

Stellungnahme

Oktober 2026

Gesetz für Daten und digitale Innovation im Gesundheitswesen (GeDIG)

Inhalt

Gesetz für Daten und digitale Innovation im Gesundheitswesen (GeDIG)	1
Präambel	3
Zusammenfassung	3
Zentrale Forderungen	4
1 EUDI Wallet und digitale Identitäten	5
EUDI Wallet frühzeitig und gleichberechtigt einsetzen	5
Identitätsnachweis und Versorgungskontext trennen	6
2 gematik und Telematikinfrastruktur	7
Marktmodell und Rolle der gematik klar begrenzen	8
Betriebsstabilität und verhältnismäßige Eingriffe sichern	9
Sichere Kommunikation technologieoffen gestalten	9
Faire Rahmenbedingungen für Primärsysteme schaffen	10
Industrie frühzeitig beteiligen und Umstellungen planbar machen	11
3 Digitale Versorgungssteuerung	11

Dem Ausschuss ist das vorliegende Dokument
in nicht barrierefreier Form zugeleitet worden.

Versorgungseinstieg für qualifizierte Anwendungen öffnen	12
Bedarfseinschätzung mit offenen Qualitätsanforderungen verbinden	12
Zusätzliche Regulierung von Terminplattformen vermeiden	13
Elektronische Überweisungen verlässlich einführen	13
4 EHDS und Gesundheitsdatennutzung	14
Zugangsstelle für die industrielle Gesundheitswirtschaft absichern	15
Zusätzliche nationale Einwilligungspflicht für Omik Daten vermeiden	15
Pflichten der Gesundheitsdateninhaber praktikabel gestalten	16
Daten für Forschung und iterative Entwicklung nutzbar machen	17
Technische Umsetzung und unabhängige Aufsicht trennen	17
5 Weitere konkrete Versorgungsanliegen	18
Kombinierte Fernüberwachungsmodelle ermöglichen	18
DiGA Verordnungen niedrigschwellig einlösbar gestalten	19
Weitere elektronische Verordnungen konsequent voranbringen	20
Reallabore für gemeinsame Innovation öffnen	20
Medikationsplan und Impfmanagement interoperabel weiterentwickeln	20
Cloud Regelungen praxistauglich umsetzen	21
Einwilligungsbasierte Datenausleitung aus der ePA praktisch ermöglichen	21
Fazit	22
Digitalisierung gemeinsam wirksam umsetzen	22
Anhang	23

Präambel

Bitkom hat den Referentenentwurf des Gesetzes für Daten und digitale Innovation im Gesundheitswesen (GeDIG) bereits umfassend kommentiert und konkrete Vorschläge für eine praxistaugliche und innovationsfreundliche Weiterentwicklung vorgelegt ([LINK Stellungnahme](#)). Die dort formulierten Forderungen behalten weiterhin Gültigkeit, soweit sie im weiteren Gesetzgebungsverfahren bislang nicht aufgegriffen wurden.

Mit der vorliegenden Stellungnahme konzentrieren wir uns auf die aus unserer Sicht zentralen Themenfelder und den weiterhin bestehenden Handlungsbedarf. Dabei geht vor allem um die Frage, wie die Digitalisierung des Gesundheitswesens konsequent vorangetrieben und digitale Innovation schneller in die Versorgung gebracht werden können. Konkrete Formulierungsvorschläge befinden sich im Anhang.

Zusammenfassung

Das GeDIG bietet die Chance, die Digitalisierung des Gesundheitswesens stärker an den Bedürfnissen von Patientinnen und Patienten sowie Leistungserbringenden auszurichten. Digitale Prozesse können den Zugang zur Versorgung erleichtern, die Zusammenarbeit verbessern und den Aufwand im Versorgungsalltag reduzieren. Die Weiterentwicklung der Telematikinfrastruktur (TI), die erweiterte Nutzung der elektronischen Patientenakte (ePA) und die nationale Umsetzung des Europäischen Gesundheitsdatenraums (EHDS) unterstützen wir ausdrücklich.

Damit diese Ziele erreicht werden, muss eine konsequente Digital-first-Politik auch in den gesetzlichen Rahmenbedingungen und ihrer Umsetzung erkennbar werden. Dazu gehören durchgängig digitale Verfahren, einfach nutzbare Zugänge und die Möglichkeit, geeignete Lösungen unterschiedlicher Anbieter miteinander zu verbinden.

Die Unternehmen der digitalen Gesundheitswirtschaft bringen dafür technische Expertise, operative Erfahrung und erhebliche Entwicklungsleistungen ein. Sie schaffen und betreiben einen wesentlichen Teil der Lösungen, auf denen digitale Versorgung aufbaut. Ihre Rolle muss bei der gesetzlichen Ausgestaltung und Umsetzung frühzeitig berücksichtigt werden. Innovation benötigt Raum zur Erprobung und Weiterentwicklung sowie verlässliche Perspektiven für Investitionen.

Der Gesetzgeber sollte deshalb klare Ziele und verbindliche Anforderungen an Qualität, Sicherheit und Interoperabilität vorgeben und ein offenes, wettbewerbliches Zusammenwirken der Akteure ermöglichen. Zusätzliche Beauftragungs-, Betriebs- und Eingriffsbefugnisse sind hinsichtlich ihres konkreten Nutzens und ihrer Folgen für Marktstruktur und Versorgung zu bewerten. Klare Rollen und unabhängige Kontrolle schaffen Vertrauen in die Entscheidungen über technische Anforderungen und Marktzugang.

Zugleich müssen neue Pflichten nach ihrem tatsächlichen Umsetzungsaufwand differenziert werden. Frühzeitig verfügbare Spezifikationen, ausreichende Entwicklungs- und Testzeiten sowie verlässliche Übergänge sind Voraussetzungen für sichere Umstellungen. Finanzierung und Verantwortlichkeiten müssen nachvollziehbar

geregelt sein. Zusätzliche Aufwände sollten durch einen konkreten Versorgungsnutzen gerechtfertigt sein und die Leistungsfähigkeit der beteiligten Akteure berücksichtigen.

Bei der Umsetzung europäischer Vorgaben sollte Deutschland die Harmonisierung konsequent unterstützen. Für den EHDS braucht es kompetente Zugangsstellen und praxistaugliche Verfahren, die den Besonderheiten der industriellen Gesundheitswirtschaft Rechnung tragen. Vermeidbare nationale Zusatzanforderungen würden den grenzüberschreitenden Datenzugang erschweren und sollten entfallen.

Zentrale Forderungen

Digitale Zugänge aus den Anwendungen der Versicherten heraus ermöglichen. Die EUDI-Wallet sollte frühzeitig im Gesundheitswesen nutzbar werden. Qualifizierte Drittanwendungen brauchen einen diskriminierungsfreien Zugang zu ePA- und Versorgungsfunktionen. Eine erfolgreiche Authentisierung sollte für verbundene Dienste weiterverwendbar sein; bestehende Zugangswege sind bis zur Verfügbarkeit eines gleichwertigen Nachfolgeverfahrens abzusichern.

TI-Stabilität mit klaren Betriebsanforderungen und unabhängiger Kontrolle stärken. Die erweiterten Befugnisse der gematik müssen gesetzlich begrenzt und hinsichtlich Nutzen, Kosten und Marktfolgen überprüft werden. Regelsetzung, Zulassung und Aufsicht sind von Beauftragung und Betrieb zu trennen. Die Zulassungsausnahme für gematik-beauftragte Dienste sollte entfallen; Sperrungen müssen letztes Mittel bleiben.

Versorgungseinstieg und Bedarfseinschätzung für qualifizierte Anbieter öffnen. Die Regelungen sollten ein offenes Zusammenspiel von ePA, Terminvermittlung und geeigneten Anwendungen von Drittanbietern ermöglichen. Für alle beteiligten Angebote müssen einheitliche Anforderungen an Qualität, Sicherheit und Interoperabilität gelten, deren Einhaltung unabhängig und interessenneutral überprüft wird. Die vorgesehene Regelung zu Terminplattformen sollte ersatzlos gestrichen werden.

EHDS-Zugang für die industrielle Gesundheitswirtschaft verbindlich organisieren. Eine domänenspezifische Zugangsstelle für die industrielle Gesundheitswirtschaft sollte im GeDIG ausdrücklich abgesichert und unter Einbindung der betroffenen Unternehmen aufgebaut werden. Die zusätzliche nationale Einwilligungspflicht für bestimmte Omik-Daten sollte entfallen. Pflichten zu Forschungskennziffern und Datenbereitstellung müssen auch für industrielle Bestandsdaten praktikabel sein.

Umsetzung planbar machen und konkrete Versorgungsprozesse verbessern. Spezifikationen, Testwerkzeuge und Übergangsfristen müssen eine sichere Einführung ermöglichen. DiGA-Verordnungen brauchen niedrighschwellige und plattformneutrale Einlösewege; kombinierte Fernüberwachungsmodelle sind zu berücksichtigen. Reallabore sollten weitere geeignete Akteure einbeziehen. Medikations- und Impfdaten müssen verlässlich und interoperabel nutzbar werden.

1 EUDI Wallet und digitale Identitäten

Mit eIDAS 2.0 entsteht ein gemeinsamer europäischer Rahmen für digitale Identitäten und sichere elektronische Nachweise. Die EUDI-Wallet bietet die Chance, diese branchenübergreifend und grenzüberschreitend zu nutzen. Im Gesundheitswesen kann sie damit die Identifizierung von Versicherten und den Zugang zu digitalen Versorgungsangeboten erleichtern. Perspektivisch sind auch digitale Nachweise für Unternehmen und Einrichtungen einzubeziehen.

Diese verbindliche Rechtsverordnung und der flächendeckende Einsatz von Wallets hat erhebliche Konsequenzen für die Weiterentwicklung der TI. Dies betrifft nicht nur digitale Identitäten für Versicherte (Gesundheits-ID) sondern auch Leistungserbringer und alle Gesundheitseinrichtungen. Darüber hinaus wird es auch Auswirkungen auf die Weiterentwicklung von TI-Fachanwendungen wie ePA, E-Rezept, KIM, TIM, u.a. haben. Die parallel in Umsetzung befindliche EU-Initiative zum EHDS setzt in Teilen ebenfalls auf die Nutzung wallet-basierter Identifizierungs- und Datenaustausch-Lösungen, wie sie die eIDAS 2.0 Verordnung vorsieht.

Bundesgesundheitsministerium und Bundesministerium für Digitales und Staatsmodernisierung sollten deshalb gemeinsam ein klares und verbindliches Zielbild für die Integration der EUDI-Wallet und perspektivisch der European Business Wallet entwickeln. Die EUDI-Wallet sollte möglichst umgehend als zentrales Identitäts- und Nachweisinstrument im Gesundheitswesen nutzbar werden. Neue Vorgaben müssen diesen Übergang unterstützen und kostenintensive Parallelentwicklungen für kurze Übergangszeiträume vermeiden.

Entscheidend sind offene Schnittstellen und die gleichberechtigte Nutzung geeigneter Identitätsmittel. Versicherte sollten digitale Angebote aus unterschiedlichen zugelassenen Anwendungen heraus nutzen können. Dabei sind digitale Identität, Versicherungsnachweis und der Nachweis eines konkreten Versorgungskontexts klar voneinander zu trennen und technisch sinnvoll zu verbinden.

Versicherte brauchen Vertrauen in das digitale Umfeld. Eine breite Aufklärungskampagne sollte staatlich beauftragt werden

EUDI Wallet frühzeitig und gleichberechtigt einsetzen

[Zu § 291 Absatz 3 und 8 sowie §§ 342 und 345a SGB V](#)

Wir begrüßen die vorgesehenen Einsatzmöglichkeiten der EUDI-Wallet. Der Entwurf sieht ihre Nutzung zur sicheren Identifikation ab Januar 2027 vor, sofern die technischen Voraussetzungen gegeben sind. Als gleichwertiger Versicherungsnachweis soll sie aber erst ab Dezember 2028 dienen und zur Authentisierung soll sie bei Vorliegen der technischen Voraussetzungen, erst ab Dezember 2030, nutzbar sein. Um ihr Potenzial für die digitale Gesundheitsversorgung frühzeitig auszuschöpfen, muss diese zeitliche Staffelung verkürzt werden. Sobald die erforderlichen technischen und sicherheitsbezogenen Voraussetzungen vorliegen, sollte die Wallet auch als Versicherungsnachweis gleichberechtigt eingesetzt werden können.

Die frühere Anerkennung muss mit einer einfachen und offenen Nutzung verbunden werden. Versicherungsstatus und Krankenversichertennummer können über interoperable und datensparsame elektronische Nachweise bereitgestellt werden. Diese sowie anerkannte digitale Identitätsnachweise müssen in allen dafür zugelassenen Anwendungen nutzbar sein, auch in Anwendungen von Drittanbietern. Versicherte dürfen dafür nicht zusätzlich eine bestimmte Krankenkassen-App oder eine separate Identitätsanwendung installieren oder verwenden müssen. Eine erfolgreiche Identifizierung und Authentisierung sollte zugleich für die verbundenen ePA- und Versorgungsfunktionen weiterverwendet werden können, damit nicht für jeden weiteren Nutzungsschritt eine erneute Anmeldung erforderlich ist.

Damit diese Wahlfreiheit praktisch wirksam wird, benötigen auch die Anbieter verlässliche Zugangsbedingungen. Wer die EU-weiten verbindlichen Anforderungen an Identität, Datenschutz, Informationssicherheit, Interoperabilität und Versorgungskontext erfüllt, sollte einen Anspruch auf Anerkennung als berechtigter Dritter haben. Die gematik muss die Anforderungen veröffentlichen und innerhalb einer gesetzlich festgelegten Frist entscheiden.

Auch die Übergangsregelungen sollten sich an diesem offenen Zugang orientieren und unnötige Parallelentwicklungen vermeiden. Die Gesundheits-ID sollte während des Übergangs optional unterstützt werden. Unternehmen, die entsprechende Funktionen bislang nicht anbieten, sollten nicht zu einer kurzfristigen zusätzlichen Umsetzung verpflichtet werden, wenn diese Funktionen bereits sicher über die EUDI-Wallet erbracht werden können. So werden Investitionen auf langfristig anschlussfähige Lösungen ausgerichtet.

Im Gesetzesverfahren sollte sichergestellt werden, dass die Frist für die Nutzung der EUDI-Wallet bei den TI-Anwendungen vom 01.12.2030 auf den 01.12.2029 vorverlagert wird und dass die gematik bis zum 01.12.2028 die technischen Voraussetzungen bei den TI-Anwendungen schafft, um den Rollout dann auch bis zum 01.12.2029 sicherstellen zu können.

Identitätsnachweis und Versorgungskontext trennen

[Zu § 291 Absatz 8, § 339 Absatz 1b und § 345a Absatz 2 SGB V](#)

Der Identitätsnachweis bestätigt, wer der Versicherte ist, und ein Versicherungsnachweis belegt den Versicherungsstatus. Der Nachweis des Versorgungskontexts erfüllt eine andere Aufgabe: Er weist die Berechtigung eines Leistungserbringers für einen konkreten Behandlungsvorgang nach. Alle Verfahren müssen sicher zusammenwirken können. Der Nachweis des Versorgungskontexts sollte aus zugelassenen Anwendungen heraus sicher und interoperabel erfolgen können, ohne einen zusätzlichen, vom Versicherten gesondert durchzuführenden Identifizierungsschritt auszulösen.

Bestehende Zugangswege wie eHealth-CardLink sollten nutzbar bleiben, bis ein sicheres, funktional gleichwertiges und offen zugängliches Nachfolgeverfahren flächendeckend verfügbar ist. Der Übergang muss anhand nachvollziehbarer Kriterien abgesichert werden. Gesetzliche und technische Vorgaben sollten die erforderlichen

Funktionen und Sicherheitsanforderungen beschreiben, statt dauerhaft eine bestimmte technische Ausgestaltung wie »PoPP Stufe 2« festzuschreiben.

