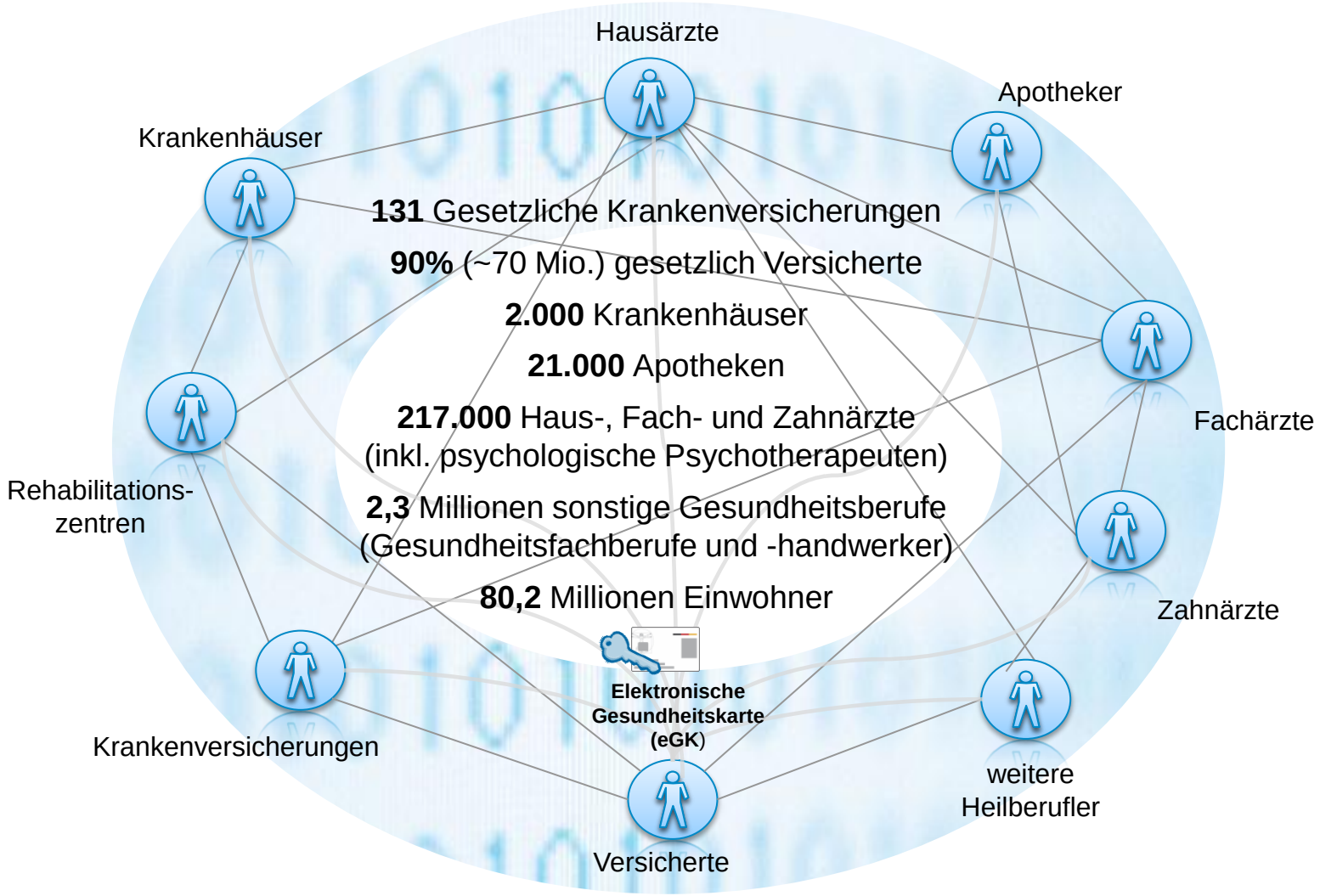
Elektronische Gesundheitskarte und Datenschutz

Prof. Dr. Arno Elmer
Hauptgeschäftsführer

gematik
Gesellschaft für Telematikanwendungen
der Gesundheitskarte mbH
Friedrichstraße 136
10117 Berlin

