweisen Doppelfunktion als Zulassungsstelle und Anbieter der E-Rezept-App insoweit davon aus, dass die E-Rezept-App nicht der Zulassungspflicht nach § 325 SGB V unterfällt.

79 Vgl. die Gesetzesbegründung zu § 307 SGB V in BT-Drs. 19/18793, S. 100: „Komponenten können dabei sowohl Computerprogramme (Software) als auch Geräte (Hardware) umfassen.“

80 Das Smartphone und sein Betriebssystem, das über standardisierte Schnittstellen die notwendigen Funktionalitäten und Konnektivitäten für die App bereitstellt, sind selbst jedoch keine Komponenten der TI, vgl. BT-Drs. 18/11870 S. 2.

81 Vgl. BT-Drs. 19/18793, S. 100f.

82 Der E-Rezept-Fachdienst und das Apothekenverzeichnis werden in der Anwendungsinfrastruktur gemäß § 306 Abs. 2 Nr. 3 SGB V betrieben. Der Identitätsdienst ist ebenfalls zur Anwendungsinfrastruktur zu zählen, jedenfalls solange er ausschließlich für das E-Rezept genutzt wird.

Dass dieses Verständnis des § 306 Abs. 2 Nr. 1 SGB V maßgeblich für die Bestimmung des Anwendungsbereichs des § 307 Abs. 1 SGB V ist, zeigt auch die Gesetzessystematik. Zwar wurde die geltende Fassung des § 307 SGB V zu einem Zeitpunkt erlassen, zu dem die Einführung einer E-Rezept-App bereits vorhersehbar war. Es kann jedoch nicht angenommen werden, dass der Gesetzgeber den Anwendungsbereich des § 307 Abs. 1 SGB V deshalb auf sämtliche im Wortsinn dezentralen Komponenten der TI, d. h. auch auf solche in der Umgebung der Versicherten, ausweiten wollte. Denn nach § 307 Abs. 1 S. 3 SGB V nimmt der Gesetzgeber für „die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Infrastruktur nach § 306 Absatz 2 Nummer 1 durch Verantwortliche nach Satz 1 […] in der Anlage zu diesem Gesetz eine Datenschutz-Folgenabschätzung nach Artikel 35 Absatz 10 der Verordnung (EU) 2016/679“ vor. Prüfgegenstand dieser gesetzlichen DSFA sind nur die von Leistungserbringern betriebenen dezentralen Komponenten. Daraus folgt im Umkehrschluss, dass als Verantwortliche im Sinne des § 307 Abs. 1 S. 1 SGB V ausschließlich die Leistungsbringer anzusehen sind.

Eine Verantwortlichkeitszuweisung an die Nutzer der E-Rezept-App durch § 307 Abs. 1 S. 1 SGB V erfolgt daher nicht. Ihre Verantwortlichkeit kann sich somit nur aus der allgemeinen Bestimmung des Art. 4 Nr. 7 HS. 1 DSGVO ergeben, letztlich also daraus, dass der Nutzer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

7.2.3.1.2 Entscheidung über die Zwecke und Mittel der Verarbeitung, Art. 4 Nr. 7 HS. 1 DSGVO

Bei Betrachtung der tatsächlichen Umstände der Nutzung der E-Rezept-App auf den Smartphones der Versicherten spricht vieles dafür, dass diese nach allgemeinen Grundsätzen für die Verarbeitung verantwortlich sind, sofern es sich um Zwecke handelt, die nicht der Haushaltsausnahme des Art. 2 Abs. 2 lit. c DSGVO unterfallen.

Bezugspunkt für die datenschutzrechtliche Verantwortlichkeit nach Art. 4 Nr. 7 HS. 1 DSGVO ist die Entscheidungsgewalt über Zwecke und Mittel einer konkreten Verarbeitungstätigkeit.[83] Diese liegt hinsichtlich der lokalen Verarbeitungstätigkeiten beim Nutzer als Betreiber der E-Rezept-App. Der Nutzer entscheidet, ob und ggf. welche App-Funktionalitäten er nutzt und welche konkreten Daten von welchen konkreten Personen er mit der E-Rezept-App verarbeitet.[84] Eine gesetzliche Pflicht zur Nutzung der E-Rezept-App für die Verwaltung von E-Rezepten eines anderen Versicherten besteht nicht. Der Nutzer kann Auskunft über die lokal in seinem Profil in der E-Rezept-App gespeicherten personenbezogenen Daten geben und diese ggf. auf Antrag des betroffenen Versicherten löschen. Auch ist der Nutzer in der Lage, die Zulässigkeit der Nutzung der E-Rezept-App für die Verwaltung von E-Rezepten anderer Personen zu gewährleisten und effektive Maßnahmen zum Schutz der personenbezogenen Daten von Versicherten, deren E-Rezepte der Nutzer verwaltet, zu ergreifen (z. B. durch Aktivierung von Sperr- und weiteren Sicherheitsmechanismen des Smartphones, zeitnahes Installieren von App- und Systemupdates und vertraulichen Umgang mit Passwörtern). Als Betreiber der E-Rezept-App ist der Nutzer auch in der Lage, eine eingetretene Verletzung des Schutzes personenbezogener Daten eines Versicherten zu erkennen (z. B. bei Verlust oder Beschädigung des Smartphones oder bei einem Bekanntwerden der Zugangsdaten), die gebotenen Schadensminderungsmaßnahmen zu ergreifen und eine gemäß Art. 33 DSGVO erforderliche Meldung an die zuständige Datenschutzaufsichtsbehörde oder eine gemäß Art. 34 DSGVO erforderliche Benachrichtigung der betroffenen Versicherten vorzunehmen.

Vor diesem Hintergrund ist es sachgerecht, den Nutzer in Konstellationen, die nicht unter die Haushaltsausnahme fallen, als Verantwortlichen für die lokale Verarbeitung personenbezogener Daten durch die E-Rezept-App anzusehen. Unabhängig von einer im Einzelfall in Betracht kommenden datenschutzrechtlichen Verantwortlichkeit, d.h. außerhalb der Haushaltsausnahme, besteht jedenfalls eine umfassende de-facto-Verantwortlichkeit des Nutzers für den Datenschutz der lokalen Verarbeitung, da die E-Rezept-App in der technischen Umgebung des Nutzers läuft, die dem konkreten Zugriff und der Kontrolle der gematik oder eines anderen Anbieters von Komponenten oder Diensten der TI aufgrund der von der gematik getroffenen Designentscheidungen entzogen ist.[85]

83 Taeger/Gabel/Arning/Rothkegel, 4. Aufl. 2022, DS-GVO Art. 4 Rn. 187.

84 Vgl. im Ergebnis ebenso: Taeger/Gabel/Arning/Rothkegel, 4. Aufl. 2022, DS-GVO Art. 4 Rn. 187; Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 35 Rn. 14a; BeckOK DatenschutzR/Hansen, 40. Ed. 1.11.2021, DS-GVO Art. 35 Rn. 10.

85 So auch die Gesetzesbegründung in BT-Drs. 19/18793, S. 129; BT-Drs. 19/20708, S. 176, wobei unklar ist, ob die Verantwortlichkeit des Nutzers im datenschutzrechtlichen oder tatsächlichen Sinne angenommen wird.

7.2.3.2 Verantwortlichkeit der gematik

Eine Verantwortlichkeit des Nutzers für lokale Verarbeitungsvorgänge der E-Rezept-App schließt eine datenschutzrechtliche Verantwortlichkeit der gematik nicht grundsätzlich aus. Da jedoch ausschließlich der Nutzer der jeweiligen App-Installation die Entscheidungsgewalt über den Einsatz der App und ihre Funktionen innehat, bleibt für eine Verantwortlichkeit der gematik nach Art. 4 Nr. 7 HS. 1 DSGVO kein Raum. Eine Verantwortlichkeit der gematik kann sich allenfalls aus einer gesetzlichen Zuweisung gemäß Art. 4 Nr. 7 HS. 2 DSGVO i. V. m. § 307 Abs. 5 S. 1 SGB V ergeben. Eine solche Zuweisung setzt jedoch voraus, dass sowohl die Tatbestandsvoraussetzungen der Öffnungsklausel des Art. 4 Nr. 7 DSGVO als auch die der Verantwortungszuweisung in § 307 Abs. 5 S. 1 SGB V vorliegen. Das heißt konkret, dass das deutsche Recht die Zwecke und Mittel der Datenverarbeitung festlegen und die gematik als Verantwortliche bestimmen muss, um eine Verantwortlichkeit der gematik zu begründen.

7.2.3.2.1 Festlegung der Zwecke und Mittel durch den Gesetzgeber, Art. 4 Nr. 7 HS. 2 DSGVO

Die Zuweisung der Verantwortlichkeit durch den Gesetzgeber erfordert nach dem Wortlaut des Art. 4 Nr. 7 HS. 2 DSGVO zunächst, dass der Gesetzgeber die Zwecke und Mittel der lokalen Verarbeitung auf dem Smartphone des Nutzers festlegt. Eine ausdrückliche Festlegung der Zwecke und Mittel ist zwar bislang nicht erfolgt; allerdings ergeben sich wesentliche Zweckfestlegungen aus dem gesetzgeberischen Auftrag an die gematik, Komponenten der TI zu entwickeln und bereitzustellen, die den „Zugriff der Versicherten auf die Anwendung zur Übermittlung ärztlicher Verordnungen“ ermöglichen, sowie aus der gesetzlichen Vorgabe, für die „elektronische Übermittlung und Verarbeitung vertragsärztlicher elektronischer Verordnungen von apothekenpflichtigen Arzneimitteln […] die Telematikinfrastruktur zu nutzen, sobald die hierfür erforderlichen Dienste und Komponenten flächendeckend zur Verfügung stehen“, §§ 311 Abs. 1 Nr. 10, 360 Abs. 1 SGB V. Weitere Vorgaben, die die Zwecke und Mittel der lokalen Verarbeitung durch die E-Rezept-App mittelbar oder unmittelbar betreffen, sind:

- Die Zugriffskomponente muss den Versicherten einen barrierefreien Zugriff auf ihre Daten ermöglichen (§§ 311 Abs. 4 S. 1, 336 Abs. 1 S. 1 SGB V).
- Die Zugriffskomponente darf den Zugriff der Versicherten erst nach ihrer Authentifizierung mit einem geeigneten technischen Verfahren, das zur Authentifizierung einen hohen Sicherheitsstandard gewährleistet, ermöglichen (§ 336 Abs. 4 SGB V).
- Die Interoperabilität der Zugriffskomponente muss gewährleistet sein (§ 360 Abs. 10 S. 3 SGB V).
- Die Zugriffskomponente muss auf die Informationen des Nationalen Gesundheitsportals nach § 395 SGB V zugreifen können und den Versicherten diese Informationen mit Daten, die in ihrem E-Rezept gespeichert sind, verknüpft anbieten können (§ 360 Abs. 12 Nr. 1 SGB V).
- Die Zugriffskomponente muss bis zum 1. Januar 2024 eine Funktion zur Übermittlung von E-Rezepten an die nationalen eHealth-Kontaktstelle bereitstellen, damit Versicherte nach vorheriger Einwilligung in die Nutzung dieses Übermittlungsverfahrens ihre E-Rezepte bei Leistungserbringern in anderen EU- Mitgliedstaaten einlösen können (§ 360 Abs. 12 Nr. 2 SGB V).

Praktisch zwingen diese Vorgaben die gematik dazu, die E-Rezept-App für die gängigen mobilen Betriebssysteme zu entwickeln und mit Funktionen auszustatten, die einen einfachen Informationsaustausch zwischen Ärzten, Zahnärzten, Nutzern und Apothekern sowie den Einsatz eines praktikablen 2-Faktor-Authentifizierungsverfahrens ermöglichen. Diese Funktionalitäten setzten einen Zugriff auf den E-Rezept-Fachdienst über das Internet, in gewissem Umfang eine lokale Speicherung und eine Auswertung bestimmter personenbezogener Daten voraus, beispielsweise um die Verknüpfung mit Informationen des Nationalen Gesundheitsportals, die elektronische Einlösung eines E-Rezepts ohne aktive Internetverbindung (durch Vorzeigen des Rezeptcodes auf dem Bildschirm) oder den Zugriff auf die NFC-Scanner-API des Betriebssystems für die Authentifizierung per eGK zu ermöglichen. Ähnlich wirkt die Vorgabe der Barrierefreiheit. Sie bedeutet praktisch, dass spezielle Betriebssystemdienste für Bedienungshilfen (Accessibility Services) verwendet werden müssen, soweit dies unter Accessibility-Gesichtspunkten geboten ist.[86]

Hinzu kommt, dass die gesetzlichen Vorgaben im Lichte des erklärten Ziels verstanden werden müssen, Akzeptanz durch möglichst hohe Sicherheit bei möglichst hohem Komfort zu generieren. Der Gesetzgeber erwartet von der gematik, eine App zu entwickeln und bereitzu-

86 Vgl. BFIT-Bund, Handreichung „Barrierefreie mobile Apps“, Version 1.3, Kap. Entwicklungsansätze für mobile Apps: „Für die Entwicklung von barrierefreien Apps kann durch die enge Verzahnung mit der Plattform die dort angebotenen und dokumentierten Funktionen direkt genutzt werden. Native Apps haben daher den Vorteil, dass der Entwickler den maximalen Einfluss auf die Barrierefreiheit der App hat, da die einzige Abhängigkeit hier zu den Schnittstellen des Betriebssystems besteht. Wir gehen aktuell davon aus, dass dadurch auch die maximal mögliche Barrierefreiheit erreicht werden kann.“, https://handreichungen.bfit-bund.de/ag03/1.3/entwicklung.html#native-span-langenappsspan (zuletzt abgerufen am 15.12.2022).

stellen, die in technischer Hinsicht und unter Usability-Gesichtspunkten den Erwartungen und Gewohnheiten weiter Kreise der Bevölkerung umfassend Rechnung trägt. Dies kann insbesondere nach den gängigen Normen für die Bewertung von Software-Usability auch die Bereitstellung von aus Nutzersicht erwartbaren oder naheliegenden unterstützenden Funktionen für die Kernaufgaben der Software erfordern.

Insgesamt ergibt sich aus den praktischen Implikationen und der gesetzgeberischen Intention, dass die wesentlichen Zwecke und Mittel der Datenverarbeitung i. S. d. Art. 4 Nr. 7 HS. 2 DSGVO festgelegt werden. Für die Bestimmung wesentlicher Zwecke oder Mittel durch die gematik in Bezug auf die lokale Verarbeitung verbleibt im Hinblick auf die konkreten Vorgaben des Gesetzgebers kein Raum mehr. Zwar sind die Vorgaben des Gesetzgebers vielfach so abstrakt, dass sie von der gematik zumindest durch die App-Programmierung bestimmt, teilweise aber auch interpretiert werden müssen, um eine bedarfsgerechte App bereitzustellen (z. B. durch unterstützende Funktionen, die nicht ausdrücklich im Gesetz vorgesehen sind wie zum Beispiel die Apothekensuche). Soweit die gematik an der Umsetzung der gesetzlichen Vorgaben durch konkretisierende Spezifikationen oder die konkrete Programmierung der E-Rezept-App mitwirkt, kann sich diese Mitwirkung jedoch nur auf untergeordnete („unwesentliche") Zwecke oder Mittel der Datenverarbeitung beziehen. Dies führt im Ergebnis dazu, dass die Programmierung der E-Rezept-App als bloße Konkretisierung der Vorgaben des Gesetzgebers angesehen werden muss.[87]

7.2.3.2.2 Gesetzliche Zuweisung der Verantwortung, § 307 Abs. 5 SGB V

Die Zuweisung der Verantwortlichkeit erfordert – neben der Festlegung der (wesentlichen) Zwecke und Mittel durch den Gesetzgeber – weiter, dass die Verantwortlichkeit gesetzlich festgelegt ist. Für lokale Datenverarbeitungen auf dem Smartphone der Nutzer findet sich eine solche Zuweisungsnorm in § 307 Abs. 5 SGB V. Nach dieser Vorschrift ist die gematik verantwortlich

„für die Verarbeitung personenbezogener Daten in der Telematikinfrastruktur […], soweit sie im Rahmen ihrer Aufgaben nach § 311 Absatz 1 [SGB V] die Mittel der Datenverarbeitung bestimmt und insoweit keine Verantwortlichkeit nach den vorstehenden Absätzen [1 bis 4] begründet ist."