Die neue Zugriffsmöglichkeit für Apotheken nach § 339 Absatz 1b ist zu begrüßen. Sie ermöglicht, den zeitlichen Zusammenhang mit der Behandlung anhand der Zugangsdaten eines E-Rezepts nachzuweisen und auf die gesetzlich vorgesehenen Medikationsdaten der ePA zuzugreifen. Dies unterstützt die Prüfung möglicher Wechselwirkungen und Kontraindikationen. Die Möglichkeit sollte sowohl bei der Einlösung über einen Papierausdruck des Tokens als auch bei einer ortsunabhängigen Versorgung über eHealth-CardLink beziehungsweise dessen Nachfolgeverfahren nutzbar sein.

2 gematik und Telematikinfrastruktur

Eine leistungsfähige und stabile TI ist die Grundlage für eine zunehmend digital vernetzte Gesundheitsversorgung. Mit der Weiterentwicklung zur TI 2.0 sollen bestehende technische Komplexität reduziert, die Ausfallsicherheit erhöht und digitale Versorgungsprozesse verbessert werden. Dieses Ziel unterstützen wir ausdrücklich. Betriebsstabilität darf jedoch nicht mit Zentralisierung gleichgesetzt werden. Der GeDIG-Entwurf überträgt der gematik zusätzliche Aufgaben bei Steuerung, Beschaffung und Zulassung sowie neue Eingriffsbefugnisse. Insbesondere der vorgesehene Übergang von wettbewerblichen Zulassungsmodellen zu zentralen Beauftragungsmodellen verändert die bisherige Markt- und Rollenverteilung grundlegend. Eine solche Entscheidung braucht nachvollziehbare Belege dafür, dass sie Sicherheit und Stabilität tatsächlich verbessert.

Aus unserer Sicht sollten zunächst die Instrumente und Prozesse gestärkt werden, die unmittelbar an den Ursachen von Betriebsstörungen ansetzen: verbindliche Qualitätsanforderungen, verlässliche Ersatzsysteme, klare Betriebsabläufe, kontrollierte Updates und belastbare Testverfahren. Klare technische und organisatorische Vorgaben können sicherstellen, dass mehrere Anbieter zuverlässig zusammenwirken. Sie können zugleich Ausfallrisiken und Abhängigkeiten begrenzen.

Dafür braucht es eine klare Rollenverteilung. Die gematik hat eine zentrale Funktion bei der Koordination der TI und bei der Festlegung von Anforderungen an Interoperabilität und Sicherheit. Werden Regelsetzung, Beauftragung, Betrieb, Zulassung und Kontrolle in einer Organisation gebündelt, entstehen Interessenkonflikte. Öffentliche und private Angebote müssen denselben transparenten Anforderungen unterliegen. Entscheidungen über Marktzugang und technische Vorgaben müssen nachvollziehbar und unabhängig überprüfbar sein.

Die Unternehmen der digitalen Gesundheitswirtschaft bringen einen wesentlichen Teil der technischen Expertise und operativen Erfahrung ein. Die Weiterentwicklung der TI sollte deshalb gemeinsam mit der Industrie erfolgen. Spezifikationen, Betriebsmodelle und Umstellungen müssen frühzeitig veröffentlicht und ausreichend konsultiert werden, damit Unternehmen ihre Investitionen und technischen Anpassungen verlässlich planen können.

Marktmodell und Rolle der gematik klar begrenzen

Zu § 311 sowie §§ 323 bis 326 SGB V

Die erweiterten Beauftragungsbefugnisse in § 311 Absatz 1 Nummer 4 und 5 eröffnen der gematik einen erheblichen Gestaltungsspielraum bei Entwicklung, Bereitstellung und Betrieb von TI-Diensten. § 323 Absatz 2 ermöglicht zudem unter bestimmten Voraussetzungen den Eigenbetrieb. Die Erhaltung eines offenen Marktmodells sollte dabei die gesetzliche Leitlinie bleiben.

Bevor weitere Dienste in ein zentrales Beauftragungsmodell überführt werden, braucht es eine vergleichende Bewertung der Handlungsoptionen. Diese muss zeigen, ob verbindliche Betriebs-, Redundanz- und Testanforderungen im bestehenden Zulassungsmodell das Stabilitätsziel ebenso wirksam erreichen können. Für kritische Komponenten sind insbesondere geografisch verteilte Redundanzen, automatisches Umschalten auf Ersatzsysteme und kontrollierte Änderungs- und Releaseprozesse vorzusehen. Die im Entwurf vorgesehene Betreiberzulassung und die zusätzlichen Erprobungs- und Testauflagen sollten als Instrumente zur Stabilisierung genutzt und in ihrer Wirkung bewertet werden.

Kosten, Finanzierung und Transformationsaufwand sind vor Strukturentscheidungen transparent offenzulegen. Auch die Folgen für Wettbewerb, Anschlussvergaben und Anbieterwechsel gehören in die Bewertung. Die Bündelung auf wenige Anbieter kann Abhängigkeiten schaffen und die Weiterentwicklung der Dienste erschweren.

Wenn die gematik verbindliche Entscheidungen gegenüber Marktteilnehmern treffen soll, müssen ihre Befugnisse und Entscheidungsspielräume im Gesetz klar begrenzt werden. Die Rechte der betroffenen Unternehmen, eine eindeutige staatliche Verantwortung und eine wirksame Aufsicht müssen gewährleistet sein. Dies ist gerade aufgrund ihrer privatrechtlichen Organisationsform wichtig. Wenn die gematik zugleich Leistungen selbst erbringt oder beauftragt, entstehen mögliche Interessenkonflikte gegenüber konkurrierenden Anbietern. Ihre Zulassungs- und Aufsichtsfunktion müsste deshalb von ihrer Auftraggeber- und Betreiberfunktion getrennt und unabhängig kontrolliert werden.

Darüber hinaus verstößt die Aufgabenübertragung an die gematik im Wege einer Beleihung (vgl. § 311 Abs. 1a Satz 1 SGB V) gegen den Funktionsvorbehalt aus Art. 33 Abs. 4 GG und kann da her einen Eingriff in die Grundrechte der Marktteilnehmer nicht rechtfertigen. Eine Übertragung hoheitlicher Befugnisse auf eine privatrechtliche Gesellschaft hat Ausnahmecharakter und bedarf laut eines Urteils des Bundesverfassungsgerichts besonderer Rechtfertigung. Der Gesetzgeber hat die wesentlichen Entscheidungen zur Ausgestaltung des Beleihungsverhältnisses selbst zu treffen. Die Substitution einer gesamten Behörde durch eine privatrechtliche Gesellschaft wirft erhebliche Fragen hinsichtlich der demokratischen Legitimation ihres hoheitlichen Handelns und der gebotenen Aufsicht. Diesen Anforderungen genügen die Regelungsinhalte nicht, da der gematik ein weiter Entscheidungsspielraum eingeräumt wird, ohne dass der Gesetzgeber die wesentlichen Vorgaben für die Ausübung dieses Ermessens selbst getroffen hat.

Für Zulassungen nach §§ 324 und 325 müssen objektive, veröffentlichte und überprüfbare Kriterien gelten. Beschränkungen der Anbieterzahl bedürfen eines

konkreten Nachweises ihrer Erforderlichkeit. Die in § 326 vorgesehene pauschale Ausnahme von Zulassung oder Bestätigung für gematik-beauftragte Komponenten und Dienste sollte gestrichen werden. Ein externer Sicherheitsnachweis ersetzt nicht sämtliche Anforderungen an Interoperabilität, Betriebsqualität und laufende Kontrolle.

Langfristige Vergaben dürfen die politische Entscheidung über die künftige Marktstruktur nicht vorwegnehmen. Strukturfestlegende Vergaben zur zusätzlichen Backend-Konsolidierung sollten erst nach Klärung des gesetzlichen Zielbilds und Bewertung der Alternativen erfolgen. Bitkom und seine Mitgliedsunternehmen bieten ihre technische und operative Expertise an, um gemeinsam tragfähige Konzepte für eine stabile TI zu entwickeln.

Betriebsstabilität und verhältnismäßige Eingriffe sichern

Zu §§ 329, 331 und 333 SGB V

Die gematik benötigt wirksame Befugnisse zur Abwehr konkreter Gefahren für Sicherheit und Funktionsfähigkeit der TI. Diese Befugnisse sollten mit einer nachvollziehbaren Eskalation, klaren Zuständigkeiten und verhältnismäßigen Maßnahmen verbunden werden. Nicht jede technische Abweichung rechtfertigt eine Zugangssperre.

Sperrungen nach § 329 Abs. 3 müssen das letzte Mittel bei einer erheblichen konkreten Gefahr sein. Die Erheblichkeit bei der Gefahrenabwehr ist entsprechend der Vermeidung von erheblichen Störungen als Voraussetzung aufzunehmen. Sperrungen sind auf den betroffenen Dienst, die Komponente oder den Zugang zu begrenzen und zeitlich zu befristen, soweit sie zur Gefahrenabwehr notwendig sind. Vorher sind mildere Maßnahmen zu prüfen und die Betroffenen anzuhören. Bei Gefahr im Verzug kann die Anhörung unverzüglich nachgeholt werden. Maßnahmen müssen begründet und unabhängig überprüfbar sein. Zudem sind Sperrungen automatisiert aufzuheben, sobald die angeordneten Maßnahmen zur Gefahrenabwehr umgesetzt wurden oder die erhebliche Gefahr nicht mehr besteht.

Eine Sperrung kann unmittelbar Dokumentation, Verordnung und Kommunikation beeinträchtigen. Da Primärsysteme und TI-Fachdienste nicht kurzfristig austauschbar sind, muss die Versorgungskontinuität ausdrücklich in die Verhältnismäßigkeitsprüfung einbezogen werden. Maßnahmen ohne weitere Ankündigung sollten auf akute Gefahr im Verzug beschränkt bleiben. Die Anweisungsbefugnisse nach § 333 sind mit denselben Verfahrensanforderungen abzustimmen.

Die Überwachung nach § 331 darf externe Systeme nur im für die Sicherheit der TI erforderlichen Umfang erfassen. Ein allgemeiner Zugriff auf außerhalb der TI betriebene Systeme wäre zu weitgehend. Sicherheitsrelevante Schnittstellen, kontrollierte Prüfnutzerzugänge, Protokollierung und der Schutz produktiver personenbezogener Daten sind klar zu regeln. Bestehende nationale und europäische Sicherheitsvorgaben sollten berücksichtigt werden, um widersprüchliche Anforderungen zu vermeiden.

Sichere Kommunikation technologieoffen gestalten

Zu § 295 sowie §§ 363a bis 363c und 363e SGB V

Wir unterstützen die verbindliche Nutzung sicherer Übermittlungsverfahren nach § 363a für die elektronische Kommunikation sowie die Ablösung des Telefax bei der Übermittlung medizinischer und pflegerischer Daten. Die gesetzliche Pflicht sollte sich auf den Rahmen der sicheren Übermittlungsverfahren ausweiten und die Auswahl eines für den jeweiligen Prozess geeigneten Verfahrens ermöglichen.

Für eine effiziente Kommunikation müssen regelmäßig auftretende Geschäfts- und Klärfälle strukturiert und standardisiert übermittelt werden können. Maßgeblich sind Sicherheit, Interoperabilität, Barrierefreiheit und eine praxistaugliche Integration in die Primärsysteme. Unterschiedliche Kommunikationssituationen können unterschiedliche Verfahren erfordern.

§ 363c Absatz 3 sollte deshalb die Nutzung sicherer Übermittlungsverfahren nach § 363a vorsehen. Auch Fachverfahren nach § 363e sollten nicht ausschließlich an den dort bezeichneten sicheren E-Mail-Dienst gebunden werden. Geeignete Messenger-Dienste nach § 363a müssen innerhalb des gesetzlichen Rahmens berücksichtigt werden; daraus folgt keine Verpflichtung zur Nutzung eines bestimmten Messenger-Dienstes.

Für Zulassung und Bereitstellung nach § 363b müssen gleiche Anforderungen für private und körperschaftliche Anbieter gelten. Die gesetzliche Anbieterrolle der Kassenärztlichen Bundesvereinigungen darf keine Bevorzugung ihrer Angebote oder Verdrängung wettbewerblicher Lösungen ermöglichen. Auch hier müssen die Anbieterrolle und hoheitliche Aufgaben klar getrennt werden.

Faire Rahmenbedingungen für Primärsysteme schaffen

Zu § 332a sowie §§ 386a bis 386c SGB V

Die diskriminierungsfreie Einbindung zugelassener TI-Komponenten ist zu unterstützen. In § 332a Absatz 2 sollte jedoch die Formulierung »unabhängig vom Aufwand des Herstellers oder Anbieters« gestrichen werden. Das grundsätzliche Verbot zusätzlicher TI-spezifischer Einbindungskosten bleibt erhalten; tatsächliche Entwicklungs- und Integrationsaufwände müssen bei der Ausgestaltung berücksichtigt werden.

Die Gewährleistung der Datenportabilität nach § 386a muss an klar definierte interoperable Formate und funktionsfähige Schnittstellen nach §371, Abs. 1 Nr. 4 geknüpft sein. Die Pflicht sollte sich auf den Austausch und die Bereitstellung der Daten beziehen. Hersteller benötigen zudem rechtzeitig verfügbare Spezifikationsvorgaben und realistische Umsetzungsfristen.

Kostenfreie standardisierte Exportfunktionen sind von zusätzlichen individuellen Leistungen wie komplexen Konvertierungen, besonderen Migrationen oder Schnittstellenanpassungen abzugrenzen. Umfang, Fristen und Verantwortlichkeiten müssen so bestimmt sein, dass Anbieter und Leistungserbringer ihre Rechte und

Pflichten verlässlich einschätzen können. Diese Abgrenzung ist auch im Umgehungsverbot nach § 386c nachzuvollziehen.

Insbesondere § 386c Absatz 1 Nummer 4 und 5 sollte zwischen einer vollständigen, archivfähigen Übertragung und der automatischen Integration in das Datenmodell eines anderen Systems unterscheiden. Auch nicht standardisierte Datenelemente können für Dokumentation und Archivierung erforderlich sein. Individuelle Freitextfelder und proprietäre Strukturen lassen sich jedoch nicht ohne Weiteres semantisch gleichwertig in jedes Zielsystem übernehmen. Hier braucht es klare Anforderungen, die die vollständige Dokumentation sichern und zugleich technisch umsetzbar sind.

Die Digitalberatung nach § 386b sollte hersteller- und anbieterneutral erfolgen. Einzelne Produkte dürfen durch die Beratungs- und Unterstützungsangebote der Kassenärztlichen Vereinigungen weder bevorzugt noch ohne sachliche Grundlage ausgeschlossen werden.

Industrie frühzeitig beteiligen und Umstellungen planbar machen

Vorschläge für §§ 312a und 316a SGB V

Für Spezifikationen und Standards der gematik sollte eine gesetzliche Mindestkommentierungsfrist von 21 Tagen vorgesehen werden. Bei komplexen Änderungen sind längere Fristen erforderlich. Konsultation, technische Spezifikation, Erprobung und verpflichtende Einführung müssen als nachvollziehbarer Prozess ausgestaltet, sein.

Eine eng umrissene Verordnungskompetenz des Bundesgesundheitsministeriums kann notwendige Anpassungen von Fristen, Übergangsregeln und Sicherheitsvorgaben erleichtern. Grundlegende Entscheidungen über Marktstruktur, Aufgabenverteilung und Eingriffsrechte müssen dem Gesetzgeber vorbehalten bleiben. Die vorgeschlagene Ermächtigung ist entsprechend zu begrenzen.

3 Digitale Versorgungssteuerung

Ein einfacher digitaler Zugang zur Versorgung kann Patientinnen und Patienten schneller zu einer geeigneten Behandlung führen und vorhandene Ressourcen besser nutzbar machen. Digitale Terminvermittlung, strukturierte Bedarfseinschätzung, elektronische Überweisungen und die ePA können hierfür sinnvoll miteinander verbunden werden.

Entscheidend ist, dass aus der besseren Vernetzung keine geschlossene digitale Versorgungskette entsteht. Der Versorgungseinstieg darf weder an ein einzelnes Frontend noch an die Systeme einzelner Institutionen gebunden sein. Versicherte sollten digitale Angebote dort nutzen können, wo ihr Versorgungsbedarf entsteht: über die ePA, eine Anwendung eines Leistungserbringers oder eine andere qualifizierte digitale Anwendung.