Das vernetzte Gesundheitssystem



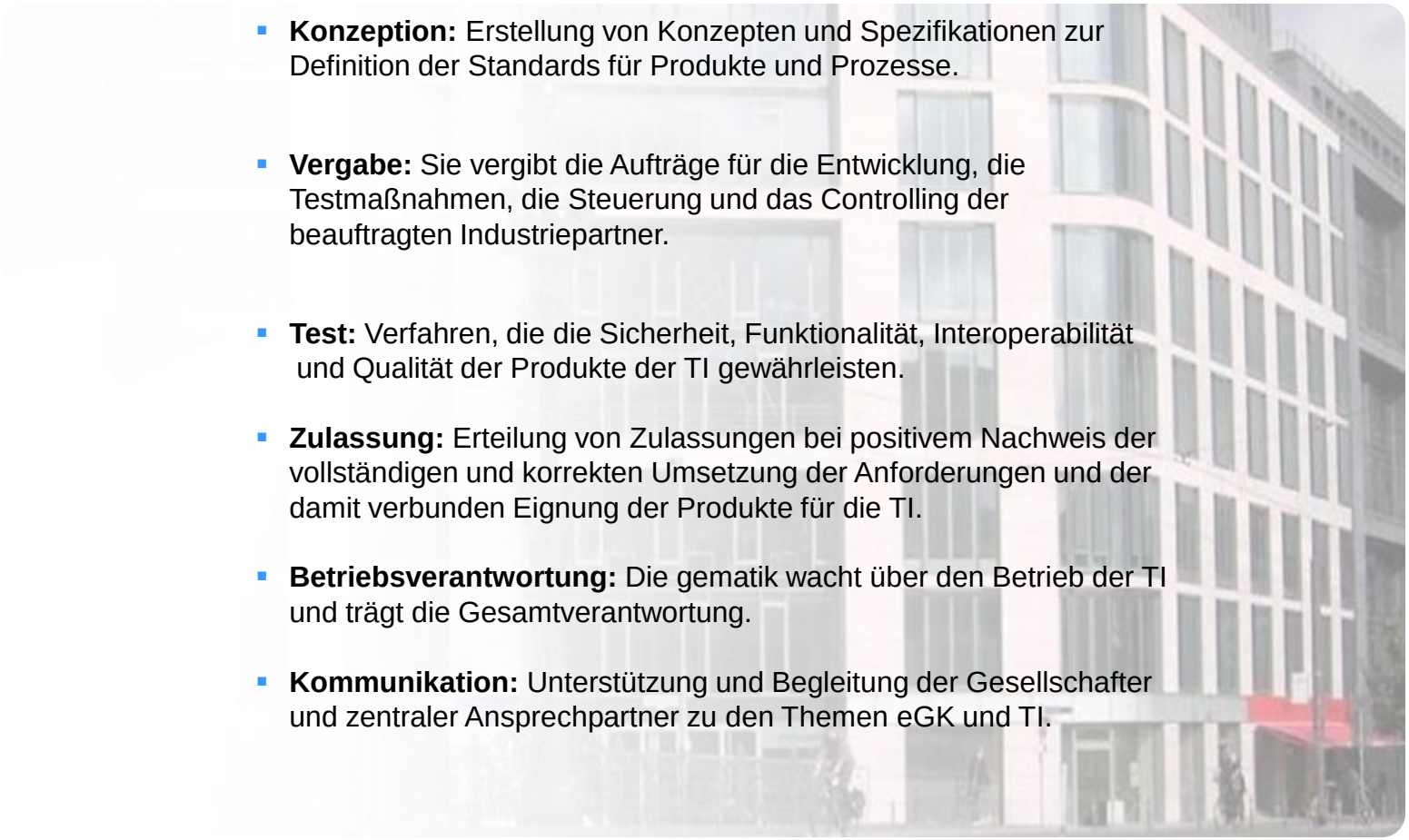
gematik - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- Einführung der elektronischen Gesundheitskarte verankert im **Gesetz zur Modernisierung der gesetzlichen Krankenversicherung** (2004).
- **Selbstverwaltung in der gesetzlichen Krankenversicherung** zuständig für den Aufbau der Telematikinfrastruktur und die Einführung der eGK.
- **gematik gegründet im Januar 2005**

- **Zentrales Koordinations- und Kommunikationszentrum** für das Thema Telematikinfrastruktur und elektronische Gesundheitskarte im deutschen Gesundheitswesen.
- Aktuell: Rund 220 IT-Experten, Anwendungsspezialisten und Projektleiter bei der gematik.
- Hauptgeschäftsführer Prof. Dr. Arno Elmer
- Die Gesellschafter:

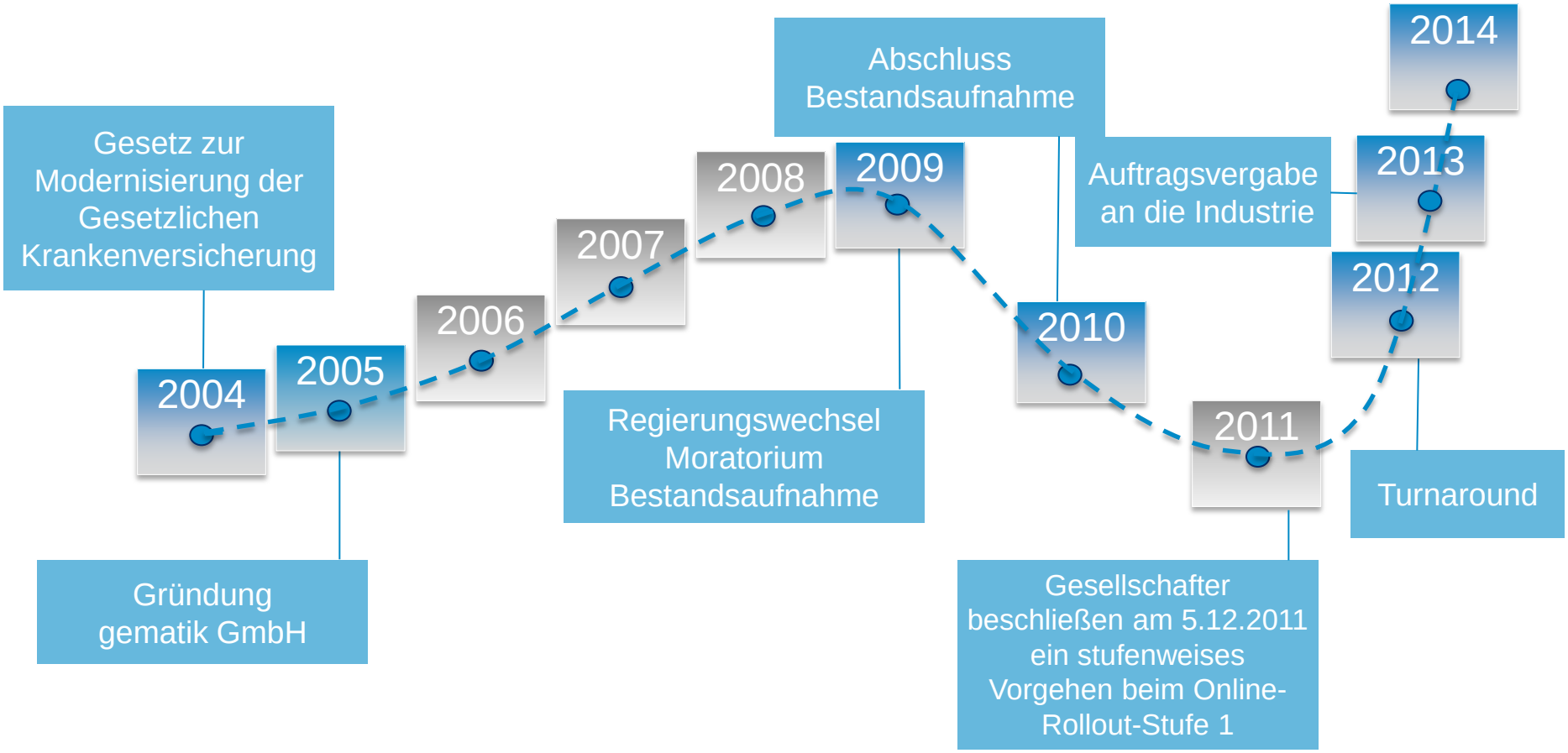
BUNDESÄRZTEKAMMER · BUNDESZAHNÄRZTEKAMMER · DAV · DEUTSCHE KRANKENHAUS GESELLSCHAFT DKG · GKV Spitzenverband · KBV · KZBV

gematik: Kompetenzzentrum der eGK / TI



- **Konzeption:** Erstellung von Konzepten und Spezifikationen zur Definition der Standards für Produkte und Prozesse.
- **Vergabe:** Sie vergibt die Aufträge für die Entwicklung, die Testmaßnahmen, die Steuerung und das Controlling der beauftragten Industriepartner.
- **Test:** Verfahren, die die Sicherheit, Funktionalität, Interoperabilität und Qualität der Produkte der TI gewährleisten.
- **Zulassung:** Erteilung von Zulassungen bei positivem Nachweis der vollständigen und korrekten Umsetzung der Anforderungen und der damit verbunden Eignung der Produkte für die TI.
- **Betriebsverantwortung:** Die gematik wacht über den Betrieb der TI und trägt die Gesamtverantwortung.
- **Kommunikation:** Unterstützung und Begleitung der Gesellschafter und zentraler Ansprechpartner zu den Themen eGK und TI.

Die Historie der gematik – Turnaround realisiert!