Diese Voraussetzungen liegen in Bezug auf die lokalen Datenverarbeitungstätigkeiten nicht vor. Zwar handelt es sich bei den lokal verarbeiteten Daten um personenbezogene Daten. Die Verarbeitung dieser Daten findet in der TI und im Rahmen der Aufgaben statt, die der gematik nach § 311 Abs. 1 SGB V übertragen wurden; schließlich wird auch keine anderweitige Verantwortlichkeit für die lokalen Verarbeitungsvorgänge nach § 307 Abs. 1 bis 4 SGB V begründet. Allerdings tritt die Vorgabe der Mittel der lokalen Verarbeitung hinter die faktische Entscheidungsgewalt des Nutzers (siehe 7.2.3.1) so weit zurück, dass von einem „bestimmen" nicht gesprochen werden kann.

Diese Einschätzung deckt sich auch mit der Auffassung des EDPB, wonach die gesetzliche Verantwortlichkeitszuweisung gemäß Art. 4 Nr. 7 HS. 2 DSGVO voraussetzt, dass als Verantwortlicher nicht irgendeine Stelle bestimmt wird, sondern eine Stelle, die „echte Kontrolle" über die lokale Verarbeitung ausübt. Diese liegt Kontrolle hinsichtlich der in Rede stehenden Verarbeitung allerdings nicht bei der gematik, sondern beim einzelnen Nutzer.

7.2.3.2.2.1.1 „Verarbeitung personenbezogener Daten"

Es wird angenommen, dass es sich bei den lokal verarbeiteten Daten um personenbezogene Daten handelt (vgl. 7.1.1.1)

7.2.3.2.2.1.2 „in der Telematikinfrastruktur"

Mit der lokalen Datenverarbeitung in der E-Rezept-App ist eine Verarbeitung personenbezogener Daten „in der Telematikinfrastruktur" i. S. d. § 307 Abs. 5 S. 1 SGB V verbunden, da es sich bei der E-Rezept-App um eine dezentrale Komponente der TI handelt (vgl. 7.2.3.1.1). Diese Aussage wird durch die Legaldefinition der „Komponente" in § 306 Abs. 4 S. 3 SGB V noch einmal bestätigt. Fraglich ist zwar, in welcher der drei Infrastrukturen der TI (vgl. 4.5.1) die E-Rezept-App zu verorten ist, da es sich weder um eine Komponente zur Authentifizierung, elektronischen Signatur, Verschlüsselung, Entschlüsselung oder zur sicheren Verarbeitung von Daten in der zentralen Infrastruktur noch um einen sicheren Zugangsdienst zur dezentralen Infrastruktur oder ein sicheres Netz i. S. d. § 306 Abs. 2 Nr. 2 SGB V handelt und die E-Rezept-App auch nicht in Kapitel 11 des SGB V aufgeführt ist, § 306 Abs. 2 Nr. 3 SGB V. Diese Frage kann hier jedoch dahinstehen, da jedenfalls feststeht, dass durch die E-Rezept-App personenbezogene Daten „in der Telematikinfrastruktur" verarbeitet werden.

87 Eine Ausnahme stellen die Verarbeitungsvorgänge für App-Funktionen dar, die keinerlei erkennbaren Anknüpfungspunkt im Gesetz haben (z. B. Erfassung von Daten für die Nutzungsanalyse); die Verantwortlichkeit richtet sich in diesen Fällen nach Art. 4 Nr. 7 HS. 1 DSGVO, was regelmäßig eine Verantwortlichkeit der gematik zur Folgen haben wird.

7.2.3.2.2.1.3 „die Mittel der Datenverarbeitung“

Die Festlegung der technischen und prozeduralen Details der Verarbeitung durch die konkrete Gestaltung der App, ihre Spezifikationen und Funktionen sind aufgabengemäße konkretisierende Mittelfestlegungen. Umfasst sind nach hier vertretener Auffassung allerdings nur solche Mittel, die nicht schon vom Gesetzgeber i. S. d. Art. 4 Nr. 7 HS. 2 DSGVO „vorgegeben“ sind (vgl. 7.2.3.2.1). Es handelt sich damit zwar um Mittel der Datenverarbeitung, allerdings nicht um wesentliche, sondern um unwesentliche Mittelfestlegungen.

7.2.3.2.2.1.4 „im Rahmen ihrer Aufgaben nach § 311 Absatz 1“

Eine Verantwortlichkeitszuweisung zur gematik nach Art. 4 Nr. 7 HS. 2 DSGVO i. V. m. § 307 Abs. 5 S. 1 SGB V setzt weiter voraus, dass die gematik die Mittel der Verarbeitung im Rahmen ihrer gesetzlichen Aufgaben nach § 311 Abs. 1 SGB V bestimmt. Diese Voraussetzungen liegen hier vor. Nach § 311 Abs. 1 Nr. 10 SGB V gehört es zu den Aufgaben der gematik, Komponenten der TI, die den Zugriff der Versicherten auf die Anwendung zur Übermittlung ärztlicher Verordnungen ermöglichen, zu entwickeln und zur Verfügung zu stellen.

7.2.3.2.2.1.5 „bestimmt“

Nach dem ausdrücklichen Wortlaut des § 307 Abs. 5 SGB V ist die gematik nur dann für die Verarbeitung personenbezogener Daten in der TI verantwortlich, wenn sie die Mittel der Datenverarbeitung bestimmt und insoweit keine Verantwortlichkeit nach den vorstehenden Absätzen begründet ist.

Das ist vorliegend nicht der Fall.

Fraglich ist zunächst, was überhaupt unter Bestimmen i. S. d. § 307 Abs. 5 S. 1 SGB V zu verstehen ist. Unstreitig dürfte ein Bestimmen dann nicht vorliegen, wenn eine Stelle weder rechtlich noch tatsächlich Einfluss auf eine konkrete Datenverarbeitung nehmen kann. Nicht ausreichen dürfte darüber hinaus aber auch jede nur untergeordnete Festlegung. Welches Ausmaß an Einflussfähigkeit konkret vorliegen muss, um von einem „Bestimmen“ zu sprechen, ist zwar bislang nicht abschließend geklärt.[88] Die besseren Gründe sprechen jedoch dafür, „Bestimmen“ synonym zu den von Art. 4 Nr. 7 und Art. 26 DSGVO verwendeten Begriffen des „Entscheidens“ und „Festlegens“ als Ausüben tatsächlicher Entscheidungshoheit („echter Kontrolle“) über Verarbeitungsmittel eines konkreten Verarbeitungsfalles zu verstehen.

Dafür sprechen zunächst teleologische Erwägungen: Die DSGVO knüpft an die Rolle des Verantwortlichen verschiedene Pflichten. Insbesondere soll der Verantwortliche dafür Sorge tragen, dass die Vorschriften der DSGVO jederzeit eingehalten werden. An dieser Verpflichtung lässt sich erkennen, dass der Verantwortliche ein gewisses Ausmaß an Kontrolle über die Datenverarbeitung haben muss.[89] Kann eine Stelle ihre Pflichten schon deshalb nicht angemessen erfüllen, weil sie die Datenverarbeitung gar nicht oder nicht wesentlich beeinflussen kann, ergibt es keinen Sinn, dieser Stelle die Rolle des Verantwortlichen per Gesetz zuzuweisen.

Dafür spricht aber auch die Leitlinie 7/2020 des EDPB. Dort heißt es: „Ist der Verantwortliche im Gesetz explizit festgelegt, ist dies für die Bestimmung, wer als Verantwortlicher handelt, maßgeblich. Dies setzt voraus, dass der Gesetzgeber diejenige Stelle als Verantwortlichen bestimmt hat, die in der Lage ist, echte Kontrolle auszuüben.“[90] Insoweit ist zunächst zu bemerken, dass die Notwendigkeit „echter Kontrolle“ ausdrücklich nur für den Fall formuliert ist, dass der Verantwortliche im Gesetz „explizit festgelegt“ ist. Es wird nicht dazu Stellung genommen, ob die Voraussetzung echter Kontrolle über eine Datenverarbeitung nach dem EDPB auch dann gelten soll, wenn – so wie in den fünf Absätzen des § 307 SGB V geschehen – lediglich eine „Bestimmung der Kriterien seiner Benennung“ erfolgt ist. Da die Möglichkeit zur gesetzliche Festlegung der Verantwortlichkeit dem gleichen Zweck wie die Möglichkeit zur Festlegung von Kriterien zur Bestimmung des Verantwortlichen dient, nämlich der Gewährleistung der Betroffenenrechte und der aufsichtsbehördlichen Kontrolle im Fall einer gesetzlichen Festlegung von Zwecken und Mitteln der Verarbeitung, ist jedoch anzunehmen, dass die Voraussetzung echter Kontrolle auch dann erforderlich ist, wenn lediglich Kriterien zur Bestimmung des Verantwortlichen gesetzlich festgelegt werden.

Aus dem begrifflichen Erfordernis echter Kontrolle ergibt sich, dass durch eine gesetzliche Verantwortlichkeitszuweisung eine Verantwortlichkeit nur derjenigen Stelle begründet werden kann, die aufgrund

88 Insoweit stellt eine gesetzlich zugewiesene Verantwortlichkeit einen relevanten, aber nicht den alleinigen Faktor der Bewertung dar, vgl. Taeger/Gabel/Arning/Rothkegel, 4. Aufl. 2022, DS-GVO Art. 4 Rn. 182. Im Ergebnis ebenso der, EDPB, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Rn. 21 ff., dort insb. Rn. 23, wonach eine gesetzliche Verantwortlichkeitsbestimmung nur „maßgeblich“ sein soll unter der Voraussetzung, dass der Gesetzgeber „diejenige Stelle als Verantwortlichen bestimmt hat, die in der Lage ist, echte Kontrolle auszuüben.“

89 vgl. Ehmann/Selmayr/Klabunde, 2. Aufl. 2018, DS-GVO Art. 4 Rn. 38.

90 EDPB, Leitlinien 7/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Rn. 23.

ihrer tatsächlichen Funktion den faktisch größten Einfluss auf die Verarbeitung hat und somit die Betroffenenrechte umfassend gewährleisten kann.[91] Eine Verantwortlichkeitszuweisung an die gematik setzt – mit anderen Worten – voraus, dass ihre tatsächliche Funktion gebührend widergespiegelt wird und die Betroffenen nicht der Möglichkeit beraubt werden, ihre Rechte gegenüber denjenigen Stellen geltend zu machen, die den faktisch größten Einfluss auf die Datenverarbeitung haben.[92]

Diese Voraussetzungen liegen hier nicht vor.

Die gematik übt keine echte Kontrolle über die lokale Verarbeitung auf dem Smartphone des Nutzers aus. Wie oben gezeigt liegt die Entscheidungshoheit für sämtliche Verarbeitungsvorgänge auf dem Smartphone beim jeweiligen Nutzer der E-Rezept-Installation. Die gematik entscheidet demgegenüber lediglich abstrakt über die Gestaltung der App und vollzieht dort, wo sie dies tut, lediglich Entscheidungen des Gesetzgebers nach. Der Gesetzgeber hat gemäß Art. 4 Nr. 7 HS. 2 DSGVO die wesentlichen Zwecke und Mittel der lokalen Verarbeitung vorgeben, die gematik die konkreten Verarbeitungszwecke und die praktischen Aspekte der Umsetzung im Rahmen ihrer Aufgabe gemäß § 311 Abs. 1 Nr. 10 SGB V festgelegt (z. B. durch Gestaltung des User Interface und der User Experience, Auswahl von konkreten Verschlüsselungsverfahren und Spezifikationsfestlegungen). Diese Festlegungen führen absichtlich dazu, dass die gematik keine Kenntnisnahme- und Zugriffsmöglichkeit hinsichtlich der lokalen Datenverarbeitung erhält. Dies hat wiederum zur Folge, dass die gematik den Pflichten eines Verantwortlichen hinsichtlich der lokalen Verarbeitung nicht nachkommen kann. Insbesondere hat die gematik keinerlei rechtliche oder technische Handhabe, auf den einzelnen Nutzer so einzuwirken, dass dieser die nur vom ihm ausführbaren Mitwirkungshandlungen etwa für die Umsetzung von Betroffenenrechten vornimmt oder die zum Schutz von personenbezogenen Daten erforderlichen Schutzmaßnahmen ergreift.[93] Auch ist die gematik – im Gegensatz zum Nutzer – nicht in der Lage, der Rechenschaftspflicht hinsichtlich der lokalen Verarbeitung durch den Nutzer nachzukommen. Anders als dieser hat jene keine Möglichkeit, um von Verletzungen des Schutzes personenbezogener Daten Kenntnis zu erlangen und eventuellen Melde- und Benachrichtigungspflichten nach Art. 33, 34 DSGVO nachzukommen, etwa wenn der Nutzer sein Smartphone verloren hat oder sich unbefugte Personen Zugang zur E-Rezept-App verschafft haben.

Vor diesem Hintergrund ist die Annahme einer Verantwortlichkeit der gematik für die lokale Verarbeitung mit dem funktionalen Konzept, das dem Begriff der Verantwortlichkeit in der DSGVO zugrunde liegt, nicht vereinbar. Die gesetzliche Bestimmung der gematik als Verantwortliche für die lokale Verarbeitung auf dem Smartphone hätte weder einen Nutzen für den Schutz personenbezogener Daten noch für die Kontrollierbarkeit der auf dem Smartphone stattfindenden Verarbeitung. Stattdessen entstünde bei Betroffenen durch die Behauptung einer gesetzlichen Verantwortlichkeit der gematik möglicherweise sogar der unzutreffende Eindruck, dass die gematik die Betroffenenrechte und den Datenschutz bei der konkreten lokalen Verarbeitung nicht nur gewährleisten muss, sondern dies auch nachweislich kann.

Dieses Ergebnis deckt sich auch mit der Begründung sowie dem Sinn und Zweck der Norm. Die Verantwortlichkeitszuweisung des § 307 Abs. 5 S. 1 SGB V soll Ausnahmefälle erfassen, bei denen die gematik beispielsweise zur Vermeidung von Störungen angemessene organisatorische und technische Vorkehrungen einschließlich des Einsatzes von geeigneten Systemen zur Erkennung von Störungen und Angriffen festlegt und insoweit zur Verarbeitung personenbezogener Daten befugt ist (§ 331 Abs. 3 und 4 SGB V).

Eine Verantwortlichkeitslücke durch die Verneinung der datenschutzrechtlichen Verantwortlichkeit der gematik für die konkrete lokale Verarbeitung entsteht nicht. Gemäß § 311 Abs. 4 SGB V ist die gematik verpflichtet, bei der Wahrnehmung ihrer Aufgaben (die auch die Bereitstellung der E-Rezept-App umfasst) die Einhaltung des Datenschutzes und der Datensicherheit sicherzustellen. Diese Pflicht trägt der tatsächlichen Funktion und dem tatsächlichen Wirkbereich der gematik angemessen Rechnung.

