Stellungnahme der unabhängigen Datenschutzbehörden der Länder

vom 18. Mai 2026

---

zum Referentenentwurf des

Bundesministeriums für Gesundheit:

Entwurf eines Gesetzes für Daten und digitale Innovation

im Gesundheitswesen

(Gesundheitsdaten-und-Innovations-Gesetz – GeDIG, Stand: 07.05.2026)

I. Vorbemerkung

Vorliegend nehmen die unabhängigen Datenschutzbehörden der Länder ohne Beteiligung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), welche bereits im Rahmen der Ressortabstimmung ihre Stellungnahme (Datum: 29.04.2026) abgegeben hat, zum Entwurf eines Gesetzes für Daten und digitale Innovation im Gesundheitswesen (GeDIG, Stand: 22.12.2025) Stellung. Auf die Stellungnahme der BfDI wird gleichwohl im Nachfolgenden an einzelnen Stellen Bezug genommen und ergänzend ausgeführt.

II. Im Einzelnen

1. Zu Artikel 1: Änderung des Fünften Buches Sozialgesetzbuch (SGB V)

§ 25b SGB V-E:

Ergänzend zu den Ausführungen der BfDI in ihrer Stellungnahme vom 29.04.2026 wird hierzu ausgeführt:

An den Bedenken der Datenschutzkonferenz gegen die einwilligungsunabhängige Verarbeitungsbefugnis der Krankenkassen aus der Stellungnahme vom 14. August 2023 (zum Referentenentwurf des Bundesministeriums für Gesundheit: Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten -Gesundheitsdatennutzungsgesetz – GDNG – Stand 03.07.2023, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf, S. 8.) wird festgehalten:

Die Regelung des § 25b SGB V verstößt gegen das Recht auf Nichtwissen und birgt das Risiko eines „gläsernen Versicherten“ mit umfassenden Beeinflussungs- und Diskriminierungsrisiken. Sowohl die Qualität der Abrechnungsdaten als auch die Expertise der Krankenkassenmitarbeitenden dürften nicht dazu geeignet sein, dass Krankenkassen Aufgaben aus dem Behandlungskontext übernehmen. Diese sind vielmehr den behandelnden Ärztinnen und Ärzten vorzubehalten. Insoweit ist es verfehlt, die Reichweite der Regelung noch zu erweitern.
Die Bezugnahme auf § 345 SGB V wirkt außerdem verunklarend; nach § 345 SGB V können Daten aus der elektronischen Patientenakte (ePA) den Krankenkassen nur „zum Zweck der Nutzung zusätzlicher von den Krankenkassen angebotener Anwendungen“ zur Verfügung gestellt werden, nicht zu einer Verarbeitung in sonstiger Weise zu den Zwecken des § 25b Absatz 1 SGB V.

Auch erscheint fraglich, wie die Freiwilligkeit der Einwilligung der Versicherten im Verhältnis zur gesetzlichen Krankenversicherung hinreichend sichergestellt werden kann, wenn hier beispielsweise finanzielle Anreize der Versicherung zur Einwilligungserteilung gewährt werden oder sonstige Nachteile bei der Verweigerung der Einwilligung drohen. Eine Notwendigkeit, den Krankenkassen nicht nur eine Befugnis zur Direkterhebung, sondern auch noch zur Erhebung bei nicht näher bezeichneten Dritten zu ermöglichen, können wir erst recht nicht erkennen. Allein die – zudem ohne konkrete Frist versehene – Verpflichtung, erhobene Daten erst nachträglich in der ePA zu speichern, stellt die gebotene Transparenz nicht hinreichend sicher. Auch sind bislang keine hinreichenden Garantien vorgesehen. Insbesondere fehlt die Normierung einer engen Zweckbestimmung und von Löschpflichten (z. B. auch im Falle des Widerrufs). Denn keinesfalls darf die Regelung dazu führen, dass mit Einwilligung zu einem bestimmten Zweck erhobene Daten sodann als bei der Kranken- oder Pflegekasse „vorliegend" im Sinne von Satz 1 angesehen werden mit der Folge, dass sie nunmehr auch zu anderen Zwecken im Sinne von Absatz 1 weiterverarbeitet werden dürften. In jedem Fall müsste eine Einwilligung außerdem nach Artikel 9 Absatz 2 Buchstabe a DS-GVO ausdrücklich erteilt werden, was der Gesetzentwurf bislang nicht normiert. Auch ist eine hinreichende Informiertheit der Einwilligenden sicherzustellen, was infolge der für § 25b Absatz 3 Satz 2 SGB V vorgesehenen Änderung, wonach nur noch eine öffentliche und keine individuelle Information vorgesehen wird, infrage steht.