Spezialgesetzliche Regelungen des Datenschutzes für die eGK sind im Sozialgesetzbuch (SGB) V festgelegt

§ 291a SGB V– elektronische Gesundheitskarte (eGK)

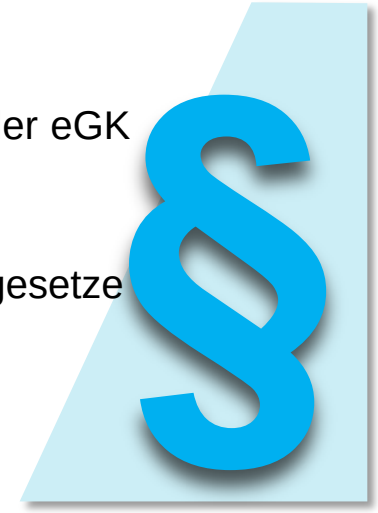
- regelt Anforderungen, Aufgaben und Ziele der eGK
- Anwendungen der eGK
  - verpflichtende administrative Anwendungen (z.B. Versichertenstammdatenmanagement)
  - freiwillige medizinische Anwendungen (z.B. Notfalldatenmanagement)
- definiert Anforderungen des Datenschutzes bzgl. der eGK

§ 291b SGB V– Gesellschaft für Telematik (gematik)

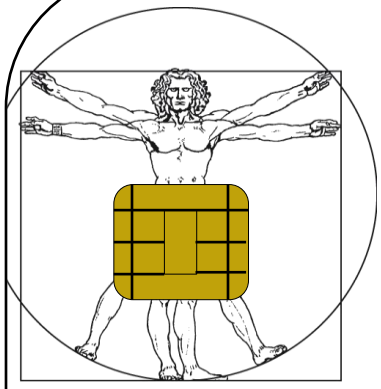
- regelt die Verantwortung der gematik
- Auftrag zur Sicherstellung des Datenschutzes bzgl. der eGK

Weitere relevante gesetzliche Regelungen

- Bundesdatenschutzgesetz bzw. Landesdatenschutzgesetze
- Strafgesetzbuch (StGB)
- Strafprozessordnung (StPO)
- SGB X (Sozialdatenschutz)



Datenschutz im Fokus



Gesundheitskarte

„Das Konzept der Gesundheitskarte ist aus Datenschutzsicht vorbildlich.“

„Es muss elektronische Kommunikation stattfinden, allerdings unter Berücksichtigung unseres Anspruchs an das Patienten- und Arztgeheimnis.“

Dr. Thilo Weichert, Landesdatenschutzbeauftragter Schleswig-Holstein

gematik und Telematikinfrastruktur

Telematikinfrastruktur ist die erforderliche interoperable und kompatible Informations-, Kommunikations- und Sicherheitsinfrastruktur
(§ 291a Abs. 7 Satz 1 SGB V).

Primäres Ziel der Einführung der Telematikinfrastruktur

- Sicherstellung hohes Datenschutz- und Datensicherheitsniveau
- Vermeidung Insellösungen, sektorenübergreifende und bundesweite Kommunikation

Etablierung einer verantwortlichen Stelle zur Erreichung dieser Ziele -> gematik

- Wahrnehmung hoheitlicher Aufgaben (Erstellung Sicherheitskonzept und interoperabler Standards, Test- und Zertifizierungsmaßnahmen)
- Unabhängigkeit bei der Schaffung eines neuen Marktes
- Neutrales Trust Center

Die „Dreisprung“ zur Sicherstellung des Datenschutzes in der TI umfasst die Phasen Design, Zulassung und Betrieb

- Einhalten der Eckpunkte des Datenschutzes der TI
- Nutzen von Methoden zur Erstellung von Datenschutzkonzepten

- Prüfung dezentraler Komponenten nach Vorgaben des BSI
- Prüfung zentraler Dienste durch unabhängige Sicherheitsgutachter

- Kontrolle der Aufrechterhaltung des Datenschutzes im Betrieb

„Privacy by Design“ in den Spezifikationen

Geprüfter Datenschutz vor Inbetriebnahme

Datenschutz im laufenden Betrieb

Einführung einer neuen Fachanwendung

Die „Dreisprung“ zur Sicherstellung des Datenschutzes in der TI umfasst die Phasen Design, Zulassung und Betrieb

- Einhalten der Eckpunkte des Datenschutzes der TI
- Nutzen von Methoden zur Erstellung von Datenschutzkonzepten

„Privacy by Design“ in den Spezifikationen

- Prüfung dezentraler Komponenten nach Vorgaben des BSI
- Prüfung zentraler Dienste durch unabhängige Sicherheitsgutachter

Geprüfter Datenschutz vor Inbetriebnahme

- Kontrolle der Aufrechterhaltung des Datenschutzes im Betrieb

Datenschutz im laufenden Betrieb

Einführung einer neuen Fachanwendung

Eckpunkte des Datenschutzes in der Telematikinfrastruktur

Die medizinischen Daten der Versicherten sind in der TI zweckgebunden nur für die medizinische Versorgung des Versicherten

- Technische Einschränkung des zugriffsberechtigten Personenkreises auf Heilberufler mit Verschwiegenheitspflicht (§ 291a Abs. 4 und 5a SGB V, § 203 StGB)
- Erweiterung des Beschlagnahmeschutzes auf die eGK (§ 97 StPO)
- Bußgeld- und Strafvorschriften bei Verstößen (§§ 307, 307b SGB V)
- Daten der TI dürfen nicht zu Persönlichkeitsprofilen verknüpft werden.