91 Simitis/Hornung/Spiecker gen. Döhmann/Petri, Datenschutzrecht, DSGVO Art. 4 Nr. 7 Rn. 26.

92 Simitis/Hornung/Spiecker gen. Döhmann/Petri, Datenschutzrecht, DSGVO Art. 4 Nr. 7 Rn. 26.

93 Die Situation ist vergleichbar mit dem typischen Fall, dass ein Softwarehersteller eine lokal ablaufende Software („Offline-Software“) abschließend programmiert, beispielsweise ein Betriebssystem oder eine Textverarbeitungs-Anwendung. Werden mit diesen Softwares personenbezogene verarbeitet, sind der jeweilige Betreiber bzw. Nutzer die Verantwortlichen, da sie über die Zwecke und Mittel hinsichtlich des konkreten Verarbeitungsvorganges (bzw. die konkret zu verarbeitenden personenbezogenen Daten) bestimmen, vgl. Taeger/Gabel/Arning/Rothkegel, 4. Aufl. 2022, DS-GVO Art. 4 Rn. 187.

7.2.4 Verarbeitung durch Betriebssystemdienste

Wie in anderen App- und Plattformkonstellationen auch stellt sich im Zusammenhang mit der E-Rezept-App die Frage, wem welche datenschutzrechtliche Rolle zufällt, wenn die App auf die vom Hersteller vorgesehene Weise auf standardisierte Betriebssystemdienste (vgl. 4.5.3) zugreift.[94] Als Verantwortliche kommen vor allem diejenigen Akteure in Betracht, die auf die Entscheidung über die konkrete Verarbeitung durch Betriebssystemdienste einen potentiell maßgeblichen Einfluss ausüben: die Nutzer, die Betriebssystemhersteller und die gematik.

7.2.4.1 Verantwortlichkeit der Nutzer

Viel spricht dafür, dass die Nutzer der E-Rezept-App auch für die Datenverarbeitung durch die Dienste des Betriebssystems datenschutzrechtlich verantwortlich sind, wenn und soweit es sich um Daten handelt, die der Haushaltsausnahme nicht unterfallen. Jedenfalls spricht viel dafür, dass eine maßgebliche de-facto-Verantwortlichkeit des Nutzers besteht.

Indem ein Nutzer die E-Rezept-App auf seinem Smartphone installiert und auf die vom Hersteller vorgesehene Art und Weise nutzt, entscheidet er über die wesentlichen Mittel der Verarbeitung, nämlich darüber, dass die App die Betriebssystemdienste des jeweiligen Betriebssystems bestimmungsgemäß zu verwenden hat, um die von der gematik beworbenen, im App Store beschriebenen oder als selbstverständlich vorausgesetzten Funktionen bereitzustellen.

Dafür sprechen insbesondere die folgenden Erwägungen:

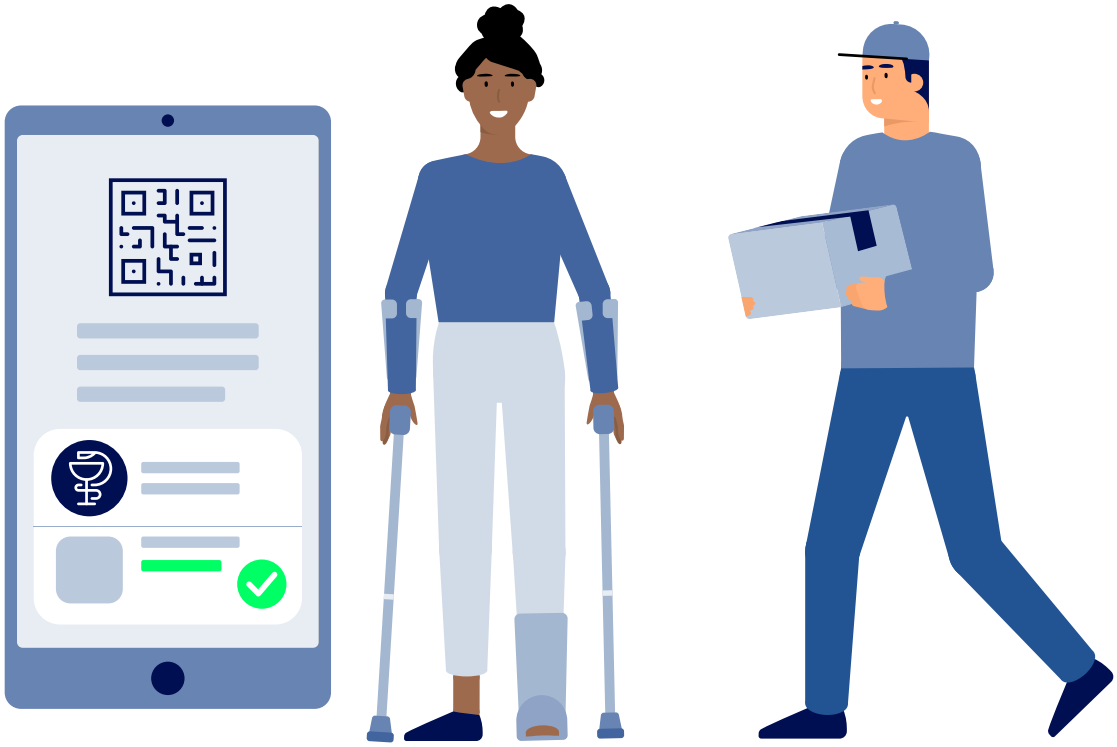
Ein Nutzer ist zur Nutzung eines Smartphones oder zum Betrieb eines bestimmten Smartphone- oder App-Setups nicht verpflichtet. Auswahl, Erwerb, Installation, Konfiguration und Betrieb der entsprechenden Geräte, Betriebssysteme und Apps liegen in seinem persönlichen (nicht unbedingt und nicht nur datenschutzrechtlichen) Zuständigkeits- und Verantwortungsbereich. Er allein entscheidet über das Ob und Wie seiner Smartphone-Nutzung. Er erwirbt ein bestimmtes Gerät und schließt mit dem jeweiligen Hersteller Nutzungs- und Lizenzvereinbarungen über das jeweilige Betriebssystem, die Betriebssystemdienste und das persönliche Nutzerkonto der jeweiligen Plattform (z. B. Google-Konto), um die für den Betrieb oder die Nutzung der Leistungen erforderlichen Nutzungsrechte zu erhalten. Der Nutzer wird informiert über das vertragliche Leistungs- und Pflichtenprogramm des Betriebssystemherstellers, die relevanten Datenverarbeitungspraktiken und erteilt gegebenenfalls die für notwendig erachteten Einwilligungen für bestimmte Verarbeitungszwecke.[95] Entsprechendes gilt auch für die Nutzung von Drittanbieter-Apps aus einem App-Store. Der Nutzer entscheidet allein, ob und welche Apps er nutzen möchte und welchen Apps er Zugriff auf (welche) Betriebssystemdienste erlaubt.

Daran ändert auch der Umstand nichts, dass weite Teile der Bevölkerung zur beruflichen oder sozialen Teilhabe heute vielfach auf die Nutzung eines Smartphones angewiesen sind. Die soziale Angewiesenheit limitiert und führt zwar die Entscheidung des Einzelnen, sie ist aber nicht so stark ausgeprägt, dass sie eine echte Wahlfreiheit von vornherein auszuschließen vermag. Selbst dort, wo der Nutzer glaubt, ein Smartphone verwenden zu müssen, führt dieser Umstand weder dazu, dass er ein bestimmtes Smartphone mit einer bestimmten Konfiguration nutzen muss, noch dazu, dass er auf diesem Smartphone (oder überhaupt) eine bestimmte App, etwa die E-Rezept-App der gematik, installiert und nutzt.

Mit der Entscheidung für die Nutzung eines bestimmten Smartphones oder einer bestimmten App ist dabei zugleich eine Obliegenheit des Nutzers verbunden, sich über Funktionen, Systemanforderungen und Datenschutzaspekte des ausgewählten Geräts und Betriebssystems sowie der gewählten App zu informieren (zum Beispiel zu Berechtigungssystemen, eventuellen Abhängigkeiten von Online- bzw. Cloud-Diensten oder zur Verfügbarkeit biometrischer Authentifizierungsdienste). Der Nutzer muss durch sachgerechte Einstellungen und laufende Aktualisierungen die Sicherheit der genutzten Betriebssystemdienste und Apps gewährleisten; sieht er sich hierzu

94 Dies betrifft insbesondere Drittanbieter-Apps, d. h. Apps, die nicht vom Hersteller des Betriebssystems angeboten werden. In der Regel sind Drittanbieter-Apps nicht standardmäßig installiert, sondern werden über den App-Store des jeweiligen Betriebssystem vertrieben. In der datenschutzrechtlichen Diskussion werden in diesem Zusammenhang besonders solche Betriebssystemdienste behandelt, die Funktionen bereitstellen, die grundsätzlich auch mit selbst entwickelten oder Diensten von anderen Anbietern realisiert werden könnten oder die unter Inkaufnahme insbesondere von Komfort- oder Sicherheitsnachteilen verzichtbar sind, weil sie für die Kernfunktionen der jeweiligen App nicht benötigt werden (Integritätsprüf-, Push- und Sicherheitsdienste). Die aufgeworfenen Fragen betreffen jedoch gleichermaßen auch technisch zwingende Betriebssystemdienste, ohne deren Nutzung eine App nicht funktionsfähig ist.

95 In diese Richtung gehen auch die Erwägungen des EDPB am Beispiel der Nutzung eines standardisierten Cloud-Services durch einen Kunden, bei dem die maßgebliche Entscheidungsbefugnis über die Verarbeitung durch den Cloud-Service gesehen wird, vgl. EDPB, Leitlinien 7/2020, zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Rn. 30.



nicht in der Lage, so muss er von der Nutzung absehen oder die Risiken tragen, die mit seinem Nutzungsverhalten verbunden sind.

Realistischerweise ist zwar anzunehmen, dass dem durchschnittlichen Nutzer die genauen technischen Details seines Betriebssystems oder seiner App nur punktuell bekannt sind. Dies spricht jedoch ebenfalls nicht gegen die Annahme, dass die Nutzung der Betriebssystemdienste auf die Entscheidung des Nutzers zurückgeht. Denn der Nutzer muss nicht über jedes einzelne Verarbeitungsmittel entscheiden. Erforderlich aber auch ausreichend ist, dass der Nutzer über die wesentlichen Mittel der Verarbeitung entscheidet. Das geschieht hier, indem er sich dazu entschließt, eine bestimmte App auf einem bestimmten Smartphone zu installieren und diese App auf eine bestimmte Art zu nutzen. Damit übt der Nutzer den entscheidenden Einfluss de facto auch auf die konkrete Verarbeitung von personenbezogenen Daten im Zusammenhang mit Betriebssystemdiensten aus. Diese Überlegungen gelten für alle Betriebssystemdienste gleichermaßen.

Es ist sachgerecht und folgerichtig, dass die Entscheidungshoheit des Nutzers nicht nur bei lokalen Verarbeitungsvorgängen bejaht wird, die ohne Nutzung von Betriebssystemdiensten ablaufen, sondern auch hinsichtlich der – zum Teil lokalen – Datenverarbeitungsvorgänge, die Betriebssystemdienste bestimmungsgemäß nutzen. Schließlich ist eine unterschiedliche Bewertung von essentiellen und nicht-essentiellen Betriebssystemdiensten datenschutzrechtlich weder geboten noch möglich. Denn das maßgebliche Kriterium der faktischen Entscheidungshoheit über die wesentlichen Mittel der konkreten Verarbeitung ist für beide Betriebssystemdienstkategorien gleichermaßen erfüllt. Daran ändert auch der Umstand nichts, dass Nutzer über essentielle Betriebssystemdienste regelmäßig besser informiert sein dürften als über nichtessentielle. Insbesondere kann eine Verantwortlichkeit auch begründet werden, wenn die eigene datenschutzrechtliche Rolle oder der Personenbezug der verarbeiteten Daten falsch oder gar nicht bewertet wird.

Dieses Ergebnis bildet die Realität zutreffend ab. Es wäre mit den Erwartungen des Nutzers nicht vereinbar, dass eine vom Nutzer installierte Drittanbieter-App von den Betriebssystemdiensten, mit denen die gewünschten oder im Lichte des jeweiligen Zwecks erwarteten und sachgerechten App-Funktionen (z. B. Push-Benachrichtigungen, wenn dies im jeweiligen Use Case naheliegend und nützlich ist) oder das gebotene hohe IT-Sicherheitsniveau ermöglicht werden, keinen bestimmungsgemäßen Gebrauch macht. Würde die E-Rezept-App diesen Erwartungen nicht entsprechen, würde dies die vom Nutzer ausgeübte Entscheidungshoheit verkennen und seine Entscheidungsbefugnis in Frage stellen.

7.2.4.2 Verantwortlichkeit der Betriebssystemhersteller

Betriebssystemhersteller kommen als Verantwortliche für einzelne Verarbeitungsvorgänge insbesondere im Rahmen von teilweise Server-basierten Betriebssystemdiensten jedenfalls dann in Betracht, wenn die Nutzung der App durch den Nutzer der Haushaltsausnahme unterfällt und der Nutzer daher kein Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist.

Da zum Installieren der App aus dem App-Store und für die Nutzung wichtiger Betriebssystemdienste ein Benutzerkonto bei dem jeweiligen Betreiber benötigt wird (Apple-ID, Google-Konto, Huawei ID), besteht das Vertragsverhältnis eines Nutzers in Deutschland nach den jeweiligen Nutzungsbedingungen mit einem irischen Tochterunternehmen des jeweiligen Betreibers. Nach allen Datenschutzbedingungen dieser Tochterunternehmen sehen diese sich jeweils als Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO für die personenbezogene Datenverarbeitung auch im Zusammenhang mit der Nutzung von Betriebssystemdiensten durch den Nutzer.

Die de-facto-Entscheidungshoheit über die konkrete Verarbeitung personenbezogener Daten durch übliche und von Apps regelmäßig genutzte Betriebssystemdienste eines bestimmten Herstellers im Zusammenhang mit der Nutzung der E-Rezept-App kann dennoch beim einzelnen Nutzer verbleiben. Dafür spricht insbesondere eine wertende Betrachtung der tatsächlichen Funktion, die Betriebssystemhersteller im Zusammenhang mit Drittanbieter-Apps erfüllen.

Betriebssystemhersteller legen in ihren Lizenzbedingungen diverse Befugnisse fest, die auch die Nutzung der Betriebssystemdienste durch Drittanbieter-Apps betreffen können. Dazu gehört regelmäßig die Verarbeitung bestimmter personenbezogener Daten, insbesondere der Geräte- und Nutzungsdaten sowie die Konto-ID des Nutzerkontos. Dazu gehört aber auch – im Fall des Apple-iOS-Betriebssystems auf Grundlage einer Einwilligung – die Verarbeitung von Daten, die bei der Nutzung von Betriebssystemdiensten durch Apps anfallen (Nutzungsdaten bzw. Telemetriedaten). Weiterhin behalten sich die Betriebssystemhersteller üblicherweise Befugnisse vor, um Betriebssystemfunktionen und -dienste im Rahmen von Softwareaktualisierungen verändern oder entfernen zu dürfen, die Nutzung von Betriebssystemfunktionen und -diensten von der Durchführung von Updates oder der Verwendung bestimmter Gerätemodelle abhängig zu machen oder um das Gerät des Nutzers auf potentielle Sicherheitsrisiken hin zu überprüfen.

Zudem behalten sich die Betriebssystemhersteller üblicherweise vor, eine vom Nutzer installierte Drittanbieter-App in bestimmten Fällen (z. B. aus Sicherheitsgründen) zu löschen.