Die ePA sollte Gesundheitsdaten sicher verfügbar machen und digitale Versorgungsprozesse unterstützen. Offene und interoperable Schnittstellen müssen ermöglichen, dass Lösungen unterschiedlicher Anbieter auf die benötigten Funktionen zugreifen und miteinander zusammenwirken können. Dabei gelten für alle Beteiligten klare Anforderungen an Datenschutz, Sicherheit und Qualität.

Dies eröffnet auch die Chance, die Arbeitsmedizin stärker mit der regulären Versorgung zu verzahnen – von der Prävention und Früherkennung bis zur Begleitung chronischer Erkrankungen. Der bereits vorgesehene ePA-Zugang für Betriebsärztinnen und Betriebsärzte muss dafür in der Praxis ankommen. Ihre Lese- und Schreibrechte könnten im GeDIG mit dem Ziel einer Gleichbehandlung mit den ärztlichen Kolleginnen und Kollegen in der vertragsärztlichen Versorgung erweitert werden. Auch die Zugriffsdauer ist entsprechend zu prüfen. So kann die ePA helfen, bislang getrennte Präventions- und Versorgungswege miteinander zu verbinden und vorhandene Ressourcen effizienter zu nutzen. All dies trägt zu einer Stärkung der Gesundheitsversorgung Arbeitnehmender bei und entlastet die kassenärztliche Versorgung.

Auch bei Terminvermittlung und Bedarfseinschätzung müssen bestehende digitale Angebote eingebunden und weiterentwicklungsfähig bleiben. Neue gesetzliche Strukturen dürfen bewährte und von Patientinnen, Patienten und Leistungserbringenden genutzte Lösungen weder ohne sachlichen Grund verdrängen noch gegenüber körperschaftlich betriebenen Systemen benachteiligen. Staatliche Vorgaben sollten die Qualität sichern und Raum für unterschiedliche technische Lösungen lassen. So können bewährte Angebote verbessert und neue Anwendungen in die Versorgung integriert werden.

Versorgungseinstieg für qualifizierte Anwendungen öffnen

Zu §§ 342 und 345a SGB V

Der Entwurf verpflichtet Krankenkassen, den digitalen Versorgungseinstieg über die Benutzeroberfläche der ePA anzubieten, und verknüpft wesentliche Funktionen mit Systemen der KBV. Diese Bereitstellung sollte um einen ausdrücklichen und gleichberechtigten Zugang über interoperable und sichere Anwendungen Dritter ergänzt werden. Versicherte müssen die Funktionen auch dort nutzen können, wo ihr Versorgungsbedarf entsteht, etwa in Anwendungen von Leistungserbringern oder anderen qualifizierten Anbietern.

Offene Schnittstellen sollten die Einbindung geeigneter Angebote für Terminvermittlung, Anamnese und Navigation ermöglichen. Zugangsbedingungen sind objektiv und diskriminierungsfrei festzulegen. Die Einbeziehung der Industrie in die Ausgestaltung ist zu begrüßen und sollte auch die konkrete Schnittstellenentwicklung und Umsetzung umfassen.

Die Verarbeitung der bei Terminvereinbarung und Versorgungseinstieg übermittelten Informationen muss anlassbezogen, zweckgebunden und auf das notwendige Maß beschränkt sein. Einwilligungen, Widerrufe und Zugriffsberechtigungen müssen

nachvollziehbar zwischen den eingebundenen Diensten verarbeitet werden können. Die technischen Vorgaben müssen die in Abschnitt 1 beschriebenen Anforderungen an eine einmalige Authentisierung und einen sicheren Nachweis des Versorgungskontexts erfüllen.

Berichtigungsersuchen zu ePA-Daten sollten Versicherte digital und niedrigschwellig auslösen können. Die inhaltliche Prüfung und Korrektur medizinischer Daten bleibt bei den jeweils verantwortlichen Leistungserbringern oder sonstigen datenverarbeitenden Stellen. Krankenkassen sollten solche Ersuchen technisch weiterleiten, ohne daraus eigene Änderungsrechte an medizinischen Inhalten abzuleiten.

Bedarfseinschätzung mit offenen Qualitätsanforderungen verbinden

Zu §§ 360b und 360c SGB V

Eine digitale Bedarfseinschätzung kann bei der Orientierung in die geeignete Versorgung unterstützen. Dafür braucht es evidenzbasierte Verfahren, klare Qualitätsanforderungen und anschlussfähige Ergebnisse. Die in § 360b bereits vorgesehene Beteiligung der Industriebundesverbände ist zu begrüßen.

Die Anforderungen sollten offene und standardisierte Schnittstellen sowie die strukturierte Übermittlung der Ergebnisse ausdrücklich einschließen. Dringlichkeit und weiterer Versorgungsbedarf müssen in Praxisverwaltungssystemen und Terminlösungen verlässlich verarbeitet werden können. Medizinische Anforderungen sind mit dem jeweiligen Versorgungskonzept abzustimmen.

§ 360c sollte keine ausschließliche Betreiberrolle der KBV vorsehen. Alle elektronischen Systeme, die die verbindlichen Anforderungen nach § 360b erfüllen, sollten eine digitale Bedarfseinschätzung bereitstellen können. Die Erfüllung der Anforderungen ist in einem transparenten, diskriminierungsfreien und interessenneutralen Verfahren nachzuweisen. Eine Institution mit eigener Anbieterrolle darf nicht ohne unabhängige Kontrolle über konkurrierende Angebote entscheiden.

Zusätzliche Regulierung von Terminplattformen vermeiden

Zu § 370c SGB V

§ 370c sollte in der derzeitigen Form gestrichen werden. Die Regelung überträgt die Ausgestaltung von Anforderungen und Nachweisverfahren für private Terminbuchungsplattformen auf Akteure, die selbst in diesem Markt tätig oder an seiner Ausgestaltung beteiligt sind. Dies begründet einen strukturellen Interessenkonflikt bei der Festlegung und Durchsetzung der Marktzugangsbedingungen. Das gilt insbesondere, soweit die KBV zugleich ein eigenes Terminvermittlungssystem betreibt.

Digitale Terminangebote leisten einen Beitrag zu nutzerfreundlichen und effizienten Versorgungsprozessen. Zusätzliche Anforderungen müssen daher auf einen konkret belegten Regelungsbedarf gestützt und erforderlich, geeignet und verhältnismäßig ausgestaltet sein. Allgemeine Vorgaben zu Datenschutz und Wettbewerb sowie erforderliche Qualitätsanforderungen gelten unabhängig davon. Ein Sonderregime darf bestehende Funktionen und Geschäftsmodelle nicht ohne ausreichende Begründung einschränken oder ihre Weiterentwicklung behindern.

Sollte ein zusätzlicher Regelungsbedarf nachgewiesen werden, sind die betroffenen Unternehmen frühzeitig einzubeziehen. Grundrechtsrelevante Entscheidungen und die Grenzen untergesetzlicher Vorgaben muss der Gesetzgeber selbst festlegen. Technische Prüfung und Marktteilnahme sind interessenneutral zu organisieren.

Elektronische Überweisungen verlässlich einführen

Zu §§ 73, 86a und 360a SGB V

Wir unterstützen die elektronische Überweisung und die dazu erforderliche Integration in Primärsysteme. Zulassungs- und Schnittstellenanforderungen, Referenzumgebungen und Testwerkzeuge müssen frühzeitig, konsolidiert und abgestimmt verfügbar sein. Zwischen verbindlicher Veröffentlichung der vollständigen Spezifikationen und verpflichtender Umsetzung sollte ein ausreichender Vorlauf vorgesehen werden; für umfangreiche Systemänderungen schlagen wir mindestens 18 Monate vor.

Dies gilt auch für neue Integrations- und Zulassungspflichten bei der Terminmeldung nach § 73 Absatz 9b. Doppelprüfungen sollten vermieden und bereits nachgewiesene Schnittstellenkonformität berücksichtigt werden. Für barrierefreie Funktionen sind praxistaugliche Leitfäden und Referenzumsetzungen bereitzustellen.

Die in § 360a Absatz 5 vorgesehene Löschung 100 Tage nach Einlösung ist von der Gültigkeit und Einlösbarkeit einer Überweisung zu unterscheiden. Aufbewahrung und Löschung müssen nachvollziehbar mit Dokumentationsanforderungen und den Funktionen der ePA abgestimmt werden. Quartalsgrenzen und Regeln zur einmaligen Einlösung sollten so gestaltet sein, dass digitale Prozesse auch bei längeren Wartezeiten funktionieren.

4 EHDS und Gesundheitsdatennutzung

Mit dem EHDS entsteht ein gemeinsamer europäischer Rahmen für die Nutzung elektronischer Gesundheitsdaten in Versorgung, Forschung und Innovation. Deutschland sollte die Umsetzung nutzen, um den Zugang zu Gesundheitsdaten einfacher, verlässlicher und grenzüberschreitend anschlussfähig zu gestalten. Zusätzliche nationale Sonderregelungen dürfen dieses Ziel nicht durch neue Hürden erschweren.

Entscheidend sind klare Zuständigkeiten und praxistaugliche Verfahren. Gesundheitsdateninhaber und Datennutzer benötigen kompetente Ansprechpartner

und müssen wissen, welche Pflichten sie erfüllen sollen. Gerade für die industrielle Gesundheitswirtschaft ist deshalb eine domänenspezifische Zugangsstelle (dHDAB) von zentraler Bedeutung. Unternehmen aus Pharma, Medizintechnik, Diagnostik und Digital Health können sowohl Daten bereitstellen als auch Daten für zulässige Forschungs- und Innovationszwecke nutzen. Die Anforderungen der Branche sind damit sehr heterogen.

Die Besonderheiten dieser Unternehmen müssen beim Aufbau der Zugangsstrukturen berücksichtigt werden. Dazu gehören der Schutz von Geschäftsgeheimnissen und geistigem Eigentum, die Qualität der Daten sowie internationale Forschungsprozesse. Die industrielle Gesundheitswirtschaft sollte deshalb frühzeitig an Aufbau und Ausgestaltung beteiligt werden. Einheitliche digitale Verfahren und eine verlässliche Anbindung an die europäischen Strukturen können unnötige Mehrfacharbeit vermeiden.

Gleichzeitig sollte Deutschland nationale Zusatzanforderungen auf das erforderliche Maß begrenzen. Der EHDS enthält bereits Schutzmechanismen für die Sekundärnutzung, darunter kontrollierte Zugangsverfahren, sichere Verarbeitungsumgebungen, Zweckbindung und behördliche Aufsicht. Weitergehende Anforderungen müssen nachvollziehbar begründet sein und mit dem Ziel eines harmonisierten europäischen Gesundheitsdatenraums vereinbar bleiben.

Für die Vorbereitung brauchen Unternehmen frühzeitig Klarheit darüber, welche Daten bereitzustellen sind, welche technischen Standards gelten und welche Stelle zuständig ist. Rechtsverordnungen und nachgelagerte Vorgaben sollten deshalb rechtzeitig, transparent und gemeinsam mit den betroffenen Akteuren erarbeitet werden.

Zugangsstelle für die industrielle Gesundheitswirtschaft absichern

Zu §§ 9 und 22 GDNG

Der Entwurf sieht domänenspezifische Zugangsstellen (dHDABs) vor und ermöglicht ihre Festlegung durch Rechtsverordnung. Diese Grundlage sollte um eine ausdrückliche und verbindliche Absicherung eines dHDAB für die industrielle Gesundheitswirtschaft ergänzt werden. Eine bloße Möglichkeit lässt für die betroffenen Dateninhaber und Datennutzer wesentliche Fragen der Zuständigkeit und Vorbereitung offen, insbesondere auch in Bezug auf die Beleihung eines Trusted Health Data Holders gem. §22 Abs. 1 Nr. 5d und die Regelungen zu Intermediation Entities gem. §22 Abs. 1 Nr. 5c.

Für den Aufbau der Zugangsstelle sind Pharma-, Medizintechnik-, Diagnostik- und Digital-Health-Unternehmen sowie Infrastruktur- und Technologieanbieter mit ihren jeweiligen Anforderungen einzubeziehen. Auch die Perspektive von KMU und Start-ups muss berücksichtigt werden. Die industrielle Gesundheitswirtschaft sollte frühzeitig an Aufbau, Organisation und praktischer Ausgestaltung beteiligt werden und hat hier klare Bereitschaft durch Initiativen wie sphin-X bereits signalisiert.

Ziel sind einheitliche digitale Antrags- und Bereitstellungsprozesse, standardisierte Schnittstellen und eine klare Zusammenarbeit mit der koordinierenden Zugangsstelle.

Wirtschaftspolitische Belange, insbesondere der Schutz von Geschäftsgeheimnissen, die Innovationsfähigkeit und die internationale Anschlussfähigkeit, müssen in der Governance angemessen vertreten sein.

Zusätzliche nationale Einwilligungspflicht für Omic-Daten vermeiden

Zu § 21 GDNG

§ 21 sieht eine ausdrückliche Einwilligung für die Sekundärnutzung bestimmter Daten nach Artikel 51 Absatz 1 Buchstaben f und g der EHDS-Verordnung vor. Erfasst sind die unter Buchstabe f genannten Daten, proteomische und transkriptomische Daten sowie weitere unter Buchstabe g fallende Daten mit vergleichbarem Re-Identifikationsrisiko.

Eine zusätzliche nationale Opt-in Pflicht würde aus unserer Sicht vermeidbares »Goldplating« schaffen und die europäische Harmonisierung erschweren. Der EHDS sieht bereits kontrollierten Zugang, sichere Verarbeitungsumgebungen, Zweckbindung, Transparenz und Aufsicht vor. Diese Schutzmechanismen sollten für die Sekundärnutzung maßgeblich sein.

Für Bestandsdaten aus klinischen Studien lassen sich zusätzliche Einwilligungen häufig nicht mehr einholen. Sponsoren verfügen regelmäßig nicht über einen direkten Kontakt zu den Teilnehmenden; auch über Studienzentren ist dieser nach Abschluss nicht stets herstellbar. Für künftige Studien entstünden zusätzliche Einwilligungs- und Dokumentationsprozesse. Unvollständige Datensätze können insbesondere bei seltenen Erkrankungen und kleinen Patientengruppen die Aussagekraft der Forschung beeinträchtigen.

Wir fordern deshalb, § 21 GDNG zu streichen und auf die zusätzliche nationale Einwilligungspflicht zu verzichten. Hilfsweise sollte mindestens Absatz 1 Nummer 3 entfallen. Die dort verlangte Bewertung eines vergleichbaren Re-Identifikationsrisikos erzeugt zusätzliche Abgrenzungs- und Dokumentationsunsicherheit für Gesundheitsdateninhaber.

Pflichten der Gesundheitsdateninhaber praktikabel gestalten

Zu §§ 3, 16, 20 und 22 sowie §§ 14 und 30 GDNG

Die Forschungskennziffer nach § 3 kann die datenschutzkonforme Verknüpfung von Daten und die Umsetzung von Widerspruchsrechten unterstützen. Sie muss jedoch auch für industrielle Dateninhaber praktikabel sein. In historischen Studienbeständen fehlt häufig die für die Generierung vorgesehene Krankenversicherungsnummer. Dafür sind rechtssichere ergänzende Verfahren erforderlich, die die Nutzbarkeit der Bestandsdaten erhalten.

Dateninhaber sollten die technische Erzeugung durch qualifizierte zentrale Dienste vornehmen lassen können. Einheitliche Regeln für Zuordnung, Datenqualität,

Korrekturen und Nachmeldungen sind erforderlich. Verbindliche Vorgaben zur Kennziffer müssen die tatsächliche Verfügbarkeit der Ausgangsdaten und angemessene Übergänge berücksichtigen. Eine zuverlässige Datenverknüpfung darf nicht an praktisch unerfüllbaren Pflichten scheitern.

Das Widerspruchsregister nach § 16 sollte verständlich, technisch schlank und mit bestehenden Strukturen abgestimmt sein. Ein einheitlicher Widerspruch gegen die Sekundärnutzung sollte den einfachen Regelfall bilden. Zusätzliche Differenzierungen nach Nutzungszwecken sind auf ihre unionsrechtliche Erforderlichkeit und den damit verbundenen Umsetzungsaufwand zu prüfen. Die Rechte betroffener Personen müssen zuverlässig und über alle beteiligten Stellen hinweg umgesetzt werden.