Versicherte nutzen die medizinischen Anwendungen der TI freiwillig

- Versicherte wählen frei aus dem Angebot medizinischer Anwendungen der TI.
- Medizinische Anwendungen erfordern eine schriftliche Einwilligung des Versicherten bei einem Arzt, Zahnarzt, Psychotherapeuten oder Apotheker.
- Versicherte können Einwilligungen jederzeit widerrufen.

Eckpunkte des Datenschutzes in der Telematikinfrastruktur

Der Versicherte hat die Hoheit über seine medizinischen Daten in der Telematikinfrastruktur

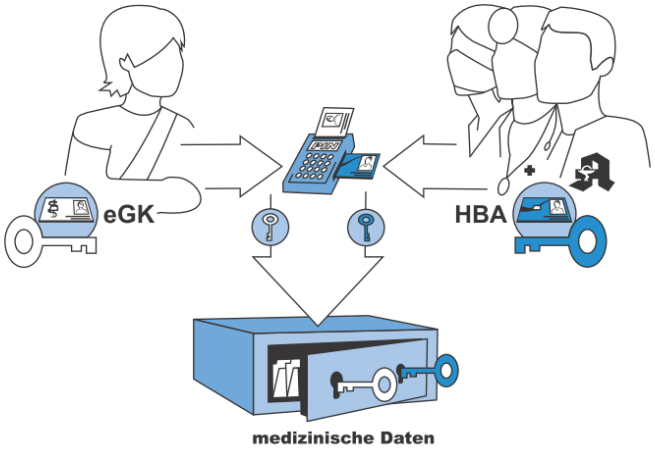
- Versicherte entscheiden darüber, welche ihrer medizinischen Daten in der TI gespeichert werden sollen.
- Versicherte entscheiden darüber, ob ihre medizinischen Daten in der TI gelöscht werden.
- Versicherte entscheiden, welchem Arzt sie welche ihrer medizinischen Daten der TI zur Verfügung stellen.
- Versicherte haben ein Recht, auf ihre medizinischen Daten in der TI zuzugreifen.
- Versicherte dürfen nicht bevorzugt oder benachteiligt werden, weil sie einen Zugriff auf ihre medizinischen Daten bewirkt oder verweigert haben (§ 291a Abs. 8 SGB V).

Eckpunkte des Datenschutzes in der Telematikinfrastruktur

Daten der Versicherten können in der TI nur im Zusammenspiel zweier Schlüssel genutzt werden

- Schlüssel 1 – eGK:
  Instrument des Versicherten zur Ausübung seiner Datenschutzrechte. Der Versicherte kontrolliert mit der eGK (inkl. seiner PIN), welcher Heilberufler auf seine Daten wann zugreifen kann.

- Schlüssel 2 – HBA/ SMC-B: Heilberufler authentisieren sich mit dem Heilberufsausweis (HBA) oder der Institutionenkarte (SMC-B).



Eckpunkte des Datenschutzes in der Telematikinfrastruktur

Der Versicherte kann alle Zugriffe auf seine Daten erkennen

- Jeder Zugriff sowie Zugriffsversuch auf die medizinischen Daten der TI wird auf der eGK protokolliert.
- Der Versicherte erkennt am Protokolleintrag, welcher Heilberufler, wann auf seine Daten zugegriffen hat.
- Medizinische Daten sind nicht Bestandteil der Protokolldaten auf der eGK – bei Bedarf kann sich der Versicherte beim protokollierten Heilberufler informieren.
- Die Protokolldaten sind alleine für den Versicherten zum Zwecke der Datenschutzkontrolle bestimmt.