Auf diese Rechte wird in den Nutzungsbedingungen und Datenschutzhinweisen hingewiesen; teilweise verpflichten Betriebssystemhersteller auch App-Entwickler, dem Nutzer bestimmte Informationen über die betriebssystemseitige Datenverarbeitung bereit zu stellen. Sie stellen an verschiedenen Stellen innerhalb ihrer Produkte und auf ihren Websites umfangreiche Informationen zu Datenschutz- und Sicherheitsfunktionen ihrer Betriebssysteme bereit und bewerben diese, da wohl angenommen wird, dass die integrierten Datenschutzfunktionen ein Kriterium für die Entscheidung von bestimmten Verbrauchergruppen für oder gegen eine bestimmte Betriebssystemplattform sind. Es kann insoweit beobachtet werden, dass dem Nutzer auch im Rahmen der Geräteeinrichtung umfangreiches Informationsmaterial über die Funktionsweise und Datenverarbeitungspraxis der Betriebssystemdienste zur Verfügung gestellt wird. In der Gesamtschau könnte durch das zur Verfügung stellen dieser Informationen durchaus eine informierte Entscheidung des Nutzers ermöglicht werden. Jedoch darf angesichts der Komplexität und des Umfangs dieser Informationen sowie der typischen Nutzergewohnheiten nicht angenommen werden, dass der Nutzer diese Gelegenheiten zur ausführlichen Information auch vollumfänglich wahrnimmt. Genauso lebensfern wäre es jedoch, anzunehmen, dass ein Nutzer völlig verkennt, dass er durch die konkrete Auswahl und Konfiguration eines bestimmten Betriebssystems sowie durch sein konkretes Nutzungsverhalten erheblichen Einfluss auf die Verarbeitungsvorgänge seines Betriebssystems im Zusammenhang mit der Nutzung von Drittanbieter-Apps nehmen kann. Im Gegenteil. Nutzer sind in einem technisch vorgegebenen Rahmen in der Lage, einzelne Betriebssystemdienste durch Konfigurationseinstellungen in den Systemeinstellungen des Betriebssystems zu beeinflussen und – in ausgewählten Fällen – zu deaktivieren.

Vor diesem Hintergrund ist festzustellen, dass die Entscheidung über Mittel und Zwecke der Verarbeitung durch die Betriebssystemhersteller in gewissem Umfang abstrakt vorgegeben wird. Die endgültige Entscheidung über die konkreten Modalitäten der Verarbeitung personenbezogener Daten durch die Betriebssystemdienste eines bestimmten Herstellers liegt jedoch nicht eindeutig bei den Betriebssystemherstellern, sondern bei den einzelnen Nutzern. Es liegt auch in deren Verantwortung, ein für ihren Bedarf geeignetes Betriebssystem auszuwählen, dieses sachgerecht zu konfigurieren und so die Vorausset-

zungen für die sichere Nutzung von Apps zu schaffen. Sollte sich ein Nutzer hierzu nicht in der Lage sehen, muss er sich Unterstützung beschaffen oder erforderlichenfalls (zunächst) von der Nutzung der betreffenden Betriebssysteme oder der E-Rezept-App absehen. Auch falls sich der Nutzer trotz einer für ihn als unzureichend wahrgenommenen Informationslage im konkreten Einzelfall für die Nutzung der E-Rezept-App entscheiden sollte, beruht die damit einhergehende Datenverarbeitung im Zusammenhang mit dem bestimmungsgemäßen Zugriff der E-Rezept-App auf die Betriebssystemdienste de facto auf einer vom Nutzer ausgeübten Entscheidungsbefugnis.

Zusammenfassend kann festgehalten werden, dass die Rechtslage hinsichtlich der Verantwortlichkeiten von Herstellern und Nutzern bei der Nutzung von Betriebssystemdiensten durch Apps nach wie vor in Teilen unklar ist und im Rahmen dieser DSFA nicht geklärt werden kann. Dies ist bei der Risikoanalyse zu berücksichtigen.

7.2.4.3 Verantwortlichkeit der gematik

Nach hier vertretener Auffassung liegt bei wertender Betrachtung aller Umstände die maßgebliche, da endgültige tatsächliche Entscheidungshoheit in erster Linie beim Nutzer. Natürlich beeinflussen die Designentscheidungen der gematik die konkreten lokalen Zugriffe auf Betriebssystemdienste, etwa durch die Weitergabe von personenbezogenen Daten. Dies gilt jedoch für jede Standardsoftware, die von einem Nutzer für bestimmte eigene Verarbeitungszwecke eingesetzt wird. Eine Verantwortlichkeit des Herstellers der Standardsoftware begründet dies nach allgemeiner Auffassung nicht. Die gematik legt abstrakt fest, dass in beschriebenen Anwendungsfällen auf bestimmte Betriebssystemdienste auf eine bestimmte Art und Weise mit der E-Rezept-App zugegriffen werden kann. Zuschreibungsobjekt der Verantwortlichkeit ist jedoch eine konkrete Verarbeitung im Einzelfall. Über diese entscheidet aus den bereits genannten Gründen allein der Nutzer. Würde man eine Entscheidungsbefugnis (auch) der gematik annehmen, so würde dies die de-facto-Entscheidungsbefugnis des Nutzers in Frage stellen. Zugleich könnte dies dahingehend verstanden werden, dass die vom Nutzer getroffenen Entscheidungen vom Gesetzgeber nicht geteilt werden. Angesichts des Umstands, dass die gematik mit der E-Rezept-App einem gesetzlichen Auftrag nachkommt, entstünde dann ein widersprüchliches Bild. Denn der Gesetzgeber hat sich – daran besteht kein Zweifel – in Kenntnis der bekannten und zum Teil nicht unkritischen Datenverarbeitungspraktiken der Betriebssystemhersteller dazu entschieden, den Bürgern gleichwohl eine Smartphone-App anzubieten. Damit hat der Gesetzgeber in Ansehung der Realität zum Ausdruck gebracht, dass er die freie Entscheidung der Bürger zur Nutzung dieser Betriebssysteme und infolge zur Übernahme der damit verbundenen Datenschutzrisiken akzeptiert. Dann aber wäre es nicht verständlich, wenn die gesetzlich festgelegte App die übliche Verwendung der integralen Betriebssystemdienste unter Verweis auf die bekannten Datenschutzgründe ablehnt. Anders läge es wohl, wenn die damit verbundenen Nachteile für die User Experience, Gebrauchstauglichkeit und Sicherheit durch den Einsatz datenschutzfreundlicherer Alternativen kompensiert würden (im Sinne einer Vorbildfunktion) – dies ist allerdings wegen der von den Betriebssystemherstellern vorgegebenen Beschränkungen, die dem Gesetzgeber ebenfalls bekannt waren, nicht oder allenfalls in Ansätzen umsetzbar.

7.2.5 Verarbeitung durch das Apothekenverzeichnis

Der Apotheken-Verzeichnisdienst ist ein apothekenverwalteter Dienst in der Anwendungsinfrastruktur gemäß § 306 Abs. 2 Nr. 3 SGB V. Somit ist gemäß § 307 Abs. 4 SGB V der Anbieter des Apotheken-Verzeichnisdienstes für die durch ihn durchgeführte personenbezogene Datenverarbeitung verantwortlich.

7.2.6 Verarbeitung durch den E-Rezept-Fachdienst

Der E-Rezept-Fachdienst ist ein Dienst in der Anwendungsinfrastruktur gemäß § 306 Abs. 2 Nr. 3 SGB V. Die Verantwortlichkeit für die personenbezogene Datenverarbeitung durch diese Dienste hat der Gesetzgeber gesetzlich den jeweiligen Anbietern zugewiesen, § 307 Abs. 4 SGB V.

7.2.7 Verarbeitung durch den Identitätsdienst

Der Identitätsdienst wird zurzeit[96] ausschließlich für die Anwendung des E-Rezepts verwendet. Daher handelt es sich bei ihm – wie bei dem E-Rezept-Fachdienst – ebenfalls um einen Dienst in der Anwendungsinfrastruktur gemäß § 306 Abs. 2 Nr. 3 SGB V. Somit ist gemäß § 307 Abs. 4 SGB V der Anbieter des Identitätsdiensts für die durch ihn durchgeführte personenbezogene Datenverarbeitung verantwortlich.

7.2.8 Verarbeitung durch den Analysedienst

Datenschutzrechtlich ist zwischen der lokalen und der serverseitigen Verarbeitung von Analysedaten zu unterscheiden:

Die lokale Verarbeitung von Analysedaten durch die App auf dem Smartphone, die der eigentlichen Nutzungsanalyse vorgelagert ist, umfasst das Generieren und Löschen der Session-IDs, die Speicherung der zuvor vom Server des Analysedienstleisters abgerufenen Konfigurationsdatei für das SDK und die Protokollierung der von der gematik festgelegten Events sowie deren gebündelten Versand in Form von Batches an den API-Endpunkt des Load Balancers des Analysedienstleisters. Diese Verarbeitungsvorgänge unterfallen dem Anwendungsbereich des § 25 Abs. 1 S. 1 TTDSG, wonach die Speicherung von Informationen in der Endeinrichtung von Nutzern oder der Zugriff auf solche Informationen, die bereits in der Endeinrichtung gespeichert sind, nur mit Einwilligung zulässig sind.

Die serverseitige Verarbeitung umfasst die Speicherung der am Load Balancers empfangenen Analysedaten, die Anonymisierung der dabei anfallenden Zugriffsdaten, die Speicherung, Auswertung und Aufbereitung der anonymisierten Daten auf dem Analyseserver sowie schließlich die Bereitstellung der aufbereiteten Daten über das Web-Frontend. Für die bis zur Anonymisierung personenbezogene Verarbeitung durch den Load Balancer ist gemäß Art. 4 Nr. 7 DSGVO die gematik verantwortlich, da sie die Entscheidungen über die Durchführung und konkrete Konfiguration des Analysedienstes sowie die Auswahl und Beauftragung des Analysedienstleisters getroffen hat.

96 Der Identitätsdienst ist anwendungsneutral konzipiert, so dass er zukünftig auch für andere oder weitere Anwendungen der Telematikinfrastruktur eingesetzt werden kann. In diesem Fall wäre zu prüfen, ob der Identitätsdienst als für den Betrieb des gesicherten Netzes notwendiger Dienst nach § 306 Abs. 2 Nr. 2 b SGV V eingestuft werden muss.

7.3 Rechtsgrundlagen

Die Rechtmäßigkeit der Datenverarbeitung setzt voraus, dass die jeweilige Verarbeitung einen Zulässigkeitstatbestand erfüllt. Die entsprechenden Tatbestände ergeben sich in erster Linie aus Art. 6 DSGVO und – soweit Gesundheitsdaten verarbeitet werden – aus Art. 9 DSGVO.

7.3.1 Lokale Verarbeitung auf dem Smartphone

Für lokale Datenverarbeitungsvorgänge einschließlich der Übermittlung personenbezogener Daten an Dienste in der Anwendungsinfrastruktur (§ 306 Abs. 2 Nr. 3 SGB V) ist der Nutzer verantwortlich. Da er nicht zugleich Verantwortlicher und Betroffener zugleich sein kann, kann eine Verantwortlichkeit des Nutzers nur dort begründet werden, wo er die Daten anderer Personen verarbeitet. Gleichzeitig ist die Anwendung der DSGVO nach der sogenannten Haushaltsausnahme ausgeschlossen, wenn Daten ausschließlich zu persönlichen oder familiären Zwecken verarbeitet werden, Art. 2 Abs. 2 lit. c DSGVO. Eine Verantwortlichkeit des Nutzers kommt für die lokale Datenverarbeitung also nur in Betracht, wenn und soweit er personenbezogene Daten anderer zu anderen als zu persönlichen oder familiären Zwecken verarbeitet. Denkbar ist beispielsweise, dass ein Nutzer E-Rezepte unentgeltlich für eine Person, die nicht zu seinem familiären Umfeld zählt, einlöst oder diese Rezepte entgeltlich, beispielsweise im Rahmen von Unterstützungsleistungen, verwaltet.

Grundsätzlich können sich derartige Verarbeitungstätigkeiten auf eine Abrede zwischen Nutzern und Versicherten, deren Daten verarbeitet werden, stützen. Diese Abrede kann im Einzelfall den Charakter einer Einwilligung oder eines Vertrages annehmen. Rechtsgrundlage der Verarbeitung ist dann Art. 6 Abs. 1 S. 1 lit. a oder b DSGVO (Einwilligung oder Vertrag). Darüber hinaus kann die Datenverarbeitung aber auch im Sinne des Art. 6 Abs. 1 S. 1 lit. c DSGVO zur Erfüllung einer rechtlichen Verpflichtung erforderlich sein, beispielsweise wenn zwischen dem Nutzer und dem Versicherten kein Familienverhältnis, aber ein Betreuungs-, Pflege- oder Vormundschaftsverhältnis im Sinne des bürgerlichen Rechts besteht und sich aus diesem Verhältnis entsprechende Pflichten ergeben, Art. 6 Abs. 1 S. 1 lit. c, Abs. 3 S. 1 lit. b DSGVO i. V. m. § 22 Abs. 1 Nr. 1 lit. a BDSG.

Schließlich erscheint es denkbar, dass der Datenschutz im Einzelfall zurücktreten muss, um lebenswichtige Interessen der betroffenen Person zu schützen (Art. 6 Abs. 1 S. 1 lit. d DSGVO).

Allerdings dürfte es sich bei den personenbezogenen Daten anderer Personen, die auf dem Smartphone und im Verantwortlichkeitsbereich des Nutzers verarbeitet werden, regelmäßig um Gesundheitsdaten handeln, deren Verarbeitung den Einschränkungen des Art. 9 Abs. 2 DSGVO unterliegt. Als Grundlage für die lokale Verarbeitung von Gesundheitsdaten durch den Nutzer kommt vor allem Art. 9 Abs. 2 lit. a DSGVO (ausdrückliche Einwilligung) in Betracht. Eine Regelung, die mit Art. 6 Abs. 1 S. 1 lit. b DSGVO vergleichbare wäre, ist zwar für die Verarbeitung von Gesundheitsdaten nicht vorgesehen; allerdings kann eine solche Einwilligung durchaus im Zusammenhang mit einem Vertragsschluss erteilt werden. Ob die lokale Verarbeitung personenbezogener Gesundheitsdaten durch private Dienstleister darüber hinaus auch auf Grundlage der Art. 9 Abs. 2 lit. b oder h DSGVO i.V.m § 22 Abs. 1 Nr. 1 lit. a bzw. b BDSG gerechtfertigt werden kann, ist in der Literatur umstritten und kann im Rahmen dieser DSFA nicht abschließend geklärt werden. Nach wohl überwiegender Auffassung handelt es sich bei Art. 9 Abs. 2 lit. b DSGVO i. V. m. § 22 Abs. 1 Nr. 1 a BDSG um eine Verweisungskette, die in die Sozialgesetzbücher verweist; nach zumindest teilweise vertretener Auffassung soll § 22 Abs. 1 Nr. 1 lit. a BDSG jedoch eigenständige Bedeutung im Bereich der Datenverarbeitung durch nichtöffentliche Stellen wie soziale Selbsthilfeorganisationen oder Stiftungen zukommen.[97] Entsprechendes gilt für § 22 Abs. 1 Nr. 1 lit. b BDSG. Nach einer Auffassung ist der Anwendungsbereich dieser Unterausnahme denkbar weit. Erfasst sein soll nahezu jede Dienstleistung im Gesundheits- oder Sozialbereich von der Physiotherapie bis hin zur kosmetischen Behandlung.[98] Nach der Gegenauffassung muss die begriffliche Weite der Norm durch Auslegung

97 Taeger/Gabel/Rose, 4. Aufl. 2022, BDSG § 22 Rn. 20.

98 Nachweise bei Taeger/Gabel/Rose, 4. Aufl. 2022, BDSG § 22 Rn. 26.

eingeschränkt werden, etwa dahingehend, dass man nur solche Dienstleistungen als „Versorgung oder Behandlung im Gesundheits- oder Sozialbereich“ gelten lässt, die von öffentlichen Leistungsträgern[99] oder im Umfeld medizinischer Leistungen[100] erbracht werden.