Die elektronische Kommunikation nach § 20 sollte verbindlicher Standard sein. Für Dateninhaber braucht es möglichst durchgängig digitale Abläufe statt paralleler Papierverfahren. Gebühren- und Sanktionsregelungen sollten verhältnismäßig, transparent und europäisch anschlussfähig ausgestaltet werden. Zusätzliche nationale Belastungen sind zu vermeiden.

§ 22 Absatz 1 Nummer 5 Buchstabe a ermöglicht bereits eine Regelung für Datensätze, die bei mehreren Gesundheitsdateninhabern vorliegen. Diese Ermächtigung muss rechtzeitig ausgefüllt werden. Unternehmen benötigen Klarheit darüber, wer welchen Datensatz bereitstellt und wie unnötige Mehrfachanforderungen vermieden werden. Auch weitere technische und organisatorische Pflichten sind frühzeitig und unter Beteiligung der betroffenen Akteure zu konkretisieren.

Daten für Forschung und iterative Entwicklung nutzbar machen

Zu § 25 GDNG sowie §§ 303e, 342 und 345b SGB V

Die Möglichkeit zur Verknüpfung von FDZ-Daten mit externen pseudonymisierten Daten ist zu begrüßen. Sie sollte über die vorgesehenen Qualitätssicherungsaufgaben hinaus für weitere berechnigte Akteure und zulässige Forschungs- und Innovationszwecke nach § 303e geöffnet werden. Die Ausleitung von ePA-Daten sollte mit einer verlässlichen Strukturierung und Qualitätsprüfung verbunden werden, damit die Daten tatsächlich nutzbar sind.

Bei § 25 GDNG sind längerfristige und iterative Vorhaben zu berücksichtigen, etwa Training, Validierung und Weiterentwicklung von KI-Systemen innerhalb eines definierten Forschungszwecks. Genehmigungen sollten auch klar beschriebene, wiederkehrende Verarbeitungsschritte und längere, dem Vorhaben angemessene Zeiträume abdecken können. Zweckbindung, behördliche Kontrolle und Schutz der Betroffenen bleiben erforderlich. Eine pauschale Begrenzung darf solche Vorhaben nicht ohne sachlichen Grund ausschließen.

Die datengestützte Information über klinische Studien nach § 345b ist zu begrüßen. Bestehende europäische Informationssysteme, insbesondere CTIS und die Trials Map der EMA, sollten interoperabel eingebunden werden, um zusätzliche Melde- und Pflegeaufwände zu vermeiden. Abgleichverfahren müssen qualitätsgesichert und

nachvollziehbar sein; die Expertise der Industrie sollte bei ihrer Entwicklung genutzt werden. Ein Opt-out-Modell für den Abgleich geeigneter Studien sollte geprüft werden.

Für die Strukturierung und Ausleitung von ePA-Daten sollten die Spezifikationen maschinenlesbare Angaben zu Herkunft und Version der Daten sowie eine klare Kennzeichnung maschinell abgeleiteter Inhalte vorsehen. Plausibilitäts- und Widerspruchsprüfungen sowie eine risikobasierte fachliche Verifikation gegen die Ausgangsdokumentation sollten bereits beim Dateninhaber unterstützt werden. Korrekturen sollten in abgeleiteten Datensätzen und wiederkehrenden Validierungen nachvollziehbar berücksichtigt werden können, unter Wahrung von Pseudonymisierung, Zweckbindung und Zugriffsrechten.

So ließe sich auch bei wiederholter KI-Validierung nachvollziehen, auf welchem Datenstand ein Ergebnis beruht und ob Korrekturen berücksichtigt wurden.

Technische Umsetzung und unabhängige Aufsicht trennen

Zu § 383a SGB V

Die Aufgaben der Stellen für digitale Gesundheit betreffen die Primärnutzung und sind von den Zugangsstellen für die Sekundärnutzung zu unterscheiden. Auch hier sollten technische Umsetzung, koordinierende Aufsicht und Beschwerdeentscheidung so verteilt werden, dass strukturelle Interessenkonflikte vermieden werden. Die gematik sollte ihre technische Kompetenz einbringen können, ohne zugleich allein über Beschwerden gegen eigene Vorgaben oder Dienste zu entscheiden. Beschwerdeverfahren müssen organisatorisch unabhängig und nachvollziehbar ausgestaltet sein.

5 Weitere konkrete Versorgungsanliegen

Neben den übergreifenden Strukturfragen enthält der Entwurf Regelungen, die unmittelbar für die Versorgung und die Entwicklung digitaler Lösungen relevant sind. Die folgenden Änderungen sollten ergänzend berücksichtigt werden.

Kombinierte Fernüberwachungsmodelle ermöglichen

Zu § 33a SGB V

Die ausdrückliche Einbeziehung von DiGA zur Fernüberwachung ist zu begrüßen. Der Normtext sollte klarstellen, dass solche Anwendungen in Kombination mit der Versorgung durch Leistungserbringer eingesetzt werden können und deren Einbeziehung zum positiven Versorgungseffekt beitragen kann. Rein digitale und kombinierte Versorgungsmodelle dürfen nicht ohne sachlichen Grund unterschiedlich behandelt werden.

DiGA Verordnungen niedrigschwellig einlösbar gestalten

Zu § 360 Absatz 4 und § 361b SGB V

Wir begrüßen das in der Gesetzesbegründung formulierte Ziel, einfache Einlösewege für elektronische DiGA-Verordnungen zu schaffen. Dieses Ziel muss jedoch durch verbindliche Vorgaben im Normtext abgesichert werden. Die vorgesehene Befugnis der Krankenkassen und weiteren Kostenträger, Verordnungsdaten zu verarbeiten, lässt noch offen, wie daraus ein einfacher und durchgängiger Einlöseprozess entsteht.

Hohe Anforderungen an die digitale Authentifizierung erschweren bislang den Zugang. Viele Versicherte verfügen weder über eine PIN für ihre elektronische Gesundheitskarte noch über eine vollständig eingerichtete GesundheitsID. Technische Hürden und zusätzliche Handlungsschritte können deshalb dazu führen, dass eine ärztlich verordnete DiGA nicht genutzt wird. Die elektronische Verordnung muss so gestaltet werden, dass auch Menschen mit wenig digitaler Erfahrung zuverlässig Zugang zur Versorgung erhalten.

Dafür sollten elektronische DiGA-Verordnungen automatisiert an den zuständigen Kostenträger übermittelt und dort verarbeitet werden können, ohne dass Versicherte zuvor gesondert aktiv werden müssen. Der Kostenträger sollte die Verordnung automatisiert bearbeiten und den Freischaltcode bereitstellen. Die Verarbeitung der Verordnung ist dabei von der tatsächlichen Nutzung zu unterscheiden: Eine abrechnungsrelevante Inanspruchnahme soll weiterhin erst erfolgen, wenn Versicherte den Freischaltcode aktivieren und die Nutzung der DiGA beginnen.

Sollte für den Zugriff des Kostenträgers eine gesonderte Autorisierung erforderlich sein, muss diese möglichst niedrigschwellig erfolgen können. In Anlehnung an § 361c Absatz 3 sollte klargestellt werden, dass eine Autorisierung auch ohne die Zugangsdaten nach § 360 Absatz 9 oder eine digitale Identität nach § 291 Absatz 8 möglich ist. Diese Regelung soll den automatisierten Prozess ergänzen, soweit eine Autorisierung notwendig bleibt.

Solange die digitalen Einlösewege noch nicht zuverlässig und flächendeckend nutzbar sind, muss eine praktikable Alternative erhalten bleiben. Leistungserbringer sollten Versicherten deshalb ergänzend zur elektronischen Übermittlung bis zum 31. Dezember 2028 einen papiergebundenen Ausdruck der Verordnung aushändigen. Damit wird verhindert, dass infrastrukturelle Defizite oder Schwierigkeiten bei der digitalen Anmeldung zu Versorgungslücken führen.

Zugleich ist die Plattformneutralität der Einlösewege gesetzlich abzusichern. Webanwendungen und native Applikationen müssen hinsichtlich Funktionalität und Erreichbarkeit gleichgestellt sein. Die technischen Vorgaben dürfen keine bestimmte Softwarearchitektur bevorzugen oder benachteiligen. So bleibt der Zugang unabhängig von der technischen Ausgestaltung einer DiGA gewährleistet.

Weitere elektronische Verordnungen konsequent voranbringen

[Zu § 360 Absatz 7 SGB V](#)

Die Verschiebung der verpflichtenden Einführung elektronischer Verordnungen für weitere Leistungsbereiche, etwa Hilfsmittel, bleibt hinter dem Anspruch zurück, die Digitalisierung der Versorgung konsequent voranzutreiben. Erforderlich ist eine verbindliche und ambitionierte Roadmap mit verlässlichen Entwicklungs-, Test- und Einführungszeiträumen.

Auch der ärztliche Sprechstundenbedarf sollte in die elektronische Verordnung einbezogen werden. Die weiterhin papiergebundene Beschaffung verursacht Medienbrüche und zusätzlichen Aufwand. Gerade im Zusammenhang mit dem vorgesehenen Dispensierrecht für Ärztinnen und Ärzte in Notfällen muss auch die Beschaffung der benötigten Arzneimittel digital unterstützt werden. Wir schlagen deshalb vor, die elektronische Verordnung des Sprechstundenbedarfs ab dem 1. Januar 2027 verbindlich vorzusehen.

Reallabore für gemeinsame Innovation öffnen

[Zu § 284a SGB V und einer Folgeänderung in § 4 Absatz 5 SGB V](#)

Reallabore können einen wichtigen Beitrag zur Erprobung datenbasierter Versorgungsansätze leisten. Der Erprobungsrahmen sollte geeignete privatwirtschaftliche Akteure, Technologiepartner sowie Forschungs- und Infrastrukturanbieter unter transparenten Bedingungen einbeziehen. Über kassengetragene Kooperationen hinaus sollte eine Öffnung für weitere geeignete Träger geprüft werden.

Für gemeinsame Reallabore sollten das zweckgebundene Zusammenführen von Daten beteiligter Akteure und eine Anpassung des genehmigten Erprobungsumfangs ausdrücklich geregelt werden. Offene Standards, nachvollziehbare Qualitätsanforderungen und Kontrolle der eingesetzten Verfahren sind erforderlich.

Medikationsplan und Impfmanagement interoperabel weiterentwickeln

[Zu §§ 31a und 350 SGB V](#)

Das in § 31a Absatz 5 vorgesehene, vom Speicherort unabhängige einheitliche Format des Medikationsplans und das technische Einvernehmen mit der Gematik sind zu begrüßen. Bei der Umsetzung sollten die Spezifikationen des elektronischen Medikationsplans als verbindliche technische Grundlage dienen. Inhalte in Primärsystemen, ePA und Papierdarstellung müssen konsistent und für die Versorgung verlässlich nutzbar sein.

Die Weiterentwicklung des digitalen Impfmanagements in der ePA ist ein wichtiger Schritt, um Versicherten einen besseren Überblick über ihren Impfstatus zu geben und die Impfquoten zu verbessern. Positiv ist insbesondere die verpflichtende Information über anstehende empfohlene Impfungen nach § 350 Absatz 4. Bei der Umsetzung sollte sichergestellt werden, dass diese Informationen über die ePA auch per einfach aktivierbarer Push-Benachrichtigung übermittelt werden können.

Zugleich sollte die digitale Impfübersicht zügig zu einem vollständigen e-Impfpass auf Basis der ärztlichen Impfdokumentation weiterentwickelt werden. Abrechnungsdaten sind hierfür nur eine Übergangslösung: Sie stehen häufig erst mit deutlicher Verzögerung zur Verfügung, erfassen etwa Impfungen durch Betriebsärzte, den Öffentlichen Gesundheitsdienst oder privat abgerechnete Reiseimpfungen nicht vollständig und enthalten nicht alle für eine verlässliche Impfdokumentation relevanten Angaben. Im GeDIG sollte der auf dem entsprechenden MIO basierende e-Impfpass daher bereits verbindlich mit einer konkreten Frist verankert werden, spätestens zum 26. März 2029 im Zusammenhang mit der Umsetzung der elektronischen Patientenakte nach dem EHDS.

Cloud-Regelungen praxistauglich umsetzen

Zu § 393 SGB V

Die vorgesehene Konkretisierung der technischen Vorgaben zum Cloud-Einsatz im Gesundheitswesen ist zu begrüßen. Da Cloud-Technologie bereits in vielen Bereichen der Versorgung eingesetzt wird, sollte für die Umsetzung der konkretisierten Anforderungen eine sechsmonatige Übergangsfrist vorgesehen werden. Damit erhalten die betroffenen Anbieter und Einrichtungen ausreichend Zeit, bestehende Systeme zu prüfen und erforderliche technische Anpassungen geordnet umzusetzen.

Einwilligungsbasierte Datenausleitung aus der ePA praktisch ermöglichen

Zu § 363 Absatz 8 SGB V und § 16 FDZGesV

Die gesetzlich vorgesehene Möglichkeit, ePA-Daten auf Grundlage einer informierten Einwilligung für Forschungszwecke bereitzustellen, sollte zügig praktisch nutzbar werden. Sie ergänzt den Zugang über das Forschungsdatenzentrum Gesundheit und ermöglicht Versicherten, Forschungsvorhaben unmittelbar und selbstbestimmt zu unterstützen. Dies stärkt die Beteiligung an der Forschung und das Vertrauen in die Nutzung von Gesundheitsdaten.

Bei der Konzeption durch die gematik sollten neben Forschungseinrichtungen und Patientenvertretungen auch die industrielle Gesundheitswirtschaft verbindlich eingebunden und technische Vorschläge weiterer geeigneter Akteure berücksichtigt werden.

Voraussetzung sind offene Schnittstellen, eine sichere und datenschutzkonforme Datenbereitstellung sowie transparente Einwilligungsprozesse. Versicherte müssen

nachvollziehen können, welche Daten sie welchen Empfängern für welche Forschungszwecke zur Verfügung stellen. Die Datenschutzaufsicht sollte frühzeitig eingebunden werden.

Fazit

Digitalisierung gemeinsam wirksam umsetzen

Durch das GeDIG sollte digitale Versorgung im Alltag erleichtert und Unternehmen verlässliche Bedingungen für Entwicklung und Betrieb geben werden. Dafür braucht es offene Zugänge, verbindliche Standards und planbare Übergänge. Die technische und operative Erfahrung der digitalen Gesundheitswirtschaft sollte frühzeitig in die Umsetzung einfließen.

Eine konsequente Digital-first-Politik muss sich in den gesetzlichen Verfahren und ihrer praktischen Umsetzung zeigen. Forschung und Innovation entfalten ihren Nutzen, wenn geeignete Lösungen in die Versorgung gelangen, weiterentwickelt werden können und unter fairen Bedingungen miteinander im Wettbewerb stehen. Bitkom und seine Mitgliedsunternehmen stehen bereit, diesen Weg gemeinsam mit Politik, Selbstverwaltung und Leistungserbringern zu gestalten.