§ 129 Absatz 5h SGB V-E in Verbindung mit § 352 Absatz 1 Nummer 5 SGB V-E:

Soweit Apothekerinnen und Apotheker Maßnahmen der assistierten Telemedizin anbieten, ist zunächst zu begrüßen, dass eine enge Zweckbindung der hierzu gewährten Zugriffsmöglichkeit der Apotheken auf die ePA normiert wird. Die enge Zweckbindung ist aber auch durch hinreichende technische und organisatorische Maßnahmen abzusichern.

§ 312 Nr. 20 SGB V-E:

Danach soll die Gesellschaft für Telematik verpflichtet werden, bis zum 1. Januar 2030 die notwendigen Maßnahmen zu treffen, damit in die Notfallversorgung eingebundene Leistungserbringer, d.h. also auch Krankenhäuser mit Notaufnahme, unabhängig von der Eröffnung eines Behandlungskontexts nach § 339 SGB V Zugriff auf die Daten der elektronischen Patientenkurzakte (§ 341 Absatz 2 Nummer 1 Buchstabe c SGB V) erhalten.

Der Begriff der „in die Notfallversorgung eingebundenen Leistungserbringer" ist sehr weit und wird nicht abschließend definiert. Notaufnahmen regulärer Krankenhäuser, Bereitschaftsarztpraxen, Notarztdienste könnten potenziell umfasst sein, ohne dass eine klare Abgrenzung besteht. Der Entwurf enthält außerdem keine explizite gesetzliche Pflicht zur Protokollierung von Notfallzugriffen auf die ePA-Kurzakte, die für Patienten einsehbar wäre. Dies ist im Hinblick auf Artikel 5 Absatz 2 DS-GVO (Rechenschaftspflicht) sowie Artikel 25 DS-GVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) und 32 DS-GVO (technische und organisatorische Maßnahmen) nicht ausreichend.

§ 338 SGB V-E:

Durch die Streichung des Absatz 1, nach dem den Versicherten bisher Komponenten zum Auslesen von Daten und Protokolldaten von elektronischen Verordnungen zustanden, werden die Versicherten auf ihr Auskunftsrecht gegenüber der koordinierenden Stelle gem. § 307 Absatz 5 SGB V verwiesen. Es ist zweifelhaft, ob den Versicherten damit die Wahrnehmung ihrer Rechte erleichtert wird, ohne dass dies

zum höheren Aufwand bei der koordinierenden Stelle führt. Es spricht einiges dafür, dass eine eigene Einsichtnahme in die Daten durch die Versicherten ein einfacherer und aufwandsärmerer Weg wäre.

§ 345 SGB V-E:

In § 345 Absatz 1 SGB V soll Satz 2 wie folgt gefasst werden:
Die Krankenkassen dürfen die Daten nach Satz 1 zu diesem Zweck verarbeiten und in der elektronischen Patientenakte speichern, soweit die Versicherten hierzu ihre vorherige Einwilligung erteilt haben.