7.3.2 Verarbeitung durch Betriebssystemdienste

Der jeweilige Verantwortliche muss die Zulässigkeit der Verarbeitung durch die Betriebssystemdienste durch Auswahl einer geeigneten Rechtsgrundlage selbst sicherstellen.[101] Im Übrigen gelten die Ausführungen unter 7.3.1 entsprechend.

Die Rechtsgrundlagen für die verschiedenen Verarbeitungsvorgänge durch Betriebssystemdienste hängt maßgeblich vom Inhalt des Nutzungsverhältnisses zwischen Hersteller und Nutzer und der konkreten Nutzungsart ab, die nicht Gegenstand dieser DSFA sind.

7.3.3 Verarbeitung durch das Apothekenverzeichnis

Rechtsgrundlage für die personenbezogene Datenverarbeitung durch den Anbieter des Apothekenverzeichnisses ist Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 307 Abs. 4 S. 1 SGB V. Die Datenverarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt, nämlich die Ermöglichung der Nutzung eines Dienstes für die E-Rezept-Anwendung in der Anwendungsinfrastruktur nach Maßgabe der von der gematik festgelegten Spezifikationen.

7.3.4 Verarbeitung durch den E-Rezept-Fachdienst

Die Rechtsgrundlage für die personenbezogene Datenverarbeitung durch den Anbieter des E-Rezept-Fachdienstes ist Art. 6 Abs. 1 lit. e und lit. c, Abs. 3 S. 1 lit. b, 9 Abs. 2 lit. h DSGVO i. V. m. § 307 Abs. 4 S. 1 SGB V. Die Verarbeitung ist für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich, nämlich die Ermöglichung der Nutzung eines Dienstes für die E-Rezept-Anwendung in der Anwendungsinfrastruktur nach Maßgabe der von der gematik festgelegten Spezifikationen.

7.3.5 Verarbeitung durch den Identitätsdienst

Rechtsgrundlage für die personenbezogene Datenverarbeitung durch den Anbieter des Identitätsdienstes ist Art. 6 Abs. 1 lit. e DSGVO i. V. m. § 307 Abs. 4 S. 1 SGB V. Die Verarbeitung ist für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich, nämlich die Ermöglichung der Nutzung eines Dienstes für die E-Rezept-Anwendung in der Anwendungsinfrastruktur nach Maßgabe der von der gematik festgelegten Spezifikationen.

99 Kühling/Buchner/Weichert, 3. Aufl. 2020, DSGVO Art. 9 Rn. 115.

100 Taeger/Gabel/Rose, 4. Aufl. 2022, BDSG § 22 Rn. 28.

101 Die Hersteller geben in ihren Datenschutzbestimmungen überwiegend die Erforderlichkeit zur Vertragsdurchführung (Art. 6 Abs. 1 lit. b DSGVO) und/oder eine Einwilligung des Nutzers als Rechtsgrundlage für die Verarbeitung personenbezogener Daten des Nutzers an.

7.3.6 Verarbeitungsvorgänge der Nutzungsanalyse

Für die Verarbeitungsvorgänge im Rahmen der Nutzungsanalyse ist die Rechtsgrundlage die in der App erteilte Einwilligung des Nutzers gemäß Art. 6 Abs. 1 lit. a DSGVO.

7.4 Pflichten des Verantwortlichen und Rechte der Betroffenen

Die DSGVO und die mitgliedsstaatlichen Datenschutzgesetze knüpfen verschiedene Rechte und Pflichten an unterschiedliche Rollen, die im Zusammenhang mit einer konkreten Verarbeitungstätigkeit stehen. Zu den Pflichten des Verantwortlichen gehört beispielsweise die Gewährleistung der Grundsätze aus Art. 5ff. DSGVO. Umgekehrt stehen der betroffenen Person gegenüber dem Verantwortlichen sogenannte Betroffenenrechte zu.

Zu den Pflichten des Verantwortlichen zählt insbesondere, dass

- Speicherfristen angemessen begrenzt (Art. 5 Abs. 1 lit. e DSGVO),
- betroffene Personen umfassend informiert werden (Art. 12ff. DSGVO),
- das Verhältnis zu involvierten Auftragsverarbeitern geklärt wurde (Art. 28 DSGVO) und
- Garantien in Bezug auf Drittlandtransfers eingehalten werden (Art. 44 ff. DSGVO).[102]

Die Rechten der Betroffenen beinhalten demgegenüber insbesondere die die Rechte aus Art. 15 ff. DSGVO. Außerdem kann die betroffene Person ihre Einwilligung jederzeit frei widerrufen, Art. 7 Abs. 3 S. 1 DSGVO.

7.4.1 Begrenzung der Speicherfrist

Nach Art. 5 Abs. 1 lit. e DSGVO dürfen personenbezogene Daten nur so lange verarbeitet werden, wie es für die Zweckerreichung erforderlich ist oder eine gesetzliche Verpflichtung zur Aufbewahrung oder Archivierung besteht. Unabhängig von der gesetzlichen Pflicht zur Aufbewahrung und Löschung haben Nutzer der E-Rezept-App verschiedene Möglichkeiten, die App und bestimmte Daten, die im Zusammenhang mit der App-Nutzung verarbeitet werden, **manuell** zu löschen. Der Nutzer kann beispielsweise

- seine E-Rezept-Installation löschen. Löscht er die App auf die vom Hersteller des Betriebssystems vorgesehene Weise, so werden alle von der App lokal gespeicherten Daten gelöscht.
- lokale Kopien von E-Rezepten jederzeit löschen, auch wenn die App nicht am E-Rezept-Fachdienst angemeldet ist. Ist die App angemeldet, können per App auch die auf dem E-Rezept-Fachdienst gespeicherten E-Rezepte gelöscht werden, solange sie nicht den Rezeptstatus „in Abgabe (gesperrt)“ haben. Wenn der Nutzer auf dem E-Rezept-Fachdienst ein E-Rezept löscht und angemeldet ist, wird auch eine etwaig gespeicherte lokale Kopie gelöscht.[103]
- verschickte Kommunikationsnachrichten als Absender löschen, wenn diese Nachrichten vom Empfänger noch nicht abgerufen wurden.[104]

102 Taeger/Gabel/Reibach, 4. Aufl. 2022, DS-GVO Art. 35 Rn. 37.

103 gemSpec_eRp_FdV_V1.1.0, S. 41f.

104 gemSpec_FD_eRp_V1, S. 51.

Aufgrund der gesetzlich angeordneten dreijährigen Speicherfrist (§ 309 Abs. 1 SGB V) kann der Nutzer die Protokolleinträge auf dem E-Rezept-Fachdienst nicht per App löschen lassen. Bestimmte Daten werden zudem **automatisch** gelöscht:

- Lokale Kopien von Fach- und Authentifizierungsdaten in der App werden – mit Ausnahme von lokal gespeicherten Rezeptcodes – mit der Abmeldung des Nutzers vom E-Rezept-Fachdienst gelöscht.
- Zugriffsdaten wie die IP-Adresse des Nutzers werden durch die Anbieter des E-Rezept-Fachdienstes, des Identitätsdienstes und des Apotheken-Verzeichnisdienstes nur für die Dauer des jeweiligen Zugriffsvorgangs gespeichert und anschließend gelöscht bzw. anonymisiert.
- Bei aktivierter Nutzungsanalyse generiert das SDK bei jedem Start eine neue zufällige Session-ID. Die alte Session-ID wird beim Ende der Session gelöscht. Unmittelbar nach Beendigung des jeweiligen Übertragungsvorgangs und vor der Weiterleitung an die Analyseanwendung löscht der Load Balancer die IP-Adresse des Nutzers aus seinem Arbeitsspeicher.
- Veraltete E-Rezepte, Medikament-Informationen, Protokolleinträge und Nachrichten auf dem E-Rezept-Fachdienst werden automatisch gemäß den gesetzlichen Löschfristen gelöscht. Die Löschfristen betragen nach dem Statuswechsel auf „quittiert“ oder „in Abgabe (gesperrt)“ 100 Tage, § 360 Abs. 11 SGB V.[105]

Weiterführende Informationen zur Begrenzung der Speicherdauer finden sich in den Datenschutzinformationen der jeweils für eine Verarbeitung Verantwortlichen.

7.4.2 Informationsrechte

Gemäß Art. 12 ff. DSGVO muss der Verantwortliche der betroffenen Person alle nach Maßgabe des Gesetzes erforderlichen Informationen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln. Die gematik erfüllt diese Pflicht hinsichtlich ihrer Verantwortlichkeit für die Verarbeitung personenbezogener Daten im Rahmen der Verarbeitungstätigkeit 8 (Nutzungsanalyse) durch die Datenschutzerklärung der E-Rezept-App. Die Datenschutzerklärung wird auch auf der Website und in den App-Stores bereitgestellt und erhält weitere allgemeine Informationen zur TI sowie dem E-Rezept-System.

Zudem plant die gematik die Veröffentlichung dieses DSFA-Berichts, der die betroffenen Personen detailliert über die relevanten Verarbeitungsvorgänge, die damit verbundenen Pflichten und ihre Rechte informiert.

Weiterhin hat der Gesetzgeber gesetzliche Informationspflichten verschiedenen Akteure der TI festgelegt, die ebenfalls Informationen im Zusammenhang mit dem E-Rezept enthalten:

- § 291 SGB V verpflichtet die Krankenkassen zur Information der Versicherten spätestens bei der Versendung der eGK in allgemein verständlicher, barrierefreier Form über die Funktionsweise der elektronischen Gesundheitskarte und über die Art der personenbezogenen Daten, die nach § 291a SGB V mittels der eGK zu verarbeiten sind.
- § 314 SGB V verpflichtet die gematik, auf ihrer Internetseite Informationen über die Telematikinfrastruktur sowie die Verantwortlichkeiten der beteiligten Akteure für die Versicherten in präziser, transparenter, verständlicher, leicht zugänglicher und barrierefreier Form zur Verfügung zu stellen.[106] Diese Informationen enthalten auch Angaben zur E-Rezept-Anwendung.
- Die gematik ist gemäß § 307 Abs. 5 SGB V verpflichtet, für die betroffenen Personen eine koordinierende Stelle einzurichten. Die koordinierende Stelle erteilt den Betroffenen allgemeine Informationen zur TI sowie Auskunft über Zuständigkeiten innerhalb der TI, insbesondere zu den datenschutzrechtlichen Verantwortlichkeiten. Die gematik ist dieser Pflicht durch die Einrichtung des Datenschutzlotsen (https://www.gematik.de/datensicherheit/datenschutzlotse) nachgekommen.

105 Siehe auch gemSpec_FD_eRp_V1, S. 23.

106 https://www.gematik.de/media/gematik/Medien/Rechtliche_Hinweise/Informationspflicht___314_OF.pdf (zuletzt aufgerufen am 15.12.2022).

› § 343 SGB V verpflichtet Krankenkassen, umfassendes, geeignetes Informationsmaterial über die elektronische Patientenakte in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und barrierefrei zur Verfügung zu stellen. Zur Unterstützung der Informationspflichten der Krankenkassen nach § 343 SGB V hat der Spitzenverband Bund der Krankenkassen im Einvernehmen mit dem BfDI geeignetes Informationsmaterial, auch in elektronischer Form, zu erstellen und den Krankenkassen zur verbindlichen Nutzung zur Verfügung zu stellen. Diese Informationen enthalten in der Regel auch Informationen zur Funktionsweise der TI und der Rolle der gematik.

Soweit Leistungserbringer die E-Rezept-Anwendung nutzen, um E-Rezepte auszustellen oder einzulösen, sind sie grundsätzlich ebenfalls gemäß Art. 12 ff. DSGVO zur Erteilung von Informationen mit Bezug zur E-Rezept-Anwendung verpflichtet.

7.4.3 Verhältnis zu Auftragsverarbeitern

Die gematik und die Anbieter der für die E-Rezept-Anwendung relevanten Dienste sind als Verantwortliche bei der Einschaltung von Subunternehmern jeweils zum Abschluss eines Auftragsverarbeitungsvertrags nach Art. 28 DSGVO verpflichtet. Dabei müssen die Anbieter neben den allgemeinen Anforderungen an eine Auftragsverarbeitung auch die von der gematik spezifizierten Datenschutz- und Sicherheitsanforderungen für Anbieter[107] beachten. Nach dem in den Spezifikationen festgelegten Modularisierungskonzept müssen die Anbieter der gematik jährlich TI-Datenschutzberichte mit ausführlichen Angaben zu den eingesetzten Subunternehmern vorzulegen. Zudem sind die Anbieter verpflichtet, beim Abschluss von Auftragsverarbeitungsverträgen alle Vereinbarungen mit dem Subunternehmern zu treffen, die für die Einhaltung der von der gematik spezifizierten Datenschutzanforderungen notwendig sind. Dies erfordert auch Vereinbarungen, die den Anbietern und der gematik mindestens jährliche Kontrollen bei ihren Subunternehmern ermöglichen.

7.4.4 Drittlandübermittlung

Nach den übergreifenden Spezifikationen für Anbieter von TI-Anwendungen müssen diese sicherstellen, dass sich die Betriebsumgebungen der mittels der TI erreichbaren Dienste auf dem Gebiet eines Mitgliedstaates der EU bzw. des EWR befindet/befinden.[108] Eine Drittlandübermittlung durch die Komponenten und Dienste des E-Rezept-Systems ist daher nicht vorgesehen bzw. wird durch die jeweiligen Spezifikationen ausgeschlossen.

Hinsichtlich der Nutzungsanalyse ist es dem von der gematik beauftragten Analytics-Dienstleister gestattet, die Infrastruktur des Cloud-Anbieters AWS zur Verarbeitung personenbezogener Daten der Nutzer einzusetzen. Es besteht insoweit das Risiko, dass AWS von in einem Drittland (z. B. USA) ansässigen Behörden zur Offenlegung von Daten verpflichtet wird. Zudem besteht – wie grundsätzlich bei jeder Einschaltung von Auftragsverarbeitern – das Risiko, dass der Auftragsverarbeiter die im Auftrag verarbeiteten Daten selbst verarbeitet. Die Erlaubnis der gematik zum Einsatz von AWS-Services steht daher unter der Bedingung, dass ausschließlich die Server in der AWS-Region Europa bzw. ausschließlich solche AWS-Dienste, die nur mit Servern in der AWS-Region Europa bereitgestellt werden können, eingesetzt werden. Da der Personenbezug der im Rahmen der Nutzungsanalyse an den Analytics-Dienstleister übermittelten Daten nur für die kurze Dauer einer einzelnen Session auf dem Load Balancer in Irland besteht und eine persistente Speicherung der Analysedaten auf dem Analyseserver in anonymisierter Form erfolgt (vgl. 7.1.1.6), kann aus Sicht der gematik hinreichend ausgeschlossen werden, dass per Fernzugriff aus einem Drittland durch AWS-Mitarbeiter oder Behörden auf die im Arbeitsspeicher des Load Balancers flüchtig verarbeiteten (noch) personenbezogenen Zugriffs- und Analysedaten der Nutzer zugegriffen und damit ein Personenbezug hergestellt wird. Soweit aus einem Drittland auf die im Analyse- oder Backupserver persistent gespeicherten (aggregierten) Analysedaten zugegriffen werden sollte, handelt es sich um anonyme Daten, die per definitionem keinen Personenbezug aufweisen (vgl. 7.1.1.6).