Anhang

Änderungen SGBV

GesetzE § 31a SGBV	Bitkom-Vorschlag
(3) Hat der Versicherte eine elektronische Patientenakte, ist der Medikationsplan dort nach § 347 Absatz 1 zu speichern. Hat der Versicherte keine elektronische Patientenakte oder hat er nach § 353 Absatz 1 der Verarbeitung der Daten aus dem Medikationsplan in der elektronischen Patientenakte oder nach § 353 Absatz 2 dem Zugriff des Arztes, der den Medikationsplan erstellt oder aktualisiert, auf Daten der elektronischen Patientenakte widersprochen, hat der Arzt den Medikationsplan in dem von ihm genutzten informationstechnischen System zu speichern.	(3) Hat der Versicherte eine elektronische Patientenakte, ist der Medikationsplan dort nach § 347 Absatz 1 zu speichern. Hat der Versicherte keine elektronische Patientenakte oder hat er nach § 353 Absatz 1 der Verarbeitung der Daten aus dem Medikationsplan in der elektronischen Patientenakte oder nach § 353 Absatz 2 dem Zugriff des Arztes, der den Medikationsplan erstellt oder aktualisiert, auf Daten der elektronischen Patientenakte widersprochen, hat der Arzt den Medikationsplan in dem von ihm genutzten informationstechnischen System zu speichern. Der Medikationsplan ist unabhängig vom Speicherort in einem einheitlichen, durch die Vereinbarung nach Absatz 4 festgelegten Format zu erstellen; abweichende Formate oder Datenstrukturen sind unzulässig.
(4) Inhalt, Struktur und die näheren Vorgaben zur Erstellung und Aktualisierung des Medikationsplans sowie ein Verfahren zu seiner Fortschreibung vereinbaren [...] im Einvernehmen mit der Gesellschaft für Telematik. In der Vereinbarung ist ein vom Speicherort unabhängiges einheitliches Format des Medikationsplans festzulegen.[...]	(4) Ergänzung Die Vereinbarung nach Satz 1 hat sicherzustellen, dass das Format des im Primärsystem des Arztes gespeicherten und auf Wunsch des Versicherten ausgedruckten Medikationsplans mit dem Format des in der elektronischen Patientenakte gespeicherten Medikationsplans inhaltlich und strukturell vollständig übereinstimmt; eine Parallelführung unterschiedlicher Formate ist unzulässig. Die Gesellschaft für Telematik stellt sicher, dass die technischen Spezifikationen des elektronischen Medikationsplans als verbindliche Grundlage für die Vereinbarung nach Satz 1 dienen.
GesetzE § 33a SGBV	Bitkom-Vorschlag
(1) Der Anspruch nach Satz 1 umfasst auch solche digitalen Gesundheitsanwendungen, die der Fernüberwachung des Gesundheitszustands von Versicherten mithilfe digitaler Technologien dienen."	Der Anspruch nach Satz 1 umfasst auch solche digitalen Gesundheitsanwendungen, die der Fernüberwachung des Gesundheitszustands von Versicherten mithilfe einer Kombination der digitalen Technologien und der Versorgung durch Leistungserbringer dienen.

GesetzE §284 a SGBV	Bitkom-Vorschlag
(1) Krankenkassen können mit Genehmigung der Aufsichtsbehörde Reallabore errichten, in denen innovative Ansätze zur Nutzung von personenbezogenen Daten, einschließlich besonderer Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, zur Erfüllung ihrer nach diesem Buch übertragenen Aufgaben befristet erprobt werden dürfen. Abweichend von § 284 Absatz 1 dürfen die am Reallabor beteiligten Krankenkassen personenbezogene Daten ihrer Versicherten nach Maßgabe der Genehmigung nach Absatz 2 und in dem gemäß Absatz 4 Satz 1 festgelegten Umfang der Erprobung verarbeiten.	(1) Krankenkassen können mit Genehmigung der Aufsichtsbehörde Reallabore errichten, in denen innovative Ansätze zur Nutzung von personenbezogenen Daten, einschließlich besonderer Kategorien personenbezogener Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, zur Erfüllung ihrer nach diesem Buch übertragenen Aufgaben befristet erprobt werden dürfen. Abweichend von § 284 Absatz 1 dürfen die am Reallabor beteiligten Krankenkassen personenbezogene Daten ihrer Versicherten sowie weitere personenbezogene Daten nach Maßgabe der Genehmigung nach Absatz 2 und in dem gemäß Absatz 4 Satz 1 festgelegten Umfang der Erprobung verarbeiten. Krankenkassen die gemäß Absatz 3 gemeinsam an einem Datenlabor beteiligt sind, dürfen für die Zwecke des Reallabors Daten die von ihnen zur Erfüllung ihrer Aufgaben erhoben oder an sie übermittelt wurden mit den Daten anderer am Reallabor beteiligter Krankenkassen zusammenführen und gemeinsam nutzen.
(4) Die zuständige Aufsichtsbehörde legt in der Genehmigung nach Absatz 2 fest, in welchem Umfang und unter welchen Bedingungen die Erprobung einer Datenverarbeitung im Reallabor ermöglicht wird sowie von welchen bundesrechtlichen Regelungen gegebenenfalls abgewichen werden darf. [...]	(4) Die zuständige Aufsichtsbehörde legt in der Genehmigung nach Absatz 2 fest, in welchem Umfang und unter welchen Bedingungen die Erprobung einer Datenverarbeitung im Reallabor ermöglicht wird sowie von welchen bundesrechtlichen Regelungen gegebenenfalls abgewichen werden darf. Auf Antrag der am Reallabor beteiligten Krankenkassen kann die zuständige Aufsichtsbehörde den Umfang der Erprobung eines bereits errichteten Reallabors anpassen. [...]
	Folgeänderung: § 4 SGBV Absatz 5 wird wie folgt ergänzt „(5) Ab dem Haushaltsjahr 2027 dürfen sich die Verwaltungsausgaben einer Krankenkasse mit Ausnahme der Verwaltungsausgaben der landwirtschaftlichen Krankenkasse und der knappschaftlichen Krankenversicherung im Verhältnis zu ihren Verwaltungsausgaben im jeweils vorangegangenen Haushaltsjahr nur nach Maßgabe der für das jeweilige Kalenderjahr nach § 71 Absatz 3 Satz 5 veröffentlichten durchschnittlichen Veränderungsrate je Versicherten erhöhen. Die Begrenzung nach Satz 1 gilt nicht für Aufwendungen zum Schutz der kritischen Infrastruktur im Bereich Sicherheit der Informationstechnik sowie für Aufwendungen, die für die Durchführung der Sozialversicherungswahlen als Online-Wahl entstehen sowie für Anwendungen für Reallabore nach § 284a. Für die Verwaltungsausgaben der knappschaftlichen

GesetzE §284 a SGBV	Bitkom-Vorschlag
	Krankenversicherung gilt § 18a Absatz 2 des Zweiten Gesetzes über die Krankenversicherung der Landwirte entsprechend.

GesetzE § 291 SGB V	Bitkom-Vorschlag
Absatz 8 wird wie folgt geändert: aa) Nach Satz 3 werden die folgenden Sätze eingefügt: „Ab dem 1. Dezember 2028 dient die Europäische Briefftasche für die Digitale Identität nach Artikel 3 Nummer 42 der Verordnung (EU) Nr. 910/2014 in Verbindung mit entsprechenden elektronischen Nachweisen in der Briefftasche in gleicher Weise wie die elektronische Gesundheitskarte als Versicherungs-nachweis nach § 291a Absatz 1. Sobald die technischen Voraussetzungen vorliegen, spätestens jedoch ab dem 1. Dezember 2030, dient die Europäische Briefftasche für die Digitale Identität nach Artikel 3 Nummer 42 der Ver-ordnung (EU) Nr. 910/2014 in Verbindung mit entsprechenden elektronischen Nachweisen in der Briefftasche der Authentisierung des Versicherten im Gesundheitswesen in gleicher Weise wie die elektronische Gesundheitskarte.“	Absatz 8 wird wie folgt geändert: aa) Nach Satz 3 werden die folgenden Sätze eingefügt: „Ab dem 1. Dezember 2028 dient die Europäische Briefftasche für die Digitale Identität nach Artikel 3 Nummer 42 der Verordnung (EU) Nr. 910/2014 in Verbindung mit entsprechenden elektronischen Nachweisen in der Briefftasche in gleicher Weise wie die elektronische Gesundheitskarte als Versicherungs-nachweis nach § 291a Absatz 1. Sobald die technischen Voraussetzungen vorliegen, spätestens jedoch ab dem 1. Dezember 2030, dient die Europäische Briefftasche für die Digitale Identität nach Artikel 3 Nummer 42 der Ver-ordnung (EU) Nr. 910/2014 in Verbindung mit entsprechenden elektronischen Nachweisen in der Briefftasche der Authentisierung des Versicherten im Gesundheitswesen in gleicher Weise wie die elektronische Gesundheitskarte.“ Die nach diesem Absatz anerkannten elektronischen Identitäts- und Versicherungsnachweise sind in allen hierfür zugelassenen Anwendungen und Diensten der Telematikinfrastruktur gleichberechtigt und diskriminierungsfrei nutzbar. Ihre Nutzung darf nicht davon abhängig gemacht werden, dass der Versicherte eine bestimmte Anwendung eines Kostenträgers oder eine gesonderte Identitätsanwendung installiert oder verwendet.“
Der neue Satz 15 wird durch den folgenden Satz ersetzt: Darüber hinaus kann die Gesellschaft für Telematik durch verbindlichen Be-schluss nach § 315 Absatz 1 Satz 1 Anbieter weiterer Dienste oder Anwendungen nach § 306 Absatz 1 Satz 2 Nummer 2 Buchstabe a als berechnigte Dritte diskriminierungsfrei festlegen.	Der neue Satz 15 wird durch den folgenden Satz ersetzt: „Darüber hinaus kann die Gesellschaft für Telematik durch verbindlichen Be-schluss nach § 315 Absatz 1 Satz 1 Anbieter weiterer Dienste oder Anwen-dungen nach § 306 Absatz 1 Satz 2 Nummer 2 Buchstabe a als berechnigte Dritte diskriminierungsfrei festlegen.“ Anbieter weiterer Dienste oder Anwendungen nach § 306 Absatz 1 Satz 2 Nummer 2 Buchstabe a sind als berechnigte Dritte anzuerkennen, wenn sie die gesetzlich und durch Rechtsverordnung festgelegten Anforderungen an Identität, Datenschutz,

GesetzE § 291 SGB V	Bitkom-Vorschlag
	Informationssicherheit, Interoperabilität und Versorgungskontext erfüllen. Die Gesellschaft für Telematik veröffentlicht die Anforderungen und entscheidet über die Anerkennung innerhalb einer gesetzlich bestimmten Frist. Eine Ablehnung ist zu begründen und muss unabhängig überprüfbar sein.

GesetzE § 311 SGBV	Bitkom-Vorschlag
(1) 4. Vergabe von Aufträgen an Anbieter für die Entwicklung, die Zurverfügungstellung und den Betrieb von Komponenten und Diensten der Telematikinfrastruktur und Zulassung von Komponenten und Diensten der Telematikinfrastruktur einschließlich der Verfahren zum Zugriff auf diese Komponenten und Dienste,	4. Vergabe von Aufträgen an Anbieter für die Entwicklung, die Zurverfügungstellung und den Betrieb von Komponenten und Diensten der Telematikinfrastruktur und Zulassung von Komponenten und Diensten der Telematikinfrastruktur einschließlich der Verfahren zum Zugriff auf diese Komponenten und Dienste, sowie Festlegung der Rahmenbedingungen.
5. Vergabe von Aufträgen an Anbieter für die Entwicklung, die Zurverfügungstellung und den Betrieb von sicheren Diensten für Verfahren zur Übermittlung medizinischer und pflegerischer Daten über die Telematikinfrastruktur und Zulassung von sicheren Diensten für Verfahren zur Übermittlung medizinischer und pflegerischer Daten über die Telematikinfrastruktur	5. Vergabe von Aufträgen an Anbieter für die Entwicklung, die Zurverfügungstellung und den Betrieb von sicheren Diensten für Verfahren zur Übermittlung medizinischer und pflegerischer Daten über die Telematikinfrastruktur und Zulassung von sicheren Diensten für Verfahren zur Übermittlung medizinischer und pflegerischer Daten über die Telematikinfrastruktur, sowie Festlegung der Rahmenbedingungen

GesetzE §325 SGBV	Bitkom-Vorschlag
(1) Die Komponenten und Dienste der Telematikinfrastruktur bedürfen der Zulassung durch die Gesellschaft für Telematik. Dabei ist nachzuweisen, dass die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Komponenten und Dienste sichergestellt werden. Im Fall einer Ausschreibung der Komponenten und Dienste durch die Gesellschaft für Telematik nach § 311 Absatz 1 Satz 1 Nummer 4 und 5 ist die Sicherheit der Komponenten und Dienste durch ein externes Sicherheitsgutachten nachzuweisen.	(1) Die Komponenten und Dienste der Telematikinfrastruktur bedürfen der Zulassung durch die Digitalagentur Gesundheit. Dabei ist nachzuweisen, dass die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Komponenten und Dienste sichergestellt werden. Im Fall einer Ausschreibung der Komponenten und Dienste durch die Gesellschaft für Telematik nach § 311 Absatz 1 Satz 1 Nummer 4 und 5 ist die Sicherheit der Komponenten und Dienste durch ein externes Sicherheitsgutachten nachzuweisen. Soweit verbindliche Rahmenbedingungen festgelegt wurden, sind diese Teil der zulassungsrelevanten Kriterien.

GesetzE § 326 SGB V	Bitkom-Vorschlag
Anbieter und Betreiber von Komponenten und Diensten der Telematikinfrastruktur müssen über die nach § 323 Absatz 2 und § 325 Absatz 1 erforderliche Zulassung oder über die nach § 327 Absatz 2 Satz 1 erforderliche Bestätigung verfügen, bevor sie die Telematikinfrastruktur nutzen. Für Komponenten und Dienste, die von der Gesellschaft für Telematik in Auftrag gegeben wurden, ist abweichend von Satz 1 eine Zulassung oder eine Bestätigung nicht erforderlich.	Anbieter und Betreiber von Komponenten und Diensten der Telematikinfrastruktur müssen über die nach § 323 Absatz 2 und § 325 Absatz 1 erforderliche Zulassung oder über die nach § 327 Absatz 2 Satz 1 erforderliche Bestätigung verfügen, bevor sie die Telematikinfrastruktur nutzen. Für Komponenten und Dienste, die von der Gesellschaft für Telematik in Auftrag gegeben wurden, ist abweichend von Satz 1 eine Zulassung oder eine Bestätigung nicht erforderlich.

GesetzE §329 SGBV	Bitkom-Vorschlag
(3) Die Gesellschaft für Telematik kann zur Abwehr von Gefahren für die Betriebsstabilität der Telematikinfrastruktur im Einzelfall und zur Vermeidung von erheblichen betrieblichen Störungen der Telematikinfrastruktur insbesondere Komponenten, Dienste sowie informationstechnische Systeme mit den technischen Schnittstellen und Modulen, die zur Nutzung der Telematikinfrastruktur im Gesundheitswesen erforderlich sind, oder einzelne Nutzer für den Zugang zur Telematikinfrastruktur sperren. Sie kann diesen Nutzern den weiteren Zugang zur Telematikinfrastruktur unter der Bedingung gestatten, dass die von der Gesellschaft für Telematik angeordneten Maßnahmen zur Gefahrenabwehr umgesetzt werden. Die Gesellschaft für Telematik kann den nach § 324 zugelassenen Anbietern und Betreibern sowie Anbietern, die eine Zulassung für Komponenten oder Dienste der Telematikinfrastruktur nach § 363a sowie § 325 oder eine Bestätigung nach § 327 besitzen, zur Beseitigung oder Vermeidung von Störungen nach Absatz 2 verbindliche Anordnungen erteilen, insbesondere 1. zur Meldung von Störungen, von festgestellten Schwachstellen eines Dienstes und von Sicherheitsvorfällen an die Gesellschaft für Telematik sowie zu Fristen, innerhalb derer diese Meldung zu erstatten ist, 2. zur Ergreifung von Maßnahmen zur Beseitigung oder Vermeidung von Störungen, von festgestellten Schwachstellen eines Dienstes und von Sicherheitsvorfällen sowie zu Fristen, innerhalb derer diese Maßnahmen umzusetzen sind, 3. zur Ergreifung von Maßnahmen bei beabsichtigten Änderungen in der Ausführung von Betriebsleistungen	„ (3) Die Gesellschaft für Telematik kann zur Abwehr von erheblichen Gefahren für die Betriebsstabilität im Einzelfall und zur Vermeidung von erheblichen betrieblichen Störungen der Telematikinfrastruktur insbesondere Komponenten, Dienste sowie informationstechnische Systeme mit den technischen Schnittstellen und Modulen, die zur Nutzung der Telematikinfrastruktur im Gesundheitswesen erforderlich sind, oder einzelne Nutzer für den Zugang zur Telematikinfrastruktur sperren, soweit dies zur Gefahrenabwehr erforderlich ist und mildere Mittel nicht ausreichen. Sie kann muss diesen Nutzern den weiteren Zugang zur Telematikinfrastruktur unter der Bedingung gestatten, dass die von der Gesellschaft für Telematik angeordneten Maßnahmen zur Gefahrenabwehr umgesetzt werden oder die erhebliche Gefahr nicht mehr besteht. Die Gesellschaft für Telematik kann den nach § 324 zugelassenen Anbietern und Betreibern sowie Anbietern, die eine Zulassung für Komponenten oder Dienste der Telematikinfrastruktur nach § 363a sowie § 325 oder eine Bestätigung nach § 327 besitzen, zur Beseitigung oder Vermeidung von Störungen nach Absatz 2 verbindliche Anordnungen erteilen, insbesondere 1. zur Meldung von Störungen, von festgestellten Schwachstellen eines Dienstes und von Sicherheitsvorfällen an die Gesellschaft für Telematik und zu Fristen, innerhalb derer diese Meldung zu erstatten ist, 2. zur Ergreifung von Maßnahmen zur Beseitigung oder Vermeidung von Störungen, von festgestellten Schwachstellen eines Dienstes und von Sicherheitsvorfällen und zu Fristen, innerhalb derer diese Maßnahmen umzusetzen sind,

GesetzE §329 SGBV	Bitkom-Vorschlag
sowie zu Fristen, innerhalb derer diese Maßnahmen zu ergreifen sind, sowie 4. zur Ergreifung von Maßnahmen zur Gewährleistung der Verfügbarkeit und Stabilität des betriebenen Dienstes innerhalb der Telematikinfrastruktur.“	3. zur Ergreifung von Maßnahmen bei beabsichtigten Änderungen in der Ausführung von Betriebsleistungen und zu Fristen, innerhalb derer diese Maßnahmen zu ergreifen sind, sowie 4. zur Ergreifung von Maßnahmen zur Gewährleistung der Verfügbarkeit und Stabilität des betriebenen Dienstes innerhalb der Telematikinfrastruktur.