Wir weisen darauf hin, dass die Einwilligung in die Verarbeitung von Gesundheitsdaten ausdrücklich erfolgen muss (Artikel 9 Absatz 2 Buchstabe a DS-GVO), die Einhaltung dieser Vorgabe durch den Gesetzeswortlaut aber nicht sichergestellt erscheint. Auch erscheint fraglich, ob Teileinwilligungen nur in die anderweitige Verarbeitung (ohne die Speicherung in der ePA) zulässig sein sollen, was nach der DS-GVO der Grundsatz wäre (vgl. EG 32 Satz 5 zur DS-GVO). Sprachlich ist zu monieren, dass auch die Speicherung in der ePA eine Verarbeitung ist, so dass fraglich erscheint, warum dies hier gesondert erwähnt wird; zudem ist unklar, ob sich die Zweckbestimmung („zu diesem Zweck“) auch auf die Speicherung in der ePA bezieht oder zu welchem Zweck diese sonst erfolgt. Unklar ist auch, ob die Einwilligung sich auch auf die Speicherung in der ePA beziehen muss oder auf welcher Rechtsgrundlage diese Verarbeitung andernfalls erfolgen soll. Dementsprechend bleibt auch ungeklärt, was bei einem Einwilligungswiderruf zu erfolgen hat, ob dann die Daten auch aus der ePA auch zu löschen sind. In jedem Fall sollte außerdem vor dem Passus „zu diesem Zweck“ das Wort „ausschließlich“ eingefügt werden, um sicherzustellen, dass die Daten nicht ohne Einwilligung zu anderen Zwecken weiterverarbeitet werden, und so das Vertrauen der Gesicherten und damit ihre Bereitschaft zu stärken, die Daten zur Verfügung zu stellen.
Wir weisen außerdem in redaktioneller Hinsicht darauf hin, dass in § 345 Absatz 2 SGB V bislang auf den nicht mehr existenten § 343 Absatz 1 SGB V verwiesen wird (obwohl § 343 Absatz 1a SGB V gemeint ist).

§ 345b SGB V-E:

Der Abgleich von Patientendaten bedarf besonderer Schutzmaßnahmen gegen die kommerzielle Auswertung von Krankheitsbildern. In Bezug auf Absatz 2 stellt sich die Frage, durch wen die Versichertendaten aus der ePA zum Abgleich mit den Anforderungen der Teilnahme an klinischen Studien verarbeitet werden sollen. Es ist klarzustellen, welche Stelle durch diese Norm zur Verarbeitung berechtigt werden soll.

§ 359a SGB V-E:

Nach § 359a SGB V-E sollen Leistungserbringer und zugriffsberechtigte Stellen auf Abrechnungsdaten in der Telematikinfrastruktur zugreifen und diese gemäß § 359a Absatz 7 S. 3 SGB V-E ausdrücklich ohne Einwilligung des Versicherten verarbeiten dürfen.

Diese in Absatz 7 vorgesehene einwilligungsfreie Lösung birgt Missbrauchsrisiken, denn Zugriffsberechtigte nach Absatz 2 umfassen neben Leistungserbringern auch Verrechnungsstellen und Kostenträger. Dabei sind insbesondere Verrechnungsstellen als Dritte ohne originäre Aufgabe im Versorgungsverhältnis tätig.

2. Zu Artikel 7: Änderung des Gesundheitsdatennutzungsgesetzes (GDNG)

§ 1 GDNG-E:

Durch den Entwurf sollen § 1 Absatz 1 und 2 GDNG eine neue Fassung erhalten.

Dabei soll es sich nach der Gesetzesbegründung (S. 177) um eine bloße Klarstellung handeln. Tatsächlich würde aber sprachlich durch die Änderungen beider Absätze eine Erweiterung des Anwendungsbereichs bewirkt. Zudem wäre in Absatz 2 die geänderte Fassung sprachlich unverständlich, da unklar bleibt, was mit einer Verarbeitung zur Weiternutzung gemeint sein soll; die Weiternutzung ist eine Form der Verarbeitung und keine Zweckbestimmung.

§ 3 GDNG-E:

Durch die neu geschaffene Vorschrift soll eine unveränderliche eindeutige pseudonyme Forschungskennziffer für natürliche Personen eingeführt werden.