107 gemSpec_DS_Anbieter_V1, S. 12.

108 gemSpec_DS_Anbieter_V1, S. 12.

7.4.5 Widerrufsrecht

Gemäß Art. 7 Abs. 3 DSGVO muss eine Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden können. Personenbezogenen Daten, die auf Grundlage einer Einwilligung verarbeitet wurden, sind nach Art. 17 Abs. 1 lit. b DSGVO grundsätzlich zu löschen, sobald die entsprechende Einwilligung widerrufen wird.

Zum Widerruf der Einwilligung in die Nutzungsanalyse können Nutzer die Funktion innerhalb der E-Rezept-App deaktivieren, die App zurücksetzen oder löschen. Wird die Installation des Nutzers auf die vom Hersteller des Betriebssystems vorgesehene Weise gelöscht oder zurückgesetzt, werden alle von der App lokal gespeicherten Daten gelöscht. Dies schließt auch etwaige Kopien seiner Session-ID oder IP-Adresse ein. Da der Personenbezug der Analyse- und Zugriffsdaten mit Löschung dieser Daten entfällt, sind in diesem Fall keine weiteren Daten zu löschen. Deaktiviert der Nutzer die Funktion innerhalb der E-Rezept-App wird die aktuelle Session-ID gelöscht und nicht mehr an den API-Endpunkt des Analysedienstes übertragen.

7.4.6 Widerspruchsrecht

Gemäß Art. 21 Abs. 1 S. 1 HS. 1 DSGVO hat die betroffene Person das Recht, jederzeit gegen eine Verarbeitung ihrer personenbezogener Daten Widerspruch einzulegen, wenn diese Datenverarbeitung für die Wahrnehmung einer Aufgabe erfolgt, die im öffentlichen Interesse liegt, oder zur Wahrung berechtigter Interessen erforderlich ist (Art. 6 Abs. 1 S. 1 lit. e oder f DSGVO).

Das Widerspruchsrecht gegenüber einer öffentlichen Stelle ist jedoch nach § 36 BDSG ausgeschlossen („besteht nicht“), soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht. Dass ein solches Interesse hier vorliegt, macht die Gesetzesbegründung an verschiedenen Stellen hinreichend deutlich. Dort wird beispielsweise ausgeführt, dass der sichere Betrieb der TI ein „überragend wichtiges Ziel des allgemeinen öffentlichen Interesses der Bundesrepublik Deutschland“ darstelle; auch im Zusammenhang mit der Verarbeitung von Forschungsdaten ist die Rede vom „allgemeinen öffentlichen Interesses der Bundesrepublik Deutschland an einer auf wissenschaftlicher Evidenz basierenden medizinischen Versorgung der Bevölkerung“.[109]

109 BT-Drs. 19/18793, S. 101f., 131, 132.

8 Bewertung der Notwendigkeit und Verhältnismäßigkeit

Die Verarbeitung von personenbezogenen Daten muss in Anbetracht des jeweils verfolgten Zwecks notwendig und verhältnismäßig sein. Notwendigkeit setzt dabei voraus, dass die Verarbeitung für die vollständige und rechtmäßige Erreichung des jeweils verfolgten Zwecks erforderlich ist, die Verhältnismäßigkeit der Verarbeitung – dass es keine alternativen und datenschutzrechtlich weniger eingreifenden Verarbeitungsformen gibt, um den jeweils verfolgten Zweck mit gleicher Wirksamkeit zu erreichen.

Die Notwendigkeit und Verhältnismäßigkeit der einzelnen Verarbeitungsvorgänge setzen voraus, dass sie hinsichtlich der verarbeiteten personenbezogenen Daten

- einem legitimen Zweck dienen,
- zur Erreichung dieses Zwecks geeignet, d. h. förderlich sind,
- erforderlich sind, d. h. es darf kein milderes (datenschutzfreundlicheres), gleichsam effektives Mittel zur Verfügung stehen, um den Zweck zu erreichen, und
- angemessen sind, d. h. die Verarbeitungstätigkeit steht nicht außer Verhältnis zum verfolgten Zweck.

8.1 Legitimer Zweck

Der Gesetzgeber hat die gematik damit beauftragt, eine sichere Zugriffskomponente für Versicherte zu entwickeln und bereitzustellen, um E-Rezepte elektronisch nutzen zu können. Im Rahmen dieses Auftrags hat er bestimmte Vorgaben gemacht, die – neben konkreten funktionalen und technischen Aspekten – auch die allgemeine Pflicht der gematik zur Wahrung der Interessen der Patienten sowie die Sicherstellung der Einhaltung der Vorschriften zur Barrierefreiheit beinhalten, § 311 Abs. 4 SGB V.[110] Ausweislich der Gesetzgebungsmaterialien bezweckt der Gesetzgeber damit vor allem, die Digitalisierung des deutschen Gesundheitswesens weiter voranzutreiben. Die Digitalisierung wird als wichtige Chance gesehen, die Versorgungs- und Behandlungsqualität sowie die Zugänglichkeit von Gesundheitsleistungen flächendeckend zu gewährleisten und zu verbessern. In der einschlägigen Gesetzesbegründung heißt es dementsprechend, der sichere Betrieb der TI stelle ein überragend wichtiges Ziel des allgemeinen öffentlichen Interesses der Bundesrepublik Deutschland dar; die Effizienzgewinne durch die Digitalisierung des Gesundheitswesens, insbesondere durch die sichere Vernetzung aller Akteure mittels der TI, sei angesichts der Herausforderungen durch den demographischen Wandel, der Zunahme der Anzahl chronisch Kranker, des Fachkräftemangels, sowie der Unterversorgung in strukturschwachen Regionen für die Sicherung des

110 Vgl. oben unter 4.4.

Niveaus der Gesundheitsversorgung schlechthin unverzichtbar.[111] Die Digitalisierung des Gesundheitswesens stellt damit das übergeordnete gesetzgeberische Ziel dar. Sie dient der öffentlichen Gesundheit und ist daher legitim.

Die gematik bezweckt mit den Verarbeitungstätigkeiten, die sie im Zusammenhang mit dem Prüfgegenstand verantwortet, Versicherten eine Zugriffskomponente für die elektronische Nutzung von E-Rezepten nach Maßgabe der eben skizzierten Vorgaben bereitzustellen. Dieser Zweck ist vom übergeordneten Zweck der öffentlichen Gesundheitsfürsorge mitumfasst. Die Entwicklung und Bereitstellung der E-Rezept-App entsprechend der gesetzlichen Vorgaben, dient ebenfalls der öffentlichen Gesundheitsfürsorge und ist daher ebenfalls legitim.[112]

8.2 Geeignetheit

Die gematik entwickelt eine native App für Smartphones mit iOS-, Android- und EMUI-Betriebssystem, um den legitimen Zweck zu erfüllen, Versicherten eine Zugriffskomponente für die elektronische Nutzung von E-Rezepten nach Maßgabe der gesetzlichen Vorgaben bereitzustellen. Die Entwicklung einer solchen App ist zur Zweckerreichung geeignet; die Geeignetheit einer nativen App wäre allenfalls dann zu verneinen, wenn ihr Funktionsumfang es Versicherten nicht erlauben würde, E-Rezepte elektronisch einzulösen, die Bereitstellung als native App die gesetzlichen Anforderungen an den Datenschutz und die Sicherheit der Zugriffskomponente nicht erfüllen würde oder aber im Widerspruch zu den Interessen der Patienten stünde. So liegt der Fall hier jedoch nicht.

8.2.1 Funktionsumfang der App

Nach einer umfassenden Analyse der gesetzlichen Anforderungen und der technischen Gestaltungsspielräume einer nativen App für die oben genannten mobilen Betriebssysteme wird davon ausgegangen, dass die während der DSFA-Durchführung verfügbare oder geplante Version der E-Rezept-App so gestaltet werden kann, dass sämtliche vom Gesetzgeber festgelegten funktionalen Anforderungen an die Zugriffskomponente erfüllt werden. Insbesondere kann die App von den Versicherten genutzt werden, um über eine sichere Internetverbindung auf den E-Rezept-Fachdienst zuzugreifen und von dort E-Rezepte herunterzuladen, anzuzeigen, „eigenständig“ zu löschen (§ 337 Abs. 2 SGB V) und elektronisch in einer Apotheke einzulösen (§ 311 Abs. 1 Nr. 10 SGB V). Die Internetverbindung ermöglicht auch den Zugriff auf die Informationen des Nationalen Gesundheitsportals nach § 395 SGB V sowie die Verknüpfung dieser Informationen mit Daten, die in einem E-Rezept gespeichert sind (§ 360 Abs. 12 Nr. 1 SGB V). Die App enthält damit alle Funktionen, die der Versicherte für den Abruf, die Speicherung sowie die Einlösung von E-Rezepten auf elektronischem Wege benötigt. Alle Funktionen der App stehen in einem direkten Zusammenhang mit der elektronischen Einlösung von E-Rezepten und erleichtern den Umgang mit diesen.

8.2.2 Bereitstellung als native App

Einer nativen App werden von den Betriebssystemherstellern sehr umfangreiche Möglichkeiten für den Zugriff auf standardisierte Betriebssystemdienste beispielsweise für die Verwendung der bereits in vielen Smartphones integrierten NFC-Schnittstelle eingeräumt. So kann der Anspruch der Versicherten realisiert werden, auf Daten im E-Rezept-Fachdienst mittels eGK bzw. eines geeigneten technischen Verfahrens, das einen hohen Sicherheitsstandard zur Authentifizierung gewährleistet, zuzugreifen (§ 336 Abs. 1

111 Vgl. BT-Drucks. 19/18793, S. 101f.

112 Vgl. BT-Drucks. 19/18793, S. 128f.

bzw. 4 SGB V). Darüber hinaus kann eine native App die mittlerweile in nahezu allen Smartphones integrierte Kamera durch die Betriebssystemdienste verwenden. Dadurch wird den Versicherten ermöglicht, die Rezeptcodes, die für den Zugriff auf ihre E-Rezepte erforderlich sind, auch dann einzugeben, wenn die Zugangsdaten in Papierform bereitgestellt werden (§ 360 Abs. 9 S. 1 SGB V).[113]

Weiterhin verfügen moderne mobile Betriebssysteme und Smartphones heute über zahlreiche Sicherheitseigenschaften, die nativen Apps die sichere Nutzung und Speicherung von Daten ermöglicht. Beispielsweise besteht für native Apps die Möglichkeit der getrennten und verschlüsselten Datenspeicherung, so dass auch die elektronische Nutzung von E-Rezepten vor Ort und ohne Internetverbindung erfolgen kann. Dass die Bereitstellung der Zugriffskomponente als native App prinzipiell geeignet ist, um die konkreten Sicherheitsanforderungen an die Zugriffskomponente zu erfüllen, ergibt sich aus dem vom BSI bestätigten Produktgutachten für die E-Rezept-App, auf das hier Bezug genommen wird.

8.2.3 Wahrung der Patienteninteressen

Die Entwicklung und Bereitstellung einer Zugriffskomponente für Versicherte zur elektronischen Nutzung und Verwaltung von E-Rezepten muss den heterogenen Interessen von Patienten größtmöglich Rechnung tragen. Sie muss insbesondere die Datensouveränität der Patienten achten, ihr Recht auf freie Apothekenwahl realisieren sowie die einfache Zugänglichkeit und leichte Verfügbarkeit der Zugriffskomponente möglichst umfassend gewährleisten.

Das Recht auf **Datensouveränität** wird durch die E-Rezept-App gefördert, da sie die Nutzung von E-Rezepten sowohl in elektronischer als auch in ausgedruckter Form (Rezeptcode) ermöglicht. Somit kann sich auch ein Patient, der sein E-Rezept in ausgedruckter Form erhalten hat, nachträglich zur elektronischen Einlösung entscheiden und damit seine zuvor getroffene Wahl eigenständig ändern. Weiterhin verfügt die E-Rezept-App über Funktionen für die Einsichtnahme in Zugriffsprotokolle und ermöglicht das eigenständige Löschen von E-Rezepten. Als native App verfügt die E-Rezept-App naturgemäß über eine Benutzeroberfläche, die den Versicherten das Auslesen von Protokolldaten und Fachdaten im E-Rezept-Fachdienst (§ 312 Abs. 6 SGB V) ermöglicht. Durch die Möglichkeit, mehrere Profile einzurichten, besteht außerdem die Möglichkeit, als Vertreter beispielsweise für Angehörige auf den E-Rezept-Fachdienst zuzugreifen.

Das Recht auf **freie Apothekenwahl** wird entsprechend den gesetzlichen Vorgaben (§ 31 Abs. 1 S. 6 SGB V) durch die konkrete Gestaltung der Apothekensuche in der E-Rezept-App gewährleistet. Die angebotenen Filterkriterien werden von der App abschließend vorgegeben und beschränken sich auf solche, die eine Bevorzugung einzelner Apotheken aus Gründen, die nicht im Interesse des Patienten liegen, unwahrscheinlich erscheinen lassen. Die Apothekendaten werden von den Apotheken selbst auf einem gesonderten Serversystem in standardisierter Form bereitgestellt und gepflegt, so dass eine Einflussnahme der gematik auf den Inhalt der Apothekendaten ausgeschlossen ist. Die App präsentiert die vollständigen vom Apotheken-Verzeichnisdienst zurückgelieferten Suchergebnisse und sortiert sie nach üblichen, transparenten Kriterien (alphabetisch oder nach Entfernung). Die App verfügt auch nicht über Funktionen, mit denen die Versicherten neue E-Rezepte direkt an eine bestimmte, vorab ausgewählte Apotheke zuweisen können oder dies durch Dritte vornehmen lassen können.

Der kostenlose Vertrieb der E-Rezept-App auch über die gängigen App-Stores fördert die niedrigschwellige **Zugänglichkeit** und **Verfügbarkeit** der Zugriffskomponente. Er ermöglicht den meisten Versicherten, die über ein Smartphone verfügen, die einfache Installation der App.

113 Vgl. BT-Drs. 19/18793, S. 128. Dass für den Zugriff auf E-Rezepte im E-Rezept-Fachdienst „Zugangsdaten“ benötigt werden, wird von den gesetzlichen Regelungen nicht ausdrücklich festgelegt, sondern von § 260 Abs. 9 SGB V vorausgesetzt.

8.2.4 Digitale Barrierefreiheit

Die E-Rezept-App ermöglicht aufgrund ihrer Gestaltung als native App ebenso wie der Vertrieb auch über die betriebssystemspezifischen App-Stores die Nutzung von speziellen Funktionen und Betriebssystemdiensten (sogenannte Bedienungshilfen), mit denen die Zugänglichkeit und Nutzung der Zugriffskomponente für Versicherte mit bestimmten Behinderungen barrierefreier gestaltet werden kann. Es wird daher davon ausgegangen, dass die Umsetzung als native App geeignet ist, die Anforderungen an die Barrierefreiheit zu erfüllen.[114]

8.2.5 Optionale Nutzungsanalyse

Die E-Rezept-App enthält eine Funktion zur Aktivierung der Nutzungsanalyse. Diese Funktion ist für den Nutzer optional und standardmäßig deaktiviert. Aktiviert der Nutzer die Nutzungsanalyse, erhält die gematik Analysedaten zum Nutzungsverhalten während einer zusammenhängenden Session. Diese Analysedaten werden in anonymisierter Form ausgewertet und geben Auskunft über potentielle technische Fehler, Optimierungspotenziale in Bezug auf die Usability sowie über die technische Ausstattung der Nutzer. Anhand dieser Erkenntnisse kann die gematik Änderungen an der App vornehmen, um die Häufigkeit von Fehlern zu reduzieren und sie allgemein bedarfsgerechter zu gestalten. Dadurch kann die Nutzbarkeit der App für möglichst viele Nutzergruppen erleichtert und an sich wandelnde Nutzungsgewohnheiten sukzessive angepasst werden, wodurch die Eigenständigkeit und Datensouveränität der Versicherten gefördert werden. Somit eignet sich die Nutzungsanalyse zur Verbesserung der Verfügbarkeit, Vertraulichkeit und allgemeinen Nutzbarkeit der App (Usability) und damit zur Bereitstellung einer sicheren Zugriffskomponente, die von möglichst vielen Versicherten mit einem dem Schutzbedarf der verarbeiteten Daten entsprechenden Datenschutzniveau angemessen genutzt werden kann.