GesetzE § 331 SGB V	Bitkom-Vorschlag
(1) Die Gesellschaft für Telematik hat für Komponenten und Dienste der Telematikinfrastruktur sowie für Komponenten und Dienste, die die Telematikinfrastruktur nutzen, aber außerhalb der Telematikinfrastruktur betrieben werden, im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik solche Maßnahmen zur Überwachung des Betriebs zu treffen, die erforderlich sind, um die Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur zu gewährleisten. Die Gesellschaft für Telematik kann zur Erfüllung ihrer Aufgaben nach Satz 1 die entsprechenden Komponenten und Dienste untersuchen. Sie kann sich hierbei der Unterstützung Dritter bedienen, soweit berechnigte Interessen des Herstellers, des Anbieters oder des Betreibers der betroffenen Komponenten oder Dienste dem nicht entgegenstehen.	Die Gesellschaft für Telematik überwacht den Betrieb der Komponenten und Dienste der Telematikinfrastruktur. Komponenten und Dienste, die außerhalb der Telematikinfrastruktur betrieben werden, dürfen nur insoweit überwacht oder untersucht werden, als dies unmittelbar zur Prüfung einer konkret benannten sicherheitsrelevanten Schnittstelle erforderlich ist. Eine weitergehende Untersuchung bedarf der vorherigen Zustimmung des Bundesamtes für Sicherheit in der Informationstechnik und der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Ein Zugriff auf produktive personenbezogene Daten ist ausgeschlossen und durch eine unabhängige Stelle zu auditieren

GesetzE §332a SGBV	Bitkom-Vorschlag
(2) Die Einbindung der Komponenten und Dienste nach Absatz 1 erfolgt ohne zusätzliche Kosten für die Nutzer der informationstechnischen Systeme unabhängig vom Aufwand des Herstellers oder Anbieters. Direkte oder indirekte Kosten im Zusammenhang mit der Wahl eines Herstellers oder Anbieters sind unzulässig.	(2) Die Einbindung der Komponenten und Dienste nach Absatz 1 erfolgt ohne zusätzliche Kosten für die Nutzer der informationstechnischen Systeme unabhängig vom Aufwand des Herstellers oder Anbieters. Direkte oder indirekte Kosten im Zusammenhang mit der Wahl eines Herstellers oder Anbieters sind unzulässig.“

GesetzE § 342 SGBV	Bitkom-Vorschlag
Folgeänderung Forderung § 350	In § 342 Absatz 2a wird die folgende Nummer 3 neu eingefügt:

GesetzE § 342 SGBV	Bitkom-Vorschlag
	3.zusätzlich, sobald die hierfür erforderlichen Voraussetzungen vorliegen, spätestens jedoch zur Bereitstellung der elektronischen Patientenakte nach Patientenakte nach § 341 Absatz 2 Nummer 1 Buchstabe c a) Daten der elektronischen Impfdokumentation nach §342 Nummer 5 als Informationsobjekt gemäß den Festlegungen nach § 355 in semantisch und syntaktisch interoperabler Form zur Verfügung gestellt werden können; die gesetzlichen Krankenkassen stellen sicher, dass Versicherte die Möglichkeit erhalten, sich über die elektronische Patientenakte nach §341 Abs.1 an anstehende Impfungen gemäß STIKO-Empfehlung informieren zu lassen.
8. zusätzlich, spätestens bis zum 1. Januar 2028, die Versicherten über die Benutzeroberfläche eines geeigneten Endgeräts die Berichtigung ihrer personenbezogenen Daten gemäß Artikel 16 der Verordnung (EU) 2016/679 gegenüber den Verantwortlichen nach § 341 Absatz 4 verlangen können; § 308 Absatz 1 und § 344 Absatz 4 bleiben unberührt.“	8. zusätzlich, spätestens bis zum 1. Januar 2028, die Versicherten über die Benutzeroberfläche eines geeigneten Endgeräts die Berichtigung ihrer personenbezogenen Daten gemäß Artikel 16 der Verordnung (EU) 2016/679 gegenüber den jeweils verantwortlichen datenverarbeitenden Stellen Verantwortlichen nach § 341 Absatz 4 verlangen können; die Krankenkassen stellen hierbei sicher, dass entsprechende Berichtigungsersuchen der Versicherten über die elektronische Patientenakte an die jeweils für die Daten verantwortlichen Leistungserbringer oder sonstigen datenverarbeitenden Stellen übermittelt werden; eine inhaltliche Änderung der Daten durch die Krankenkassen erfolgt nicht. § 308 Absatz 1 und § 344 Absatz 4 bleiben unberührt.

GesetzE § 345a SGB V	Bitkom-Vorschlag
(1) Die Krankenkassen bieten spätestens ab dem 1. Februar 2028 ihren Versicherten über die Benutzeroberfläche der elektronischen Patientenakte nach § 342 Absatz 2 Nummer 1 Buchstabe b einen Funktionsbereich für den digitalen Versorgungseinstieg an. Der Funktionsbereich für den digitalen Versorgungseinstieg umfasst insbesondere das Angebot 1. einer Buchung von in § 75 Absatz 1a genannten Behandlungsterminen unter Nutzung des von der Kassenärztlichen Bundesvereinigung nach § 370a Absatz 1 Satz 1 betriebenen elektronischen Systems,	(1) Die Krankenkassen bieten spätestens ab dem 1. Februar 2028 ihren Versicherten über die Benutzeroberfläche der elektronischen Patientenakte nach § 342 Absatz 2 Nummer 1 Buchstabe b einen Funktionsbereich für den digitalen Versorgungseinstieg an. Die Krankenkassen haben den digitalen Versorgungseinstieg so auszugestalten, dass 1. das Recht der Versicherten, eine Terminbuchungslösung nach Satz 2 Nummer 1 für den

GesetzE § 345a SGB V	Bitkom-Vorschlag
2. der Nutzung des in § 75 Absatz 1a Satz 3 Nummer 4 genannten bundesweit einheitlichen, standardisierten Ersteinschätzungsverfahrens und 3. der Nutzung von Komponenten der Telematikinfrastruktur, die den Zugriff der Versicherten auf elektronische Überweisungen nach § 360a ermöglichen, sobald diese zur Verfügung stehen.	digitalen Versorgungseinstieg jederzeit frei zu wählen, gewährleistet ist, und 2. ein bidirektionaler Wechsel zwischen der Benutzeroberfläche nach § 342 und der vom Versicherten gewählten Terminbuchungslösung nach Satz 2 Nummer 1 möglich ist. Die Krankenkassen müssen eine von der Benutzeroberfläche nach § 342 unabhängige Integration der Angebote des Funktionsbereichs nach Satz 1 in Anwendungen von Drittanbietern ermöglichen. Der Funktionsbereich für den digitalen Versorgungseinstieg umfasst insbesondere das Angebot 1.einer Buchung in § 75 Absatz 1a genannten Behandlungsterminen und von Terminen für telemedizinische Leistungen bei einem Leistungserbringer nach § 95 Absatz 1 Satz 1 nach Wahl des Versicherten unter Nutzung des Systems nach § 370a Absatz 1 oder einer anderen funktional und sicherheitstechnisch gleichwertigen Terminbuchungslösung, sofern die Gleichwertigkeit durch vorherige und regelmäßig wiederholte Überprüfung bestätigt ist, unter Nutzung des von der Kassenärztlichen Bundesvereinigung nach § 370a Absatz 1 Satz 1 betriebenen elektronischen Systems 2. der Nutzung des in § 75 Absatz 1a Satz 3 Nummer 4 genannten bundesweit einheitlichen, standardisierten Ersteinschätzungsverfahrens und
(2) Die Krankenkassen bieten den Versicherten in dem Funktionsbereich für den digitalen Versorgungseinstieg durch die Integration der verfügbaren technischen Funktionen einen einfach bedienbaren Weg in eine bedarfsgerechte Versorgung an. Sie stellen dazu insbesondere sicher, dass der Versicherte 1. nach Vereinbarung und erfolgter Bestätigung eines Behandlungstermins mit einem an der vertragsärztlichen Versorgung nach § 95 Absatz 1 Satz 1 teilnehmenden Leistungserbringer diesem Leistungserbringer einen Zugriff auf seine elektronische Patientenakte erteilen kann und dass der Zugriff im Falle einer Stornierung des Termins wieder entzogen wird, 2. einem an der vertragsärztlichen Versorgung nach § 95 Absatz 1 Satz 1 teilnehmenden Leistungserbringer im Fall seiner telemedizinischen Versorgung von seiner	(2) Die Krankenkassen bieten den Versicherten in dem Funktionsbereich für den digitalen Versorgungseinstieg durch die Integration der verfügbaren technischen Funktionen einen einfach bedienbaren Weg in eine bedarfsgerechte Versorgung an. Sie stellen dazu insbesondere sicher, dass der Versicherte 1. nach Vereinbarung und erfolgter Bestätigung eines Behandlungstermins mit einem an der vertragsärztlichen Versorgung nach § 95 Absatz 1 Satz 1 teilnehmenden Leistungserbringer diesem Leistungserbringer einen Zugriff auf seine elektronische Patientenakte erteilen kann und dass der Zugriff im Falle einer Stornierung des Termins wieder entzogen wird, 2. einem an der vertragsärztlichen Versorgung nach § 95 Absatz 1 Satz 1 teilnehmenden Leistungserbringer im Fall seiner telemedizinischen Versorgung von seiner

Gesetz § 345a SGB V	Bitkom-Vorschlag
Krankenkasse einen Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung über sichere Übermittlungsverfahren nach § 363a Absatz 1 oder über Dienste nach § 291b Absatz 1 übermitteln lassen kann, 3. nach Vereinbarung eines Termins mit einem an der vertragsärztlichen Versorgung nach § 95 Absatz 1 Satz 1 teilnehmenden Leistungserbringer diesem die Information übermitteln kann, dass er mit der Kontaktaufnahme über den Sofortnachrichtendienst nach § 363a Absatz 1 Satz 1 Nummer 1 einverstanden ist und er diesen Sofortnachrichtendienst für die weitere Kommunikation nutzen möchte, und 4. nach Nutzung des in § 75 Absatz 1a Satz 3 Nummer 4 genannten bundesweit einheitlichen, standardisierten Ersteinschätzungsverfahrens die Ergebnisse der Ersteinschätzung in seiner elektronischen Patientenakte speichern kann.	Krankenkasse einen Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung über sichere Übermittlungsverfahren nach § 363a Absatz 1 oder über Dienste nach § 291b Absatz 1 übermitteln lassen kann, 3. nach Vereinbarung eines Termins mit einem an der vertragsärztlichen Versorgung nach § 95 Absatz 1 Satz 1 teilnehmenden Leistungserbringer diesem die Information übermitteln kann, dass er mit der Kontaktaufnahme über den Sofortnachrichtendienst nach § 363a Absatz 1 Satz 1 Nummer 1 einverstanden ist und er diesen Sofortnachrichtendienst für die weitere Kommunikation nutzen möchte, und 4. nach Nutzung des in § 75 Absatz 1a Satz 3 Nummer 4 genannten bundesweit einheitlichen, standardisierten Ersteinschätzungsverfahrens die Ergebnisse der Ersteinschätzung in seiner elektronischen Patientenakte speichern kann. Die Krankenkassen stellen sicher, dass die Funktionen des digitalen Versorgungseinstiegs über offene, interoperable und diskriminierungsfreie Schnittstellen aus zugelassenen Anwendungen Dritter genutzt werden können. Die Nutzung darf nicht von der Installation oder Verwendung einer bestimmten Anwendung der Krankenkasse oder einer gesonderten Identitätsanwendung abhängig gemacht werden. Eine erfolgreiche Authentisierung des Versicherten ist für die im Rahmen des digitalen Versorgungseinstiegs verbundenen Anwendungen und Dienste nutzbar. Eine erneute Authentisierung darf nur verlangt werden, soweit dies aufgrund einer besonderen gesetzlichen Sicherheitsanforderung erforderlich ist.