Eine solche Kennziffer – zumal im Bereich der gemäß Artikel 9 DS-GVO besonders geschützten Gesundheitsdaten – stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Nach der Gesetzesbegründung (Seite 179) handelt es sich hierbei um eine nationale Kennziffer im Sinne des Artikel 87 DS-GVO. Erforderlich sind daher geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen. Ob die im Gesetzentwurf bislang vorgesehenen Maßgaben hier ausreichend sind, erscheint fraglich.
So wird bei Kühling/Buchner, Kommentar zur DS-GVO, BDSG, 4. Auflage 2024, zu Artikel 87 unter Rn. 17 f., u. a. Folgendes ausgeführt:

„Um die Erstellung von Persönlichkeitsprofilen im öffentlichen Bereich zu verhindern, bedarf es bezüglich der Nutzung der Identifizierungsangaben einfach-gesetzlicher Nutzungseinschränkungen. Die bedürfen einer gesetzlichen Grundlage, die der Normenbestimmtheit und -klarheit sowie dem Grundsatz der Verhältnismäßigkeit genügt. Für die Betroffenen muss die größtmögliche Transparenz bei der Erhebung, der Speicherung und bei möglichen Zusammenführungen bei Nutzungen hergestellt werden. Erfolgen heimliche Verarbeitungen, so sind Garantien vorzusehen, mit denen der Rechtsschutz für die Betroffenen eröffnet wird. Bedeutsam ist, dass durch die Verwendung des Kennzeichens keine berechtigten Vertraulichkeitserwartungen verletzt werden. Bedeutsam ist ferner, ob der Betroffene selbst den Erhebungs- oder Verarbeitungsanlass durch eigenes Verhalten gegeben hat, oder ob eine mit einer erhöhten Eingriffstiefe verbundene anlasslose Verarbeitung erfolgt und welche tatsächlichen Konsequenzen sich daraus ergeben können. Der Umstand, dass mit der Ziffer noch keine umfassende Erschließung aller oder eines sehr großen Teils von Verwaltungsdatenbanken erfolgt, genügt als Garantie nicht.
Die Garantien können darin bestehen, dass die zulässigen Anwendungen, Zwecke und Datenumfänge abschließend aufgeführt werden, oder dass nur bestimmte Berechtigte die Kennzeichen verwenden dürfen. Dabei ist die Relevanz für das Persönlichkeitsrecht zu berücksichtigen. Möglich ist auch ein Verbot der elektronischen Speicherung oder das Verbot der Zusammenführung bestimmter Datenbestände. Mit Prüfziffern können Übertragungsfehler vermieden werden. Eine geeignete Maßnahme kann darin bestehen, dass nur eine verwaltungsinterne Nutzung erlaubt und eine öffentliche Verwendung der Kennziffer durch Private verboten wird. Es ist eine Verwendungsbeschränkung, zB nur zur Identitätsfeststellung, möglich. Eine Drittnutzung kann verboten werden, auch wenn dies in der Praxis schwer vermeid- und sanktionierbar sein mag. Normative Vorgaben zur Sicherung der Datenschutzgrundsätze bedürfen der technischen Umsetzung durch die in Art. 32 vorgesehenen Maßnahmen. In jedem Fall muss durch die Garantien bewirkt werden, dass die Erstellung von Profilen der Persönlichkeit des Betroffenen ganz oder auch nur teilweise verhindert werden, mit denen Rückschlüsse auf Art und Inhalt von Beziehungen, Kommunikationsverhalten und Kommunikationsinhalte, soziales Umfeld, persönliche Angelegenheiten,

Interessen, Neigungen und Gewohnheiten sowie Einkommens- und Vermögensverhältnisse möglich werden."