114 Vgl. BFIT-Bund, Handreichung „Barrierefreie mobile Apps“, Version 1.3, Kap. Entwicklungsansätze für mobile Apps. Es ist dabei anzumerken, dass der Gesetzgeber bislang keine konkreten Kriterien für die Bewertung der Barrierefreiheit von Apps vorgegeben hat.

8.3 Erforderlichkeit

Die Entwicklung einer nativen App für Smartphones mit den genannten Betriebssystemen ist auch erforderlich, um Versicherten eine Zugriffskomponente für die elektronische Nutzung von E-Rezepten nach Maßgabe der gesetzlichen Vorgaben bereitzustellen. Dies gilt zunächst für die Bereitstellung der App an und für sich, darüber hinaus aber auch für die Verarbeitungsvorgänge, die durch Nutzung einer nativen App erst ermöglicht werden: die Datenverarbeitung durch Betriebssystemdienste und die Speicherung von Daten auf dem Endgerät des Nutzers. In allen drei Fällen sind datenschutzfreundlichere Mittel zwar prinzipiell denkbar, aber nicht gleich wirksam bei der Umsetzung der gesetzlichen Vorgaben.

8.3.1 Alternativen zur Bereitstellung als native App

Es wird davon ausgegangen, dass die Bereitstellung der Zugriffskomponente in Form einer nativen App nicht nur geeignet, sondern auch erforderlich für die Erreichung des oben genannten Zwecks ist.[115]

Eine Zugriffskomponente könnte zwar prinzipiell auch als Web-Anwendung (also als Website, die im stationären und/oder mobilen Webbrowser angezeigt wird) oder als Anwendung für stationäre PCs bereitgestellt werden. Eine solche alternative Umsetzung wäre jedoch aus mehreren Gründen nicht gleichwertig mit der Umsetzung als native App.

Eine Bereitstellung als rein stationäre Anwendung schließt die mobile Nutzung aus, wohingegen eine native App sowohl im häuslichen Bereich als auch von unterwegs genutzt werden kann. Dies ermöglicht beispielsweise die im Versichertenalltag praktisch bedeutsame Einlösung von E-Rezepten etwa direkt nach einem Arztbesuch bzw. vor dem Aufsuchen einer Apotheke. Insofern ist die Bereitstellung der Zugriffskomponente als native App einer stationären Lösung im Hinblick auf den verfolgten Zweck deutlich überlegen.

Eine Umsetzung als Web-Anwendung wäre sowohl für stationäre als auch mobile Anwendungsfälle möglich, da sowohl stationäre Endgeräte als auch Smartphones typischerweise über einen Webbrowser verfügen. Dies würde die Nutzung der Zugriffskomponente unabhängig von der Verwendung eines bestimmten Betriebssystems oder eines persönlichen Benutzerkontos für einen App-Store ermöglichen, so dass der Versicherte eine von ihm nicht gewollte Datenübermittlung an Apple, Google oder Huawei verhindern könnte. Der Funktionsumfang einer solchen Web-Anwendung wäre gegenüber einer nativen App jedoch deutlich reduziert. So verfügt eine Web-Anwendung nicht über die Möglichkeit zur sicheren lokalen Speicherung von E-Rezepten und Zugangsdaten auf dem Gerät, stattdessen übernimmt der jeweils genutzte Webbrowser die Datenverwaltung. Damit wäre eine Web-Anwendung nicht geeignet, um eine sichere elektronische Einlösung von E-Rezepten ohne Internetverbindung vor Ort in einer Apotheke zu ermöglichen (vgl. § 311 Abs. 1 Nr. 10 SGB V).

Für die Verwaltung der Zugangsdaten mehrerer Versicherter auf dem gleichen Gerät wäre zudem eine Cloud-basierte Kontoverwaltung erforderlich, was eine Speicherung von personenbezogenen Daten auf einem Server sowie die Notwendigkeit einer Internetverbindung zur Folge hätte.

Weiterhin könnte die gesetzlich angeordnete Authentifizierung mittels der NFC-fähigen eGK nicht realisiert werden, da der Zugriff auf die NFC-Betriebssystemdienste derzeit nur für native Apps angeboten wird. Auch eine Kommunikation mit Apotheken und die zuverlässige Benachrichtigung über neue E-Rezepte, Mitteilungen oder Statusänderungen könnte mit einer Web-Anwendung aufgrund deren fehlender Fähigkeit zum Hintergrundbetrieb nicht realisiert werden.

115 Aus den Gesetzesmaterialien ergibt sich eindeutig, dass der Gesetzgeber von der gematik die Bereitstellung einer nativen „E-Rezept-App“ für gängige Smartphone-Betriebssysteme erwartet, vgl. z. B. nur BT-Drs. 19/8753, S. 81.

8.3.2 Nutzung von Betriebssystemdiensten

Die konkrete Nutzung von standardisierten Betriebssystemdiensten durch die App ist erforderlich, damit sie ihren Zweck erreichen kann.

Die Erforderlichkeit ergibt sich zunächst aus den technischen Zwängen, denen jeder App-Anbieter ausgesetzt ist. Eine App ist bereits für die Bereitstellung grundlegender Funktionen (z. B. Anzeige von Texten, lokale Speicherung von Daten) zwingend auf die Nutzung gewisser Betriebssystemdienste angewiesen.

Hinsichtlich der von der App genutzten sogenannten nicht-essentiellen Betriebssystemdienste muss bei der gebotenen wertenden Betrachtung (vgl. 7.2.4) ebenfalls von der Erforderlichkeit ihrer Nutzung bzw. der dadurch ermöglichten Datenverarbeitung ausgegangen werden. Denn die von der App genutzten nicht-essentiellen Betriebssystemdienste dienen ausschließlich der Sicherheit und der Nutzerfreundlichkeit des elektronischen Einlöseprozesses in Bezug auf die Zugriffskomponente für die Versicherten und betreffen damit maßgebliche Anforderungen des oben genannten Zwecks.

Der für die Root-Erkennung unter Android genutzte Betriebssystemdienst SafetyNet Attestation ermöglicht die Integritätsprüfung des Smartphones des Nutzers. Die grundsätzliche Erforderlichkeit einer Integritätsprüfung ergibt sich aus der Anforderung für die gematik, eine sichere Zugriffskomponente zur Verfügung zu stellen, die durch die Prüfvorschrift des BSI (O.Resi_5) konkretisiert wird. Bei Verzicht auf eine Integritätsprüfung könnten die Nutzer nicht vor (unerkannten) Sicherheitsrisiken durch potentielles Rooting gewarnt werden, wodurch sich das Risiko eines ungewollten Datenabflusses erhöhen würde. Es ist insoweit nicht ersichtlich, dass die Nutzung eines alternativen Dienstes anstelle der vom Nutzer bereits auf seinem Smartphone bereitgestellten und betriebenen SafetyNet-Attestation-Schnittstelle eine datenschutzfreundlichere und insbesondere datensparsamere Lösung darstellen kann, zumal sie mit einer Übermittlung von Integritäts- und Zugriffsdaten an einen weiteren externen Dienstleister verbunden wäre. Im Übrigen beschränkt sich die Integritätsprüfung aus der App-Perspektive auf lokale Verarbeitungsvorgänge; ein auf einem Server bereitgestellter Verifikationsdienst zur Prüfung der Echtheit der an die App weitergegebenen Attestation wird von der App nicht kontaktiert. Entsprechendes gilt hinsichtlich des für die Root-Erkennung unter EMUI genutzten Betriebssystemdienstes Safety Detect SysIntegrity von Huawei.

Die Nutzung der Standard-Betriebssystemdienste für Push-Mitteilungen ist ebenfalls erforderlich, soweit deren Schnittstellen vom Nutzer für die App bereitgestellt werden. Die gematik hat die auf dem Markt verfügbaren Push-Dienste umfassend analysiert und ist zu dem Ergebnis gelangt, dass die betriebssystemeigenen Push-Dienste zurzeit aus technischen Gründen alternativlos sind, um den oben genannten Zweck zu fördern. Die betriebssystemeigenen Push-Dienste ermöglichen den Erhalt von Mitteilungen per Push-Verfahren, indem bei Eingang einer Mitteilung das Betriebssystem im Hintergrund die zuständige App „weckt“ und ihr dann die (verschlüsselte) Mitteilung zur weiteren Verwendung übergibt. Auf diese Weise erhöht sich die Wahrscheinlichkeit des zeitnahen Zugangs der Mitteilung deutlich. Die Nutzung des Push-Verfahrens ist alternativen Push-Diensten aufgrund der technischen Restriktionen der mobilen Betriebssysteme nicht möglich. Alternative Push-Dienste verwenden daher das Polling-Verfahren, so dass die betreffende App im Hintergrund in definierten Zeitintervallen (z. B. alle 20 Minuten) bei einem Server nach neuen Mitteilungen fragen muss. Dieses Verfahren bedingt einen höheren Energieverbrauch und ist unzuverlässiger, da die App dauerhaft im Hintergrund aktiv sein muss. Aufgrund der potentiell zeitkritischen und gesundheitsrelevanten Mitteilungen, die der Nutzer über die App im Zusammenhang mit der elektronischen Einlösung von E-Rezepten austauscht, kann die Nutzung alternativer Push-Dienste jedenfalls in Fällen, in denen der Nutzer der App eine lokale Schnittstelle zu den betriebssystemspezifischen Push-Diensten bereitstellt, nicht als gleichwertige Alternative angesehen werden.

Die Nutzung der verfügbaren Betriebssystemdienste für die lokale Authentifizierung mittels biometrischer Verfahren ist erforderlich, um das vom Gesetzgeber vorgegebene hohe Sicherheitsniveau des Authentifizierungsverfahrens ohne aktive Verwendung der eGK zu erreichen. Zur Erreichung eines hohen Sicherheitsniveaus muss ein 2-Faktor-Authentifizierungsverfahren verwendet werden, welches durch die Verwendung der biometrischen Authentifizierungsdienste des genutzten Betriebssystems als Faktor neben den auf dem Gerät lokal gespeicherten Zugangsdaten umgesetzt werden kann. Ein Verzicht auf die sachgerechte und übliche Einbindung von eventuell verfügbaren biometrischen Authentifizierungsdiensten auf dem Gerät des Nutzers würde die Usability der App erheblich beeinträchtigen und den Erwartungen und Gewohnheiten der Nutzer widersprechen. Das daraus resultierende Akzeptanzhindernis wiederum würde eine erhebliche Hürde für die

Nutzung des E-Rezepts und somit für die angestrebte Digitalisierung des Gesundheitssystems darstellen.

Soweit die App vor diesem Hintergrund bestimmungsgemäßen Gebrauch von den vom Nutzer bereitgestellten und lokal betriebenen Schnittstellen von Betriebssystemdiensten macht, ist die Erforderlichkeit ihrer Nutzung durch die App mangels gleichwertiger, datenschutzfreundlicherer Alternativen zu bejahen.

8.3.3 Optionale Nutzungsanalyse

Die optionale Nutzungsanalyse ist erforderlich, um zuverlässige und aussagekräftige Ergebnisse über das allgemeine Nutzungsverhalten, technische Fehler und den tatsächlichen Bedarf der Nutzer zu gewinnen. Der Einsatz von anderen in Betracht kommenden Analyseverfahren (z. B. analoge Befragungen, Face-to-Face-Interviews, reine Web-Befragungen) würde nicht nur erhebliche Hürden für die Kooperationsbereitschaft der Nutzer schaffen und einen erheblichen zeitlichen Mehraufwand bedeuten, sondern auch zu unzuverlässigeren Informationen (insbesondere zum Nutzungsverhalten) sowie zu einer deutlich kleineren Datenbasis führen, die weniger aussagekräftig ist. Die Verwendung einer optionalen Funktion zur Nutzungsanalyse ist demgegenüber eine bewährte, übliche und den Nutzern vertraute Vorgehensweise, um den Nutzern die Unterstützung der Entwickler bei der Verbesserung von Software zu ermöglichen.

Die optionale Nutzungsanalyse ist mit Blick auf den verfolgten Zweck so datensparsam wie möglich ausgestaltet. Die Funktion ist optional und standardmäßig deaktiviert (Privacy-by-default). Weiterhin werden lediglich Analysedaten in Bezug auf eine Session erhoben; eine Session-übergreifende Datenerfassung oder gar eine App-übergreifende Datenerfassung (Cross-Channel-Tracking) erfolgt nicht. Daten werden nicht zu einem zusammenhängenden Profil verdichtet. Die erhobenen Analysedaten werden zum frühestmöglichen Zeitpunkt auf einem in der EU betriebenen Server anonymisiert, bevor sie zur eigentlichen Nutzungsanalyse verwendet werden. Eine Verkettung von Daten ist anhand dieses Verfahrens sachgerecht verhindert.

Damit stehen derzeit keine gleichwertigen, datenschutzfreundlicheren Alternativen zur von der gematik geplanten optionalen Nutzungsanalyse zur Verfügung.

8.3.4 Datenspeicherung

Die lokalen Verarbeitungsvorgänge der App beschränken sich auf das für den oben genannten Zweck notwendige Maß.

Die kurzzeitige lokale Speicherung der vom E-Rezept-Fachdienst heruntergeladenen Daten ist erforderlich, damit der Nutzer diese Daten einsehen und im Rahmen der App-Funktionen eigenständig verwalten kann. Die lokale Speicherung über den einzelnen aktiven Nutzungsvorgang hinaus ist erforderlich, damit der Nutzer die Daten auch ohne Internetverbindung einsehen und elektronisch vor Ort bei einer Apotheke einlösen oder, je nach technischer Ausstattung, über eine direkte WiFi- oder Bluetooth-Verbindung mit einem Dritten teilen kann, etwa mittels der Betriebssystemdienste AirDrop (iOS) und Nearby Share (Android, EMUI). Eine automatische Löschung von lokal gespeicherten Fachdaten ist zur Risikoreduzierung nicht erforderlich bzw. wäre sogar schädlich und ist mit dem Ziel der Datensouveränität der Versicherten nicht vereinbar. Sämtliche lokal gespeicherten Fachdaten werden dem Nutzer in der App übersichtlich angezeigt, so dass er sie bei Bedarf zu einem von ihm selbst festgelegten Zeitpunkt jederzeit eigenständig ganz oder teilweise löschen kann. Zertifikate und Zugangsschlüssel im Speicher der App werden nach Ablauf ihrer Gültigkeit bzw. bei Session-Ende gelöscht.

Durch Deinstallieren der App kann der Nutzer sämtliche von der App selbst gespeicherten und verwalteten Daten von seinem Smartphone löschen. Die im Bereich des Betriebssystems abgelegten Daten (z. B. private Schlüssel in der SecureEnclave) werden innerhalb von Android und iOS in den Shared Preferences bzw. im Keyring abgelegt und nach dem Deinstallieren der App ungültig.