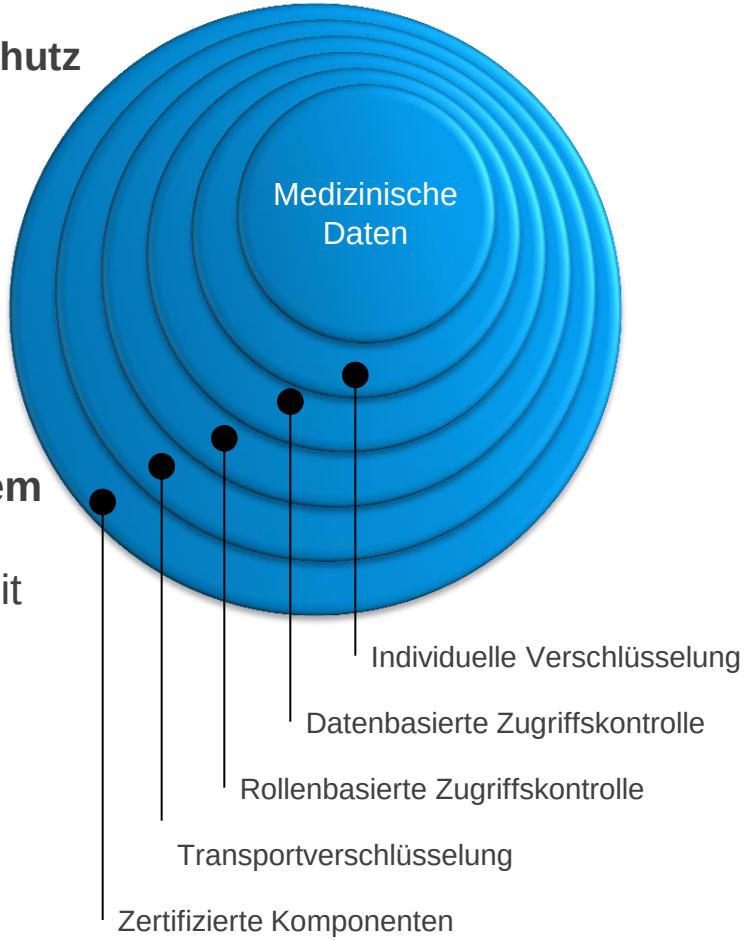
Die TI muss für Versicherte und Heilberufler praktikabel sein

- Verfahren müssen für Versicherte und Heilberufler praktikabel und alltagstauglich sein, damit sie ihre Datenschutzrechte wahrnehmen können.
- Bestimmte Versichertengruppen (etwa temporär Kranke, chronisch Kranke, Notfallpatienten oder Pflegefälle) dürfen nicht benachteiligt werden.

Eckpunkte des Datenschutzes in der Telematikinfrastruktur

Informationssicherheit zur Gewährleistung des Datenschutzes

- Die TI setzt **Sicherheitsmaßnahmen zum Schutz** der **medizinischen Daten** ein
  - **Verschlüsselung** und **digitale Signaturen**
  - technischer Zugriffsschutz und Authentisierung
  - **Kommunikation über abgesicherte Kanäle**
  - privates Netz
  - Anonymisierung (z.B. Intermediär bei VSDM)
  - …
- **Sicherheitsmechanismen nach aktuellem Stand von Technik und Wissenschaft** (Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik)
- **Keine zentralen Server** im Internet und **keine Cloud-Lösungen**
- Betrieb der Dienste der TI in Deutschland



Methoden zur Erstellung von Datenschutzkonzepten

Anforderungen des Datenschutzes werden von Anfang an in der Telematikinfrastruktur betrachtet:

- Entwickler von Anwendungen, Komponenten und Diensten der TI müssen bereits im Design Methoden zum Datenschutz anwenden, die von der gematik vorgegeben sind.
- Die Methoden gewährleisten eine einheitliche Vorgehensweise und die vollständige Betrachtung des Datenschutzes in der TI.
- Ergebnis ist ein Datenschutzkonzept, in dem die Maßnahmen nachvollzogen werden können, mit denen die gesetzlichen Regelungen des Datenschutzes umgesetzt werden.

Die „Dreisprung“ zur Sicherstellung des Datenschutzes in der TI umfasst die Phasen Design, Zulassung und Betrieb

- Einhalten der Eckpunkte des Datenschutzes der TI
- Nutzen von Methoden zur Erstellung von Datenschutzkonzepten

„Privacy by Design“ in den Spezifikationen

- Prüfung dezentraler Komponenten nach Vorgaben des BSI
- Prüfung zentraler Dienste durch unabhängige Sicherheitsgutachter

Geprüfter Datenschutz vor Inbetriebnahme

- Kontrolle der Aufrechterhaltung des Datenschutzes im Betrieb

Datenschutz im laufenden Betrieb

Einführung einer neuen Fachanwendung

In der Zulassung muss die Umsetzung der Anforderungen des Datenschutzes nachgewiesen werden

- Die Zulassung **dezentraler Komponenten** erfordert eine Evaluierung und Zertifizierung nach Common Criteria gemäß den Vorgaben des BSI
  - Protection Profiles für das Kartenbetriebssystem der Smartcards der TI (eGK, HBA, SMC-B, Gerätekarten für Konnektor und Kartenterminal)
  - Protection Profiles für Konnektor, eHealth-Kartenterminal und mobiles Kartenterminal

- Die Zulassung **zentraler Dienste** erfordert ein Sicherheits-gutachten
  - **Unabhängiger Sicherheitsgutachter** prüft die Anforderungen des Datenschutzes und der Sicherheit und dokumentiert die Ergebnisse in einem Sicherheitsgutachten.
  - Die gematik definiert die Anforderungen an das Sicherheitsgutachten und die Qualifikation des Sicherheitsgutachters.
  - Die gematik prüft das Sicherheitsgutachten und spricht ggf. die Zulassung aus.