In Bezug zur Forschungskennziffer ist insbesondere zu beachten, dass die Nutzung durch eine Vielzahl von Stellen, und zwar nicht nur verwaltungsintern, erfolgen wird und dass es sich bei den verarbeiteten Daten um sehr sensible Daten handelt. Allein zur Durchsetzung des Widerspruchsrecht erscheint die Einführung einer solchen lebenslangen Kennziffer nicht geboten. Dabei ist insbesondere hinsichtlich § 3 Absatz 5 GDNG-E aus technischer Sicht kritisch zu sehen, dass die Ermöglichung der sektorenübergreifenden Verknüpfung den Schutz durch die Forschungskennziffer alleine schwächt und ggf. die Re-Identifikation der Versicherten vereinfacht bzw. ermöglicht. Auch können Gesundheitsdateninhaber durch die Verwendung der Forschungskennziffer eigene Zuordnungstabellen generieren. Aus der praktischen aufsichtsrechtlichen Tätigkeit ist außerdem bekannt, dass „Datenpannen" in Form einer De-Pseudonymisierung auch in sensiblen Bereichen wie der Forschung mit Gesundheitsdaten vorkommen. Die Folgen können für die betroffenen Personen gravierend sein – und wären bei einer lebenslang anhaftenden identischen Kennziffer unüberschaubar. Dagegen wäre es ein milderes Mittel, eine Forschungskennziffer nur jeweils für ein Forschungsvorhaben zu vergeben.
Für Fälle, in denen Gesundheitsdateninhaber und Gesundheitsdatennutzer identisch sind, führt der Entwurf außerdem zu einer Diskrepanz zwischen § 3 GDNG-E und § 10 Absatz 2 GDNG-E: Gesundheitsdateninhaber sollen nach § 3 GDNG-E die Forschungskennziffer verarbeiten und zur Verknüpfung verwenden dürfen; gegenüber Gesundheitsdatennutzern wird die Forschungskennziffer dagegen nach § 10 Absatz 2 S. 2 GDNG-E nicht offengelegt.

Aus technischer Sicht sollte schließlich in Absatz 2 die Formulierung „im Benehmen" durch „im Einvernehmen" ersetzt werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Kernkompetenz bzgl. kryptographischer Vorgaben (vgl. Technische Richtlinie BSI-TR 02102). Auskunft über die kryptografischen Vorgaben für Projekte des Bundes gibt die Technische Richtlinie BSI TR-03116. Ferner wirkt das BSI an der Erstellung und Pflege internationaler Vorgaben und Standards auf dem Gebiet der Kryptografie mit. Dies geschieht unter anderem im DIN-Normungsausschuss NA 043-01-27 AA und im Rahmen der Mitarbeit bei SOG-IS. Dadurch ist sichergestellt, dass das Verfahren dem Stand der Technik angemessen und das Vertrauen in das Verfahren nicht gefährdet ist. Ähnliches gilt für die Einbeziehung des oder der BfDI.

§ 7 GDNG-E:

§ 7 GDNG-E sieht in Satz 1 vor, die koordinierende Zugangsstelle beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) einzurichten.

Nach Artikel 57 Absatz 1 Buchstabe b der Verordnung (EU) 2025/327 des Europäischen Parlamentes und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847 (EHDS-VO) übernehmen die Zugangsstellen für Gesundheitsdaten u.a. auch die Pseudonymisierung oder Anonymisierung von Daten der Gesundheitsdateninhaber und erhalten somit auch personenbeziehbare medizinische Daten. Beim BfArM ist bereits das Forschungsdatenzentrum Gesundheit (FDZ) angesiedelt (§ 303d SGB V), bei dem medizinische Daten (pseudonymisiert) gespeichert werden. Die Aufgabe der Pseudonymisierung und damit die Möglichkeit zur Reidentifizierung ist dabei auf eine Vertrauensstelle (§ 303c SGB V) beim Robert-Koch-Institut (RKI) ausgelagert. Die Vertrauensstelle und das FDZ sind räumlich, organisatorisch und personell eigenständig zu führen (§ 303a Absatz 2 Satz 1 SGB V). Das RKI führt die Aufgabe der Vertrauensstelle eigenständig und getrennt von seinen übrigen Aufgaben und das BfArM führt die Aufgabe des FDZ eigenständig und getrennt von seinen übrigen Aufgaben (§ 2 Absatz 3 Satz 1 Forschungsdatenzentrum Gesundheit-Verordnung). Das BfArM nimmt somit in unterschiedlichen Gesetzen unterschiedliche Aufgaben war, die eigentlich getrennt werden sollten.

Für die koordinierende Zugangsstelle sollten daher Regelungen zur personellen, räumlichen und technisch-organisatorischen Trennung und zu Weisungsbefugnissen innerhalb des BfArM aufgenommen werden, um eine direkte interne Verknüpfung von Daten beider Stellen zu verhindern.