8.4 Angemessenheit

Schließlich ist die Entwicklung einer nativen App für Smartphones mit iOS-, Android- und EMUI-Betriebssystem auch angemessen. Die Angemessenheit ist gegeben, wenn die Nachteile der Verarbeitung für die betroffenen Personen – einschließlich des bei jeder Verarbeitung personenbezogener Daten gegebenen Eingriffs in das Grundrecht auf Datenschutz gemäß Art. 8 der Charta der Grundrechte der Europäischen Union (GrCh) sowie mögliche Eingriffe in andere Rechte – in einem angemessenen Verhältnis zu den Vorteilen der Verarbeitung für die legitimen Interessen des Verantwortlichen stehen. Es sind daher die Interessen der betroffenen Personen mit den Interessen des Verantwortlichen abzuwägen. Im Fall der E-Rezept-App stehen sich die Interessen der gematik als Verantwortlichem und die Interessen der Nutzer und Versicherten gegenüber. Soweit die App die sichere, barrierefreie und praktikable Nutzung von E-Rezepten ermöglichen soll, sind die Interessen der gematik und der betroffenen Personen insoweit gleichgerichtet. Demgegenüber stehen die Interessen der Nutzer und Versicherten, nicht überwacht zu werden oder infolge der Nutzung oder Nichtnutzung der App rechtliche, wirtschaftliche oder gesundheitliche Nachteilen zu erleiden.

Es würde zunächst gegen die Angemessenheit der Verarbeitung sprechen, wenn die Nutzung von E-Rezepten einschließlich der Wahrnehmung aller Versichertenrechte davon abhängig wäre, die mobile Plattform eines bestimmten Herstellers zu nutzen und diesem personenbezogene Daten preiszugeben. Vorliegend ist jedoch festzustellen, dass Versicherte das neue E-Rezept als Rezeptcode ohne Nutzung der E-Rezept-App ebenso wie das bekannte analoge Papierrezept („rosa Zettel“) verwenden können; es liegt in der Natur der Sache, dass in letzterem Falle die Vorteile der App-basierten Nutzung nicht genutzt werden können. Darüberhinausgehende Nachteile entstehen dem Versicherten allerdings nicht. Weiterhin besteht die Möglichkeit der Installation einer apk-Datei, so dass die App auch auf Android-Betriebssystemen ohne Google-Bindung verwendet werden kann.

Ebenfalls würde es gegen die Angemessenheit der Verarbeitung sprechen, wenn die Nutzung der E-Rezept-App nur unter Inkaufnahme unzumutbarer Datenschutzrisiken auf Seiten des Nutzers bzw. Versicherten möglich wäre. Davon ist – auch mit Blick auf die Erfahrungen in Ländern, in denen die elektronische Verordnung bereits etabliert ist, vgl. 4.3 – nicht auszugehen. Es liegt in der Natur der Sache, dass die Nutzer für die von ihnen genutzten und betriebenen mobilen Geräte zuständig und verantwortlich sind. Eine gewisse technische Kompetenz und „digitale Mündigkeit“ auf Seiten der Nutzer und Versicherten ist eine notwendige Voraussetzung nicht nur für die sichere Nutzung der App, sondern auch für die Digitalisierung des Gesundheitssystems und digitale Teilhabe im Allgemeinen. Gleiches gilt für die Akzeptanz spezifischer Risiken, die grundsätzlich mit jeder Datenverarbeitung einhergehen. Fraglich ist somit allein, ob das Ausmaß der den Nutzern zukommenden Verantwortlichkeit in einem angemessenen Verhältnis zur Höhe des der Nutzung der App zurechenbaren Datenschutzrisikos steht. Unter Berücksichtigung der bereits umgesetzten und bei der Risikoanalyse zugrunde gelegten bereits geplanten Risikobehandlungsmaßnahmen wird diese Frage im Ergebnis bejaht. Die gematik hat umfassend berücksichtigt, dass die Anforderungen an die sachgerechte und sichere Nutzung von digitalen Gesundheitsdiensten mitunter hohe Anforderungen an die technische und soziale Kompetenz der Versicherten stellen. Das umgesetzte App-Design kann verhindern, dass bei den erwartbaren auch ungünstigen Verhaltensweisen, insbesondere bei einer Nutzung auf unsicheren und technisch ungeeigneten Smartphones, unverhältnismäßige Datenschutzrisiken entstehen. So wird der Nutzer auf potentielle Sicherheitsrisiken deutlich hingewiesen, etwa bei Verwendung eines manipulierten Betriebssystems. Weitere vorsorgliche Hinweise erfolgen vor der Vornahme irreversibler Aktionen (z. B. Löschung von E-Rezepten auf dem E-Rezept-Fachdienst). Das Onboarding führt den Nutzer in die Zwecke, die Funktionsweise und spezifischen Risiken der Nutzung der E-Rezept-App ein, wobei die gematik einen typischen Nutzer zugrunde legt, der bisher wenig oder keine Erfahrungen bei der Nutzung von digitalen Anwendungen des Gesundheitssystems gesammelt hat. Die Wirksamkeit dieser Maßnahmen hat die gematik durch Testnutzer überprüfen lassen. Die Nutzung der App auf eindeutig ungeeigneten oder unsicheren Geräten wird, soweit möglich, bereits auf technischer Ebene unterbunden, beispielsweise indem vom BSI als unsicher eingestufte biometrische Authentifizierungsverfahren des Be-

triebssystems nicht mit der E-Rezept-App genutzt werden können. Die gematik hat bereits umfangreiche flankierende Maßnahmen zur Information und Aufklärung der Nutzer aus verschiedenen Zielgruppen hinsichtlich des E-Rezepts ergriffen und wird ihre Bemühungen in dieser Hinsicht zukünftig weiter verstärken. Insoweit wird allerdings vorausgesetzt, dass auch andere Akteure des Gesundheitsbereichs ihre bisherigen Maßnahmen auf dem Gebiet der Verbesserung der allgemeinen digitalen Kompetenz der Bürgerinnen und Bürger und im Besonderen der digitalen Gesundheitskompetenz nicht nur fortsetzen, sondern deutlich ausbauen. Die Verbesserung der digitalen Kompetenz der Versicherten ist alternativlos, um der mit der Digitalisierung einhergehenden wachsenden Eigenverantwortlichkeit des Einzelnen für den Datenschutz und die Sicherheit seiner Daten Rechnung zu tragen.

9 Risikoanalyse

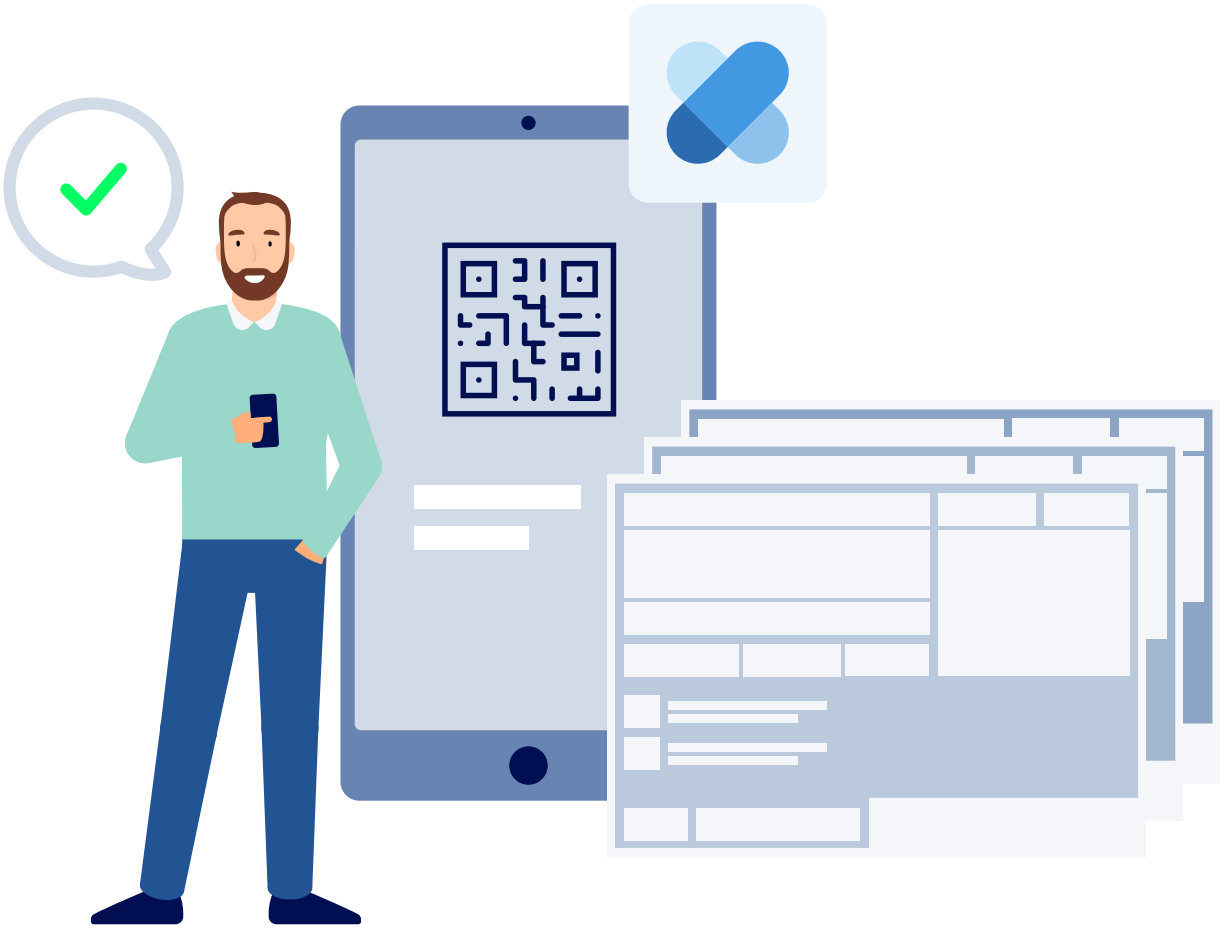
Die Datenverarbeitungstätigkeiten und -vorgänge im Zusammenhang mit der E-Rezept-App sind gemäß Art. 35 Abs. 7 lit. c DSGVO einer Bewertung der damit verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen zu unterziehen. Diese Bewertung wurde für die E-Rezept App wie im Folgenden dargelegt durchgeführt. Sie hat zu dem Ergebnis geführt, dass die Verarbeitung unter Berücksichtigung aller technischen und organisatorischen Maßnahmen nicht zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Eine vorherige Konsultation der Aufsichtsbehörde gemäß Art. 36 Abs. 1 DSGVO war demzufolge nicht erforderlich. Die Ergebnisse der Risikoanalyse wurden bei der Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge (siehe Ziffer 8) berücksichtigt.

Im Zeitraum vom 20.10. bis 25.11.2022 wurden in einem strukturierten Verfahren – dazu sogleich – Bedrohungen identifiziert und bewertet, die bei lebensnaher Betrachtung durch die Datenverarbeitungen im Zusammenhang mit der App für die Rechte und Freiheiten der betroffenen Personen bestehen. Das Ergebnis der Risikobewertung ist diesem Bericht als **Anlage Risikoanalyse** beigefügt. Zur Erläuterung wird auf Folgendes hingewiesen:

Die betrachteten Risiken entstehen in Lebenssachverhalten im Zusammenhang mit der E-Rezept-App. Diese liegen der Identifikation und Bewertung von Risiken zugrunde und werden in dieser DSFA sowie in der Risikoanalyse als Verarbeitungstätigkeiten referenziert. Gegenüber der Beschreibung der Verarbeitungstätigkeiten in diesem Bericht sind die Beschreibungen in der Risikoanalyse auf das für die Risikobewertung notwendige Maß beschränkt.

Ausgangspunkt der Identifikation von Bedrohungen sind die Verarbeitungstätigkeiten. Diese werden auf bestimmte risikobegründende oder -erhöhende Umstände menschlicher oder technischer Art hin untersucht. Wenn sich diese Umstände direkt auf die Verarbeitung von Daten im Zusammenhang mit der App beziehen, werden sie als Bedrohung berücksichtigt. Die identifizierten Bedrohungen werden zunächst anhand einheitlicher Charakteristika als mögliche und relevante Ereignisse beschrieben. Ein Element dieser Beschreibung ist die Bestimmung eines oder mehrerer Angreifertypen, die ihrerseits in Hinblick auf ihre Motivation, ihr Know-How und Ressourcen spezifiziert werden. Weiterhin werden die von der gematik im Zusammenhang mit der E-Rezept-App etablierten Maßnahmen auf die jeweilige Bedrohung bezogen und beschrieben. Dabei wird das mit einer Maßnahme im Schwerpunkt zu schützende Gewährleistungsziel des Datenschutzes und der Datensicherheit referenziert. Schließlich wird eine detaillierte Beschreibung des möglichen Ereignisses gegeben und angedeutet, welches Risiko aufgrund dieses Ereignisses für die Rechte und Freiheiten Betroffener entsteht.

Die Bewertung der Bedrohung erfolgt in Hinblick auf die Zielgröße des Risikos einer Verarbeitungstätigkeit für die Rechte und Freiheiten der betroffenen Personen. Das Risiko ist in die drei Kategorien „niedrig“, „mittel“ und „hoch“ unterteilt oder anderenfalls als „nicht einschlägig“ eingestuft. Das Risiko ist als Produkt zweier Faktoren konzipiert. Hierbei handelt es sich um die Wahrscheinlichkeit, mit der sich ein bestimmtes Bedrohungsszenario realisiert (Eintrittswahrscheinlichkeit), und das Ausmaß des im Falle der Realisierung entstehenden Schadens für Betroffene (Schaden). Beiden Faktoren können die Werte „niedrig“, „mittel“, „hoch“ und „sehr hoch“ zugeordnet werden. In Bezug auf den Schaden kann zusätzlich der Wert „kein Schaden“ zugeordnet werden. Die eigentliche Bewertung, d. h. die Zuordnung der Werte zu den Faktoren erfolgte auf Grund der abgestimmten Einschätzung der Beteiligten.



Für die sieben untersuchten Datenverarbeitungstätigkeiten[116] wurden insgesamt 20 Bedrohungen identifiziert. Hiervon wurden in der initialen Bewertung fünf Bedrohungen der Risikokategorie „niedrig“ und 14 der Risikokategorie „mittel“ zugeordnet. Nur eine Bedrohung wurde in der initialen Bewertung der Risikokategorie „hoch“ zugeordnet.

Hierbei handelt es sich um die Bedrohung der Offenlegung von Gesundheitsdaten aufgrund eigenen, unvorsichtigen Umgangs der Nutzer mit den Daten in der E-Rezept-App. Zur Mitigation dieses Risikos verständigte man sich darauf, dass von der gematik eine weitere Maßnahme umgesetzt wird. Hierbei handelt es sich um einen ausdrücklichen Warnhinweis, der den Nutzern in der App angezeigt wird und der sie dazu anhält, umsichtig mit den sensiblen Gesundheitsinformationen umzugehen. Die Wirksamkeit der Mitigation wird evaluiert werden.

116 Die Verarbeitungstätigkeit 8 – Nutzungsanalyse ist in dieser vorläufigen Entwurfsfassung nicht berücksichtigt, weil erforderliche Informationen zum eingebundenen Dienstleister noch in Klärung begriffen sind.

10 Nachhaltige Sicherung des Datenschutzes

In regelmäßigen Abständen müssen Kernelemente des Datenschutzes im Rahmen eines wirksamen Datenschutzmanagements überprüft werden.

Die Datenschutzfolgenabschätzung wird im Rahmen der Entwicklung der E-Rezept-App fortgesetzt und dieser Bericht hinsichtlich relevanter Änderungen fortgeschrieben werden.

11 Anhang

Anlage 1: Risikoanalyse (Version 1.0)

Impressum

Herausgeber:
gematik GmbH
Friedrichstraße 136
10117 Berlin

Gestaltung: DreiDreizehn GmbH, Berlin