Gesetzestext § 345a SGB V	Bitkom-Vorschlag
(3) Sobald die entsprechenden technischen Möglichkeiten zur Verfügung stehen, bieten die Krankenkassen den Versicherten an, die Funktionen in dem Funktionsbereich für den digitalen Versorgungseinstieg zu personalisieren. Sie ermöglichen dazu insbesondere, dass der Versicherte einrichten kann, dass 1. seine Daten, die in seiner elektronischen Patientenakte oder bei der Krankenkasse gespeichert sind, in dem in § 75 Absatz 1a Satz 3 Nummer 4 genannten bundesweit einheitlichen, standardisierten	(3) Sobald die entsprechenden technischen Möglichkeiten zur Verfügung stehen, bieten die Krankenkassen den Versicherten an, die Funktionen in dem Funktionsbereich für den digitalen Versorgungseinstieg zu personalisieren. Sie ermöglichen dazu insbesondere, dass der Versicherte einrichten kann, dass 1. seine Daten, die in seiner elektronischen Patientenakte oder bei der Krankenkasse gespeichert sind, in dem in § 75 Absatz 1a Satz 3 Nummer 4 genannten bundesweit einheitlichen, standardisierten

Gesetzestext § 345a SGB V	Bitkom-Vorschlag
Ersteinschätzungsverfahren und für ein bedarfsgerechtes Angebot von Behandlungsterminen nach § 75 Absatz 1a genutzt werden und 2. die Daten aus einer elektronischen Überweisung nach § 360a sowie nach Nutzung des in § 75 Absatz 1a Satz 3 Nummer 4 genannten bundesweit einheitlichen, standardisierten Ersteinschätzungsverfahrens die Ergebnisse der Ersteinschätzung für ein bedarfsgerechtes Angebot von Behandlungsterminen nach § 75 Absatz 1a genutzt werden.	Ersteinschätzungsverfahren und für ein bedarfsgerechtes Angebot sowie für die Personalisierung der Terminsuche über eine Terminbuchungslösung nach Satz 2 Nummer 1 genutzt werden, 2. die Daten aus einer elektronischen Überweisung nach § 360a sowie nach Nutzung des in § 75 Absatz 1a Satz 3 Nummer 4 genannten bundesweit einheitlichen, standardisierten Ersteinschätzungsverfahrens die Ergebnisse der Ersteinschätzung für ein bedarfsgerechtes Angebot von Behandlungsterminen nach § 75 Absatz 1a genutzt werden Terminen über eine Terminbuchungslösung nach Satz 2 Nummer 1. Die Funktionen nach Satz 1 Nummer 1 und 2 setzen die informierte Einwilligung des Versicherten voraus.
(5) Nach Vereinbarung und erfolgter Bestätigung eines Behandlungstermins des Versicherten mit einem an der vertragsärztlichen Versorgung nach § 95 Absatz 1 Satz 1 teilnehmenden Leistungserbringer werden die jeweils benötigten Informationen anlassbezogen automatisiert übermittelt, insbesondere 1. von dem Versicherten die Krankenversichertennummer des Versicherten nach § 290 Absatz 1 an die Kassenärztliche Bundesvereinigung und von der Kassenärztlichen Bundesvereinigung an den Leistungserbringer, 2. von dem Leistungserbringer die Betriebsstättennummer und die in § 313 Absatz 1 genannte eindeutige Identifikationsnummer seiner Leistungserbringerorganisation an die Kassenärztliche Bundesvereinigung und von der Kassenärztlichen Bundesvereinigung an den Versicherten, 3. von dem Versicherten die in Absatz 2 Satz 2 Nummer 3 genannte Information an die Kassenärztliche Bundesvereinigung und von der Kassenärztlichen Bundesvereinigung an den Leistungserbringer. Die Kassenärztliche Bundesvereinigung sieht die verpflichtende Übermittlung der Identifikationsnummern nach Satz 1 sowie die verpflichtende Übermittlung der in Absatz 2 Satz 2 Nummer 3 genannten Information in den Festlegungen nach § 370a Absatz 2 und 5 vor. Die Kassenärztliche Bundesvereinigung löscht die Daten nach Satz 1 und 2, nachdem der Termin stattgefunden hat oder storniert wurde.	(5) Nach Vereinbarung und erfolgter Bestätigung eines Behandlungstermins des Versicherten mit einem an der vertragsärztlichen Versorgung nach § 95 Absatz 1 Satz 1 teilnehmenden Leistungserbringer werden die jeweils benötigten Informationen anlassbezogen automatisiert übermittelt, insbesondere 1. von dem Versicherten die Krankenversicherthenummer des Versicherten nach § 290 Absatz 1 an die Kassenärztliche Bundesvereinigung und von der Kassenärztlichen Bundesvereinigung an den Leistungserbringer, 2. von dem Leistungserbringer die Betriebsstättennummer und die in § 313 Absatz 1 genannte eindeutige Identifikationsnummer seiner Leistungserbringerorganisation an die Kassenärztliche Bundesvereinigung und von der Kassenärztlichen Bundesvereinigung an den Versicherten, 3. von dem Versicherten die in Absatz 2 Satz 2 Nummer 3 genannte Information an die Kassenärztliche Bundesvereinigung und von der Kassenärztlichen Bundesvereinigung an den Leistungserbringer. Die Kassenärztliche Bundesvereinigung sieht die verpflichtende Übermittlung der Identifikationsnummern nach Satz 1 sowie die verpflichtende Übermittlung der in Absatz 2 Satz 2 Nummer 3 genannten Information in den Festlegungen nach § 370a Absatz 2 und 5 vor. Die Kassenärztliche Bundesvereinigung löscht die Daten nach Satz 1 und 2, nachdem der Termin stattgefunden hat oder storniert wurde. Die übermittelten Daten dürfen von den Krankenkassen nur zum Zweck der Terminbuchung und -verwaltung

Gesetzestext § 345a SGB V	Bitkom-Vorschlag
	verarbeitet werden und sind unverzüglich zu löschen, sobald sie für diesen Zweck nicht mehr erforderlich sind.

GesetzE § 361b SGBV	Bitkom Vorschlag
Krankenkassen und die weiteren Kostenträger nach § 362 Absatz 1 dürfen zum Zwecke der Einlösung elektronischer Verordnungen von digitalen Gesundheitsanwendungen nach § 360 Absatz 4 auf Daten der Versicherten in vertragsärztlichen elektronischen Verordnungen zugreifen und diese verarbeiten.	Krankenkassen und die weiteren Kostenträger nach § 362 Absatz 1 dürfen zum Zwecke der Einlösung elektronischer Verordnungen von digitalen Gesundheitsanwendungen nach § 360 Absatz 4 auf Daten der Versicherten in vertragsärztlichen elektronischen Verordnungen zugreifen und diese automatisiert verarbeiten. Die Verarbeitung nach Satz 1 erfolgt, ohne dass es einer gesonderten Aktion oder Mitwirkung der Versicherten bedarf.
(bisher nicht enthalten)	Zum Zugriff nach Absatz 1 können die Krankenkassen und die weiteren Kostenträger nach § 362 Absatz 1 durch den Versicherten auch ohne die in § 360 Absatz 9 genannten Zugangsdaten oder eine digitale Identität nach § 291 Absatz 8 autorisiert werden.
(bisher nicht enthalten)	In § 360 Abs. 4 werden nach Satz 1 folgende Sätze eingefügt: Ergänzend zur elektronischen Übermittlung nach Satz 1 haben Leistungserbringer den Versicherten bis zum 31. Dezember 2028 einen papiergebundenen Ausdruck der Verordnung auszuhändigen. Die Dienste und Komponenten zur Einlösung elektronischer Verordnungen für digitale Gesundheitsanwendungen sind plattformneutral auszugestalten. Es ist sicherzustellen, dass die Funktionalität und Erreichbarkeit der Einlösewege für Webanwendungen und native Applikationen identisch sind. Verfahren, die eine bestimmte Technologieform bevorzugen oder benachteiligen, sind unzulässig.“
(7) Ab dem 1. Juni 2029 sind die in Absatz 2 Satz 1 genannten Leistungserbringer sowie die in Absatz 4 Satz 1 genannten Psychotherapeuten verpflichtet, Verordnungen von Heilmitteln elektronisch auszustellen und für deren Übermittlung Dienste und Komponenten nach Absatz 1 zu nutzen. Ab dem 1. Juli 2030 sind die in Absatz 2 Satz 1 genannten Leistungserbringer sowie die in Absatz 4 Satz 1 genannten Psychotherapeuten verpflichtet, Verordnungen von Hilfsmitteln, Verordnungen von Verbandmitteln nach § 31 Absatz 1 Satz 1, Verordnungen von Harn- und Blutteststreifen nach § 31 Absatz 1 Satz 1, Verordnungen von Medizinprodukten nach § 31 Absatz 1, sowie Verordnungen von bilanzierten Diäten zur enteralen	(7) Ab dem 1. Juni 2029 sind die in Absatz 2 Satz 1 genannten Leistungserbringer sowie die in Absatz 4 Satz 1 genannten Psychotherapeuten verpflichtet, Verordnungen von Heilmitteln elektronisch auszustellen und für deren Übermittlung Dienste und Komponenten nach Absatz 1 zu nutzen. Ab dem 1. Juli 2030 sind die in Absatz 2 Satz 1 genannten Leistungserbringer sowie die in Absatz 4 Satz 1 genannten Psychotherapeuten verpflichtet, Verordnungen von Hilfsmitteln, Verordnungen von Verbandmitteln nach § 31 Absatz 1 Satz 1, Verordnungen von Harn- und Blutteststreifen nach § 31 Absatz 1 Satz 1, Verordnungen von Medizinprodukten nach § 31 Absatz 1, sowie Verordnungen von bilanzierten Diäten zur enteralen

GesetzE § 361b SGBV	Bitkom Vorschlag
Ernährung nach § 31 Absatz 5 elektronisch auszustellen und für deren Übermittlung Dienste und Komponenten nach Absatz 1 zu nutzen. [....]“	Ernährung nach § 31 Absatz 5 elektronisch auszustellen und für deren Übermittlung Dienste und Komponenten nach Absatz 1 zu nutzen. Ab dem 1. Januar 2027 sind die in Absatz 2 Satz 1 genannten Leistungserbringer sowie die in Absatz 4 Satz 1 genannten Psychotherapeuten verpflichtet, Verordnungen von Sprechstundenbedarf elektronisch auszustellen und für deren Übermittlung Dienste und Komponenten nach Absatz 1 zu nutzen. [....]“

GesetzE § 360a SGBV	Bitkom-Vorschlag
(5) Überweisungsdaten und Informationen zur Einlösung der elektronischen Überweisung sind mit Ablauf von 100 Tagen nach Einlösung der elektronischen Überweisung zu löschen.	(5) Überweisungsdaten und Informationen zur Einlösung der elektronischen Überweisung sind mit Ablauf von 100 Tagen nach Einlösung der elektronischen Überweisung zu löschen.

GesetzE § 360b SGBV	Bitkom-Vorschlag
(1) Die Kassenärztliche Bundesvereinigung vereinbart mit dem Spitzenverband Bund der Krankenkassen bis zum [zwölf Monate nach Inkrafttreten] die Anforderungen an ein elektronisches System zur standardisierten und strukturierten Erhebung gesundheitlicher Beschwerden, zur Einschätzung der Notwendigkeit und Dringlichkeit der Behandlung sowie zur Zuordnung der Behandlungsbedarfe in die geeignete Versorgungsebene (digitale Bedarfseinschätzung). Die digitale Bedarfseinschätzung unterstützt die Versicherten zielgerichtet bei deren Zugang in die Notfall-, Akut- oder ambulante Regelversorgung. Bei der Vereinbarung nach Satz 1 sind die Regelungen und Vorgaben nach § 75 Absatz 1a Satz 3 Nummer 4 in Verbindung mit Absatz 7 Satz 1 Nummer 6 sowie die Vorgaben der Vereinbarung nach § 87 Absatz 2o Nummer 4 zu beachten. Das Bundesministerium für Gesundheit ist auf Verlangen über den Vereinbarungsstand zu unterrichten. Die Vereinbarung nach Satz 1 ist im Benehmen zu treffen mit 1. den maßgeblichen medizinischen Fachgesellschaften, 2. der Bundesärztekammer, 3. der Bundespsychotherapeutenkammer, 4. der Deutschen Krankenhausgesellschaft, 5. der Gesellschaft für Telematik, 6. dem Gemeinsamen Bundesausschuss und	(1) Die Kassenärztliche Bundesvereinigung vereinbart mit dem Spitzenverband Bund der Krankenkassen bis zum [zwölf Monate nach Inkrafttreten] die Anforderungen an ein elektronisches System zur standardisierten und strukturierten Erhebung gesundheitlicher Beschwerden, zur Einschätzung der Notwendigkeit und Dringlichkeit der Behandlung sowie zur Zuordnung der Behandlungsbedarfe in die geeignete Versorgungsebene (digitale Bedarfseinschätzung). Die digitale Bedarfseinschätzung unterstützt die Versicherten zielgerichtet bei deren Zugang in die Notfall-, Akut- oder ambulante Regelversorgung. Bei der Vereinbarung nach Satz 1 sind die Regelungen und Vorgaben nach § 75 Absatz 1a Satz 3 Nummer 4 in Verbindung mit Absatz 7 Satz 1 Nummer 6 sowie die Vorgaben der Vereinbarung nach § 87 Absatz 2o Nummer 4 zu beachten. Das Bundesministerium für Gesundheit ist auf Verlangen über den Vereinbarungsstand zu unterrichten. Die Vereinbarung nach Satz 1 ist im Benehmen zu treffen mit 1. den maßgeblichen medizinischen Fachgesellschaften, 2. der Bundesärztekammer, 3. der Bundespsychotherapeutenkammer, 4. der Deutschen Krankenhausgesellschaft, 5. der Gesellschaft für Telematik,

GesetzE § 360b SGBV	Bitkom-Vorschlag
7. den auf Bundesebene für die Wahrnehmung der Interessen der Patienten und der Selbsthilfe chronisch kranker und behinderter Menschen maßgeblichen Organisationen. 8. den für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen sowie der Medizintechnologie.	6. dem Gemeinsamen Bundesausschuss und 7. den auf Bundesebene für die Wahrnehmung der Interessen der Patienten und der Selbsthilfe chronisch kranker und behinderter Menschen maßgeblichen Organisationen. 8. den für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen sowie der Medizintechnologie und Anbietern informationstechnischer Systeme.
Abs. 3 Nr. 1 h) technischen Hochverfügbarkeit, Redundanz, technischen Resilienz und Praktikabilität, und	h) technischen Hochverfügbarkeit, Redundanz, Strukturiertheit der Daten, technischen Resilienz und Praktikabilität, und

GesetzE § 361b SGBV	Bitkom-Vorschlag
(1) Krankenkassen und die weiteren Kostenträger nach § 362 Absatz 1 Satz 1 dürfen zum Zwecke der Einlösung elektronischer Verordnungen von digitalen Gesundheitsanwendungen nach § 360 Absatz 4 auf Daten der Versicherten in vertragsärztlichen elektronischen Verordnungen zugreifen und diese verarbeiten.“	(1) Krankenkassen und die weiteren Kostenträger nach § 362 Absatz 1 Satz 1 sowie Apotheken dürfen zum Zwecke der Einlösung elektronischer Verordnungen von digitalen Gesundheitsanwendungen nach § 360 Absatz 4 auf Daten der Versicherten in vertragsärztlichen elektronischen Verordnungen zugreifen und diese verarbeiten.“

GesetzE § 363b SGBV	Bitkom-Vorschlag
(1) Die für die sicheren Übermittlungsverfahren nach § 363a Absatz 1 erforderlichen Komponenten und Dienste der Telematikinfrastruktur bedürfen der Zulassung gemäß § 325. Im Fall einer Auftragsvergabe für die Entwicklung, Zurverfügungstellung, den Betrieb und die Zulassung der Komponenten und Dienste durch die Gesellschaft für Telematik nach § 311 Absatz 1 Satz 1 Nummer 4 und 5 ist die Sicherheit der Komponenten und Dienste durch ein externes Sicherheitsgutachten nachzuweisen. Dabei ist nachzuweisen, dass die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Komponenten und Dienste sichergestellt werden.	(1) Die für die sicheren Übermittlungsverfahren nach § 363a Absatz 1 erforderlichen Komponenten und Dienste der Telematikinfrastruktur bedürfen der Zulassung gemäß § 325. Im Fall einer Auftragsvergabe für die Entwicklung, Zurverfügungstellung, den Betrieb und die Zulassung der Komponenten und Dienste durch die Gesellschaft für Telematik nach § 311 Absatz 1 Satz 1 Nummer 4 und 5 ist die Sicherheit der Komponenten und Dienste durch ein externes Sicherheitsgutachten nachzuweisen. Dabei ist nachzuweisen, dass die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Komponenten und Dienste sichergestellt werden.
(2) Der Anbieter eines sicheren Übermittlungsverfahrens nach § 363a Absatz 1 muss über die nach § 324 erforderliche Zulassung verfügen. Die Kassenärztlichen	(2) Der Anbieter eines sicheren Übermittlungsverfahrens nach § 363a Absatz 1 muss über die nach § 324 erforderliche Zulassung verfügen. Die Kassenärztlichen

GesetzE § 363b SGBV	Bitkom-Vorschlag
Bundesvereinigungen können Anbieter eines sicheren Übermittlungsverfahrens sein, sofern das sichere Übermittlungsverfahren nur Kassenärztlichen Vereinigungen und deren Mitgliedern zur Verfügung gestellt wird.	Bundesvereinigungen können Anbieter eines sicheren Übermittlungsverfahrens sein, sofern das sichere Übermittlungsverfahren nur Kassenärztlichen Vereinigungen und deren Mitgliedern zur Verfügung gestellt wird.

GesetzE § 363c SGBV	Bitkom-Vorschlag
(3) Leistungserbringer, die an die Telematikinfrastruktur angeschlossen sind, sind verpflichtet den sicheren E-Mail-Dienst nach § 363a Absatz 1 Nummer 2 für die elektronische Kommunikation mit denjenigen zu nutzen, die an die Telematikinfrastruktur angeschlossen sind.	Leistungserbringer, die an die Telematikinfrastruktur angeschlossen sind, sind verpflichtet sichere Übermittlungsverfahren nach § 363a zu nutzen.