Die „Dreisprung“ zur Sicherstellung des Datenschutzes in der TI umfasst die Phasen Design, Zulassung und Betrieb

- Einhalten der Eckpunkte des Datenschutzes der TI
- Nutzen von Methoden zur Erstellung von Datenschutzkonzepten

„Privacy by Design“ in den Spezifikationen

- Prüfung dezentraler Komponenten nach Vorgaben des BSI
- Prüfung zentraler Dienste durch unabhängige Sicherheitsgutachter

Geprüfter Datenschutz vor Inbetriebnahme

- Kontrolle der Aufrechterhaltung des Datenschutzes im Betrieb

Datenschutz im laufenden Betrieb

Einführung einer neuen Fachanwendung

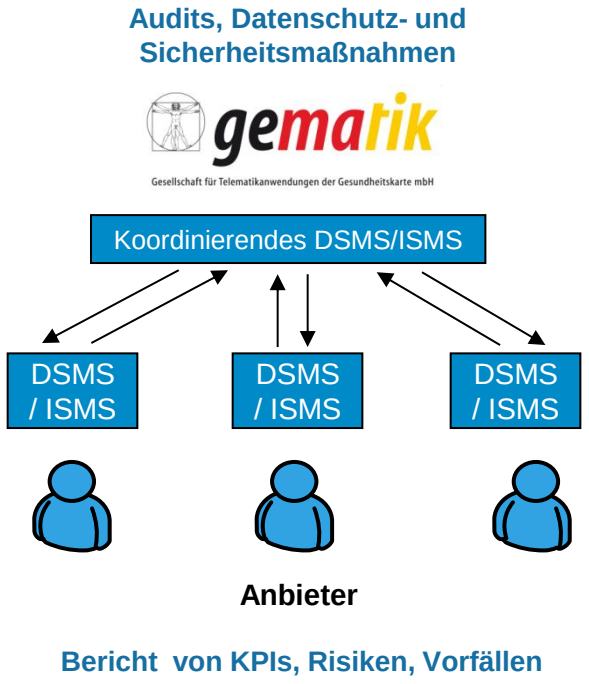
Zur Aufrechterhaltung von Datenschutz & Sicherheit errichtet die gematik ein koordinierendes DSMS und ISMS

Verantwortung der gematik:

- Koordinierung von Maßnahmen bei übergreifenden Vorfällen oder Risiken
- Durchführung von anlassbezogenen Audits
- Auswertung der Kennzahlen, Ableitung von Maßnahmen, Pflege des Kennzahlenmodells

Verantwortung der Anbieter:

- Einhaltung der rechtlichen Anforderungen an den Datenschutz
- Einführung und Aufrechterhaltung eines Datenschutz- und Informationssicherheits-managementsystems (DSMS/ISMS)
- sofortige Meldung übergreifender Vorfälle und Risiken an die gematik
- regelmäßige Übermittlung von Kennzahlen
- zu Datenschutz & Informationssicherheit



Die eGK leistet einen entscheidenden Beitrag, den Datenschutz im Gesundheitswesen zu erhöhen