§ 18 GDNG-E:

Nach § 18 GDNG-E soll die BfDI für die Überwachung und Durchsetzung der Anwendung des Rechts zum Widerspruch nach Artikel 71 EHDS-VO sowie für die Überwachung der Anwendung des Kapitels IV der EHDS-VO bzgl. des Schutzes personenbezogener Daten für nicht-öffentliche Stellen zentral und abweichend von § 40 BDSG zuständig werden. Kapitel IV der EHDS-VO beinhaltet die sog. Sekundärnutzung elektronischer Gesundheitsdaten.

Zur Rechtfertigung der vorgesehenen Sonderzuständigkeit der BfDI heißt es in der nun vorliegenden Gesetzesbegründung u. a. (S. 96, 199):

„Verbliebe die Zuständigkeit für die Datenschutzaufsicht im Anwendungsbereich der EHDS-Verordnung bei den Datenschutzaufsichtsbehörden der Länder, würde sich die Vielzahl der zu lösenden Rechtsfragen mit der Vielzahl der im Kreis der Datenschutzaufsichtsbehörden vertretenen Rechtsauffassungen multiplizieren. Ein solcher Zustand würde Hindernisse für einen reibungslosen funktionierenden Binnenmarkt für Daten kreieren und nicht beseitigen, digitale Innovationen hemmen und nicht fördern sowie einer optimalen Nutzung der Daten zum Wohle von Patienten entgegenstehen und ist damit im gesamtstaatlichen Interesse nicht hinnehmbar“.

Die vorgesehene Alleinzuständigkeit der BfDI für nicht-öffentliche Stellen im Bereich des Kapitels IV der EHDS-VO wird – wie bereits im Schreiben des Co-Vorsitzes des AK Gesundheit und Soziales der DSK vom 5.3.2026 dargelegt – kritisch beurteilt: Denn dies führt nicht nur hinsichtlich der Primär- und Sekundärnutzung von Gesundheitseinrichtungen zu einem Auseinanderfallen der Aufsichtszuständigkeit, sondern auch hinsichtlich der EHDS-Sekundärnutzung und „allgemeiner Sekundärnutzung“ (Forschung, Qualitätssicherung etc.) und damit zu einer erheblichen Zersplitterung der Aufsichtszuständigkeiten und in Folge auch zu Intransparenz bei den Betroffenen:

„In diesem Fall fiele eine Primärnutzung, etwa über Krankenhäuser, Apotheken oder Arztpraxen, in die Zuständigkeit der Länder (siehe dazu auch Artikel 22 EHDS), unabhängig davon, ob es sich um Gesundheitsdaten, Abrechnungsdaten, Beschäftigtendaten, Lieferantendaten etc. handelt, während die – ggf. von der gleichen nicht-öffentlichen Stelle – vorgenommene EHDS-Sekundärnutzung in die Zuständigkeit der BfDI fallen würde. Auch für die übrige „Sekundärnutzung“ von Gesundheitsdaten durch nicht-öffentliche Gesundheitseinrichtungen (z.B. Forschungsvorhaben nach GDNG, klinische Prüfungen etc.) sind die Aufsichtsbehörden der Länder zuständig.

Ein solches Auseinanderfallen von Zuständigkeiten führt zu einer Verkomplizierung. Beispielsweise müssten die datenschutzrechtlichen Informationsdokumente in Krankenhäusern stärker nach Versorgung (primäre Nutzung) und „allgemeiner Sekundärnutzung“ einerseits und EHDS-Sekundärnutzung differenzieren und jeweils eine andere Aufsichtsbehörde nachvollziehbar und leicht verständlich aufführen. Betroffene Personen könnten sich mit ihren Anliegen oft an die falsche Aufsichtsbehörde wenden, was zusätzlichen Aufwand bei der Abstimmung erzeugen würde. Das ist nicht bürger- und nicht grundrechtsfreundlich. Ferner besteht ein erheblicher Abstimmungsaufwand der Verantwortlichen mit zwei Aufsichtsbehörden. Eine doppelte Aufsichtszuständigkeit führt für die Verantwortlichen nicht zu einem Bürokratieabbau, sondern zu zusätzlichen Belastungen und Unklarheiten, da für diese nicht ohne weiteres immer klar erkennbar sein könnte, in welchem Regelungsregime sie sich befinden […]. In der bislang angedachten künstlichen Trennung der Datenschutzaufsicht für Primär- und Sekundärnutzung würden Kontrollwege intransparent und unübersichtlich – und damit für Grundrechtsträger erschwert. Zudem werden in den