GesetzE § 363e	Bitkom-Vorschlag
(1) Eine Organisation kann zur Unterstützung der Gesundheitsversorgung oder zur Unterstützung, Verarbeitung oder Dokumentation ihrer medizinischen oder administrativen Prozesse ein bestimmtes Fachverfahren, im Einvernehmen mit der Gesellschaft für Telematik, nutzen. Ein Fachverfahren ist ein standardisiertes Verfahren, das das sichere Übermittlungsverfahren nach § 363a Absatz 1 Satz 1 Nummer 2 nutzt. Das Einvernehmen nach Satz 1 soll spätestens drei Monate bevor das Fachverfahren für die Nutzung im Rahmen des sicheren Übermittlungsverfahrens nach § 363a Absatz 1 Satz 1 Nummer 2 veröffentlicht oder einzelnen Nutzergruppen zur Verfügung hergestellt werden. Dies gilt insbesondere für solche Fachverfahren,	(1) Eine Organisation kann zur Unterstützung der Gesundheitsversorgung oder zur Unterstützung, Verarbeitung oder Dokumentation ihrer medizinischen oder administrativen Prozesse ein bestimmtes Fachverfahren, im Einvernehmen mit der Gesellschaft für Telematik, nutzen. Ein Fachverfahren ist ein standardisiertes Verfahren, das das sichere Übermittlungsverfahren nach § 363a Absatz 1 Satz 1 Nummer 2 nutzt. Das Einvernehmen nach Satz 1 soll spätestens drei Monate bevor das Fachverfahren für die Nutzung im Rahmen des sicheren Übermittlungsverfahrens nach § 363a Absatz 1 Satz 1 Nummer 2 veröffentlicht oder einzelnen Nutzergruppen zur Verfügung hergestellt werden. Dies gilt insbesondere für solche Fachverfahren,

GesetzE § 370c	Bitkom-Vorschlag
	§ 370c in der derzeitigen Fassung komplett zu streichen.

GesetzE § 383a SGB V	Bitkom-Vorschlag
(1) Stellen für digitale Gesundheit gemäß Artikel 19 der Verordnung (EU) 2025/327 sind	(1) Stellen für digitale Gesundheit gemäß Artikel 19 der Verordnung (EU) 2025/327 sind

GesetzE § 383a SGB V	Bitkom-Vorschlag
1. das Bundesministerium für Gesundheit im Hinblick auf die Aufgaben gemäß Artikel 19 Absatz 2 Buchstabe a, c und f der Verordnung (EU) 2025/327 und 2. die Gesellschaft für Telematik im Hinblick auf die Aufgaben gemäß Artikel 19 Absatz 2 Buchstabe b, d, e, g, h und j bis m der Verordnung (EU) 2025/327.	1. das Bundesministerium für Gesundheit im Hinblick auf die Aufgaben gemäß Artikel 19 Absatz 2 Buchstabe a, c und f der Verordnung (EU) 2025/327 und 2. die Gesellschaft für Telematik im Hinblick auf die Aufgaben gemäß Artikel 19 Absatz 2 Buchstabe b, d, e, g, h und j bis m der Verordnung (EU) 2025/327. 2.eine vom Bundesministerium für Gesundheit organisatorisch unabhängige Stelle für digitale Gesundheit im Hinblick auf die Aufgaben nach Artikel 19 Absatz 2 Buchstaben b, d, e, g, h und j bis m der Verordnung (EU) 2025/327.' § 383a Absatz 2 wird wie folgt gefasst: 'Die Koordinierung und die Erstellung des Tätigkeitsberichts obliegen dem Bundesministerium für Gesundheit oder einer von ihm bestimmten unabhängigen Stelle.' In § 383a Absatz 3 werden die Wörter 'bei der Gesellschaft für Telematik eingerichteten koordinierenden Stelle' durch 'bei einer organisatorisch unabhängigen zentralen Beschwerdestelle' ersetzt. Die gematik kann dieser Stelle technische Auskünfte erteilen, darf aber nicht alleinige Entscheidungs- oder Filterinstanz sein.

GesetzE § 386a SGBV	Bitkom-Vorschlag
(1) Hersteller nach § 384 Satz 2 Nummer 3 haben den Leistungserbringern, die informationstechnisches System dieses Herstellers nutzen, auf deren Verlangen die personenbezogenen Gesundheitsdaten ihrer Patienten unverzüglich und kostenfrei im interoperablen Format bereitzustellen und den Leistungserbringern den Zugriff auf Patientendaten nach diesem Buch im interoperablen Format zu ermöglichen. § 630f Absatz 3 und § 630g des Bürgerlichen Gesetzbuches bleiben hiervon unberührt.	(1) Hersteller nach § 384 Satz 2 Nummer 3 haben den Leistungserbringern, die informationstechnisches System dieses Herstellers nutzen, auf deren Verlangen die personenbezogenen Gesundheitsdaten ihrer Patienten unverzüglich und kostenfrei im interoperablen Format bereitzustellen sofern die Datenbereitstellung nach §371, Abs. 1 Nr. 4 automatisiert generiert werden kann und den Leistungserbringern den Zugriff den Austausch von Patientendaten nach diesem Buch im interoperablen Format zu ermöglichen. § 630f Absatz 3 und § 630g des Bürgerlichen Gesetzbuches bleiben hiervon unberührt.
(4) Stellt der Hersteller die begehrten Informationen entgegen Absatz 1 nicht, nicht rechtzeitig oder nicht im interoperablen Format bereit, so ist er dem Leistungserbringer zum Ersatz des daraus entstehenden Schadens verpflichtet.	"Stellt der Hersteller die begehrten Informationen entgegen Absatz 1 nicht, nicht rechtzeitig oder nicht im interoperablen Format bereit, so ist er dem Leistungserbringer zum Ersatz des daraus entstehenden Schadens verpflichtet." Eine nicht rechtzeitige Bereitstellung ist gemäß dem Kommentar zu Abs. 1 näher zu definieren.

GesetzE § 386b SGBV	Bitkom-Vorschlag
Die Kassenärztlichen Vereinigungen sollen vertragsärztlichen Leistungserbringern Beratungs- und Unterstützungsangebote in Fragen der Digitalisierung der Versorgungsprozesse und Praxisorganisation sowie der Verbesserung der Cybersicherheit machen.“	Die Kassenärztlichen Vereinigungen sollen vertragsärztlichen Leistungserbringenden Beratungs- und Unterstützungsangebote in Fragen der Digitalisierung der Versorgungsprozesse und Praxisorganisation, sowie der Verbesserung der Cybersicherheit machen. Nicht gestattet sind dabei die Bewerbung einzelner Hersteller oder Anbieter informationstechnischer Systeme oder digitaler Anwendungen.

GesetzE § 386c SGBV	Bitkom-Vorschlag
(5) die Vorenthaltung von Datenelementen, die nicht nach § 385 Absatz 2 Satz 1 Nummer 1 verbindlich festgelegt sind, die jedoch notwendig sind, um die den Leistungserbringern obliegenden Pflichten zur Dokumentation und Archivierung von Patientendaten sicherstellen zu können.	(5) die Vorenthaltung von Datenelementen, die nicht nach § 385 Absatz 2 Satz 1 Nummer 1 verbindlich festgelegt sind, die jedoch notwendig sind, um die den Leistungserbringern obliegenden Pflichten zur Dokumentation und Archivierung von Patientendaten sicherstellen zu können. Für diese Datenelemente genügt die Bereitstellung in einem gängigen, strukturierten und maschinenlesbaren Format; eine Bereitstellung im interoperablen Format nach § 386a Absatz 2 ist insoweit nicht notwendig.

GesetzE §393 SGBV	Bitkom-Vorschlag
(1) Leistungserbringer im Sinne des Vierten Kapitels und Kranken- und Pflegekassen sowie ihre jeweiligen Auftragsverarbeiter dürfen Sozialdaten und Gesundheitsdaten auch im Wege des Cloud-Computing-Dienstes verarbeiten, sofern die Voraussetzungen der Absätze 2 bis 4 erfüllt sind. Ein Zugriff zu Wartungs- und Supportzwecken gilt nicht als Verarbeitung nach Satz 1, wenn durch technische Vorkehrungen nach dem Stand der Technik, insbesondere durch Verschlüsselung, sichergestellt ist, dass die Daten dabei nicht zur Kenntnis genommen oder auf sonstige Weise verarbeitet werden können.	(1) Leistungserbringer im Sinne des Vierten Kapitels und Kranken- und Pflegekassen sowie ihre jeweiligen Auftragsverarbeiter dürfen Sozialdaten und Gesundheitsdaten auch im Wege des Cloud-Computing-Dienstes verarbeiten, sofern die Voraussetzungen der Absätze 2 bis 4 erfüllt sind. Ein Zugriff zu Wartungs- und Supportzwecken gilt nicht als Verarbeitung nach Satz 1, wenn durch technische Vorkehrungen nach dem Stand der Technik, insbesondere durch Verschlüsselung, sichergestellt ist, dass die Daten dabei nicht zur Kenntnis genommen oder auf sonstige Weise verarbeitet werden können. Satz zwei gilt ab dem ... [einsetzen: Datum des letzten Tages des sechsten auf die Verkündung folgenden Kalendermonats].

Änderungen SGB XI

GesetzE § 106d SGBXI	Bitkom-Vorschlag
§ 106d Verpflichtende Nutzung von sicheren Übermittlungsverfahren (1) Pflegekassen sind verpflichtet, zur Kommunikation mit den Versicherten auch den Sofortnachrichtendienst nach § 363a Absatz 1 Satz 1 Nummer 1 des Fünften Buches zu nutzen. Leistungserbringer können zur Kommunikation mit den Versicherten den Sofortnachrichtendienst nach § 363a Absatz 1 Satz 1 Nummer 1 des Fünften Buches nutzen.	§ 106d Verpflichtende Nutzung von sicheren Übermittlungsverfahren (1) Pflegekassen sind verpflichtet, zur Kommunikation mit den Versicherten auch den Sofortnachrichtendienst nach § 363a Absatz 1 Satz 1 Nummer 1 des Fünften Buches zu nutzen. Leistungserbringer können zur Kommunikation mit den Versicherten den Sofortnachrichtendienst nach § 363a Absatz 1 Satz 1 Nummer 1 des Fünften Buches nutzen. Leistungserbringer können zur Kommunikation mit den Versicherten den Sofortnachrichtendienst nach § 363a Absatz 1 Satz 1 Nummer 1 des Fünften Buches nutzen und müssen diesen nutzen, sofern der Versicherte diesen Kommunikationskanal, z.B. nach § 345a SGB V (2) 3., gewählt hat. [...]

Änderungen GDNG

GesetzE § 3 GDNG	Bitkom-Vorschlag
(3) Gesundheitsdateninhaber sollen für die von ihnen gehaltenen Datensätze mit personenbezogenen elektronischen Gesundheitsdaten Forschungskennziffern erzeugen und speichern. Gesundheitsdateninhaber dürfen hierzu den unveränderbaren Teil der Krankenversichertennummer nach § 290 Absatz 1 Satz 2 des Fünften Buches Sozialgesetzbuch zur Erzeugung der Forschungskennziffer verarbeiten.	(3) Gesundheitsdateninhaber sollen für die von ihnen gehaltenen Datensätze mit personenbezogenen elektronischen Gesundheitsdaten Forschungskennziffern erzeugen oder von einem zentralen, hierfür zertifizierten Dienst erzeugen lassen und speichern. Gesundheitsdateninhaber oder der zentrale Dienst als Auftragsdatenverarbeiter gem. Satz 1 dürfen hierzu den unveränderbaren Teil der Krankenversichertennummer nach § 290 Absatz 1 Satz 2 des Fünften Buches Sozialgesetzbuch zur Erzeugung der Forschungskennziffer verarbeiten.

GesetzE § 21 GDNG	Bitkom-Vorschlag
Besondere Vorschriften für elektronische Gesundheitsdaten nach Artikel 51 Absatz 1 Buchstabe f und g der Verordnung (EU) 2025/327 (1) Die Verarbeitung folgender elektronischer Gesundheitsdaten für die Sekundärnutzung	Besondere Vorschriften für elektronische Gesundheitsdaten nach Artikel 51 Absatz 1 Buchstabe f und g der Verordnung (EU) 2025/327 (1) Die Verarbeitung folgender elektronischer Gesundheitsdaten für die Sekundärnutzung

ist nur zulässig, wenn die betroffene Person nach Artikel 9 Absatz 2 Buchstabe a der Datenschutz-Grundverordnung in die Verarbeitung dieser Daten für die Sekundärnutzung eingewilligt hat: 1. elektronische Gesundheitsdaten nach Artikel 51 Absatz 1 Buchstabe f der Verordnung (EU) 2025/327, 2. proteomische und transkriptomische Daten nach Artikel 51 Absatz 1 Buchstabe g der Verordnung (EU) 2025/327, 3. andere Daten nach Artikel 51 Absatz 1 Buchstabe g der Verordnung (EU) 2025/327, soweit das bei der Verarbeitung dieser Daten bestehende Re-Identifikationsrisiko für die betroffenen Personen dem der Daten in den Fällen der Nummern 1 oder 2 entspricht. (2) Die koordinierende Zugangsstelle für Gesundheitsdaten hat für die erforderliche Einwilligung betroffener Personen Musterinformationen und -erklärungen für die Gesundheitsdateninhaber zur Verfügung zu stellen.	ist nur zulässig, wenn die betroffene Person nach Artikel 9 Absatz 2 Buchstabe a der Datenschutz-Grundverordnung in die Verarbeitung dieser Daten für die Sekundärnutzung eingewilligt hat: 1. elektronische Gesundheitsdaten nach Artikel 51 Absatz 1 Buchstabe f der Verordnung (EU) 2025/327, 2. proteomische und transkriptomische Daten nach Artikel 51 Absatz 1 Buchstabe g der Verordnung (EU) 2025/327, 3. andere Daten nach Artikel 51 Absatz 1 Buchstabe g der Verordnung (EU) 2025/327, soweit das bei der Verarbeitung dieser Daten bestehende Re-Identifikationsrisiko für die betroffenen Personen dem der Daten in den Fällen der Nummern 1 oder 2 entspricht. (2) Die koordinierende Zugangsstelle für Gesundheitsdaten hat für die erforderliche Einwilligung betroffener Personen Musterinformationen und -erklärungen für die Gesundheitsdateninhaber zur Verfügung zu stellen.
--	--

GesetzE § 25 GDNG	Bitkom-Vorschlag
(1) Für ein Vorhaben der Gesundheits- und Versorgungsforschung dürfen die Verantwortlichen mit Genehmigung der zuständigen Datenschutzaufsichtsbehörde die erforderlichen Gesundheitsdaten nach Maßgabe dieser Vorschrift ohne Einwilligung der betroffenen Personen verarbeiten. 2. [...] Eine Genehmigung nach Satz 1 darf nur für inhaltlich und zeitlich begrenzte Vorhaben erteilt werden. Die Genehmigung kann jederzeit ganz oder teilweise zurückgenommen, widerrufen oder mit Nebenbestimmungen versehen werden.	(1) Für ein Vorhaben der Gesundheits- und Versorgungsforschung dürfen die Verantwortlichen mit Genehmigung der zuständigen Datenschutzaufsichtsbehörde die erforderlichen Gesundheitsdaten nach Maßgabe dieser Vorschrift ohne Einwilligung der betroffenen Personen verarbeiten. 2. [...] Eine Genehmigung nach Satz 1 darf nur für inhaltlich und zeitlich begrenzte Vorhaben erteilt werden oder erforderlichenfalls auch inhaltlich und zeitlich unbegrenzt. Die Genehmigung kann jederzeit ganz oder teilweise zurückgenommen, widerrufen oder mit Nebenbestimmungen versehen werden.

Bitkom vertritt mehr als 2.300 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.

Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Dr. Verena Benz | Bereichsleiterin Pharma & Medtech

T +49 30 27576-270 | v.benz@bitkom.org

Dr. Ariane Schenk | Bereichsleiterin E-Health

T +49 30 27576-231 | a.schenk@bitkom.org

Verantwortliches Bitkom-Gremium

AK E-Health & AK Pharma & Medtech

Copyright

Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.