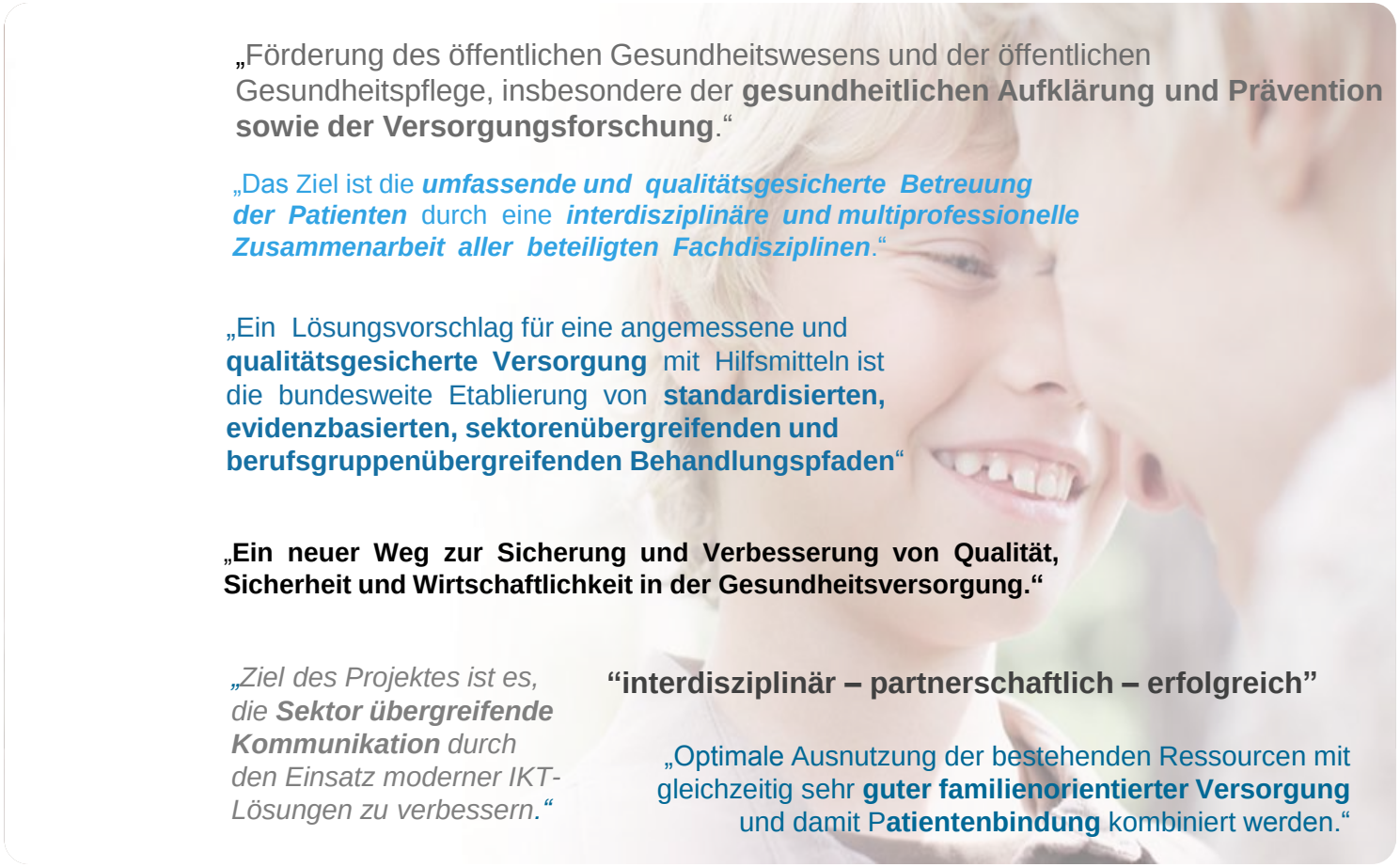
Die gematik stärkt den Datenschutz der Beteiligten – nachhaltig

- Die TI trägt durch ihre Datenschutzlösungen nachhaltig dazu bei, die Datenschutzrechte der Beteiligten zu stärken.
- Die Maßnahmen des Datenschutzes der TI stehen allen – insbesondere auch zukünftigen – Anwendungen der TI zur Verfügung.
- Die Entwickler von Anwendungen können das Datenschutzniveau in ihren Anwendungen mit angemessenem Aufwand einfach erhöhen, ohne selbst Datenschutzmaßnahmen entwickeln zu müssen.

Die gematik vernetzt das Gesundheitswesen – sicher

- Die TI vernetzt das deutsche Gesundheitswesen und bietet die sichere Basis für eine Vielzahl von medizinischen Anwendungen.
- Die Schweigepflicht der Heil- und Gesundheitsberufe und das Vertrauensverhältnis zwischen Arzt und Patient werden in der TI durch technische Sicherheitsmaßnahmen gewährleistet.

Warum Vernetzung? Kommentare Teilnehmer Medizin Management Preis 2013



„Förderung des öffentlichen Gesundheitswesens und der öffentlichen Gesundheitspflege, insbesondere der **gesundheitlichen Aufklärung und Prävention sowie der Versorgungsforschung**."

„Das Ziel ist die ***umfassende und qualitätsgesicherte Betreuung der Patienten*** durch eine ***interdisziplinäre und multiprofessionelle Zusammenarbeit aller beteiligten Fachdisziplinen***."

„Ein Lösungsvorschlag für eine angemessene und **qualitätsgesicherte Versorgung** mit Hilfsmitteln ist die bundesweite Etablierung von **standardisierten, evidenzbasierten, sektorenübergreifenden und berufsgruppenübergreifenden Behandlungspfaden**"

„Ein neuer Weg zur Sicherung und Verbesserung von Qualität, Sicherheit und Wirtschaftlichkeit in der Gesundheitsversorgung."

*„Ziel des Projektes ist es, die **Sektor übergreifende Kommunikation** durch den Einsatz moderner IKT-Lösungen zu verbessern."*

"interdisziplinär – partnerschaftlich – erfolgreich"

„Optimale Ausnutzung der bestehenden Ressourcen mit gleichzeitig sehr **guter familienorientierter Versorgung** und damit P**atientenbindung** kombiniert werden."

Wir vernetzen das Gesundheitswesen. Sicher.

gematik

Vielen Dank für Ihre Aufmerksamkeit.

Prof. Dr. Arno Elmer
Hauptgeschäftsführer

Arno.Elmer@gematik.de