Datenschutzbehörden Doppelstrukturen aufgebaut, da ja die – verfassungsrechtlich determinierte – Zuständigkeit für öffentliche Stellen in den Ländern verbliebe. Auch dies ist nicht effektiv“.

§ 25 GDNG-E:

§ 25 GDNG-E soll den bisherigen § 6 GDNG ersetzen. Hierzu gibt es folgende Anmerkungen:

Materiell soll die bisherige Regelung nur insoweit geändert werden, dass bei der Beschreibung des Zwecks der Weiterverarbeitung in Absatz 1 Satz 1 Nummer 2 nach „zur medizinischen, zur rehabilitativen und zur pflegerischen Forschung“ eingefügt werden soll: „einschließlich dem Entwickeln von KI-Modellen und KI- Systemen im Sinne von Artikel 3 Nummer 1 der Verordnung (EU) 2024/1689 im Gesundheitsbereich“. Aus dieser Formulierung mit „einschließlich“ wäre aber nicht hinreichend klar erkennbar, ob es sich um medizinische, rehabilitative und pflegerische Forschung handeln muss oder ob auch ein „schlichtes“ Entwickeln von KI-Modellen und KI-Systemen zulässig sein soll (was die Begründung des Entwurfs allerdings vorauszusetzen scheint). Zum Zwecke der Normenklarheit und Vermeidung von Missverständnissen mit möglicherweise weitreichenden Folgen bei der Gesetzesanwendung sollte bereits im Gesetzestext klargestellt werden, dass es sich immer um Forschung handeln muss.

Präzisierung der Antragsbefugnis:
§ 6 Absatz 3 Satz 4 GDNG bzw. § 25 Absatz 3 Satz 4 GDNG-E erfasst ausschließlich „öffentlich geförderte Zusammenschlüsse datenverarbeitender Gesundheitseinrichtungen“. Offen lässt das Gesetz jedoch, wer genau Förderadressat sein muss und ob eine Förderung für die gesamte Dauer der antragsgegenständlichen Datenverarbeitung vorliegen muss.

Präzisierung des behördlichen Prüfprogramms:
§ 6 Absatz 3 Satz 4 GDNG bzw. § 25 Absatz 3 Satz 4 GDNG regeln nicht ausdrücklich, von welchen Voraussetzungen die Erteilung einer behördlichen Zustimmung abhängen soll. Gerade angesichts des gesetzgeberisch intendierten beschleunigten Prüfverfahrens (Soll-Monats-Frist in § 6 Absatz 3 Satz 5 GDNG), sollte das Gesetz unter Berücksichtigung der jeweiligen Prüf- und Darlegungsaufwände hinreichend bestimmt zum Ausdruck bringen, von welchen Voraussetzungen die Erteilung der Zustimmung abhängig ist.

Federführende Zuständigkeit:
Die in § 5 GDNG niedergelegten Regelungen zur federführenden Zuständigkeit einer Datenschutzaufsichtsbehörde finden im Rahmen des bisherigen Zustimmungsverfahrens nach § 6 Absatz 3 Satz 4 GDNG keine Anwendung, wenn eine öffentliche Stelle (etwa ein Uniklinikum) an dem Forschungsvorhaben beteiligt ist. Hier wird eine entsprechende Überarbeitung angeregt, um auch für diesen Fall eine gesetzlich federführende Aufsichtsbehörde zu bestimmen.

In seiner derzeitigen Ausgestaltung führt § 25 Absatz 3 Satz 4 GDNG-E dazu, dass jeweils eigene, isolierte Anträge auf Zustimmung durch die einzelnen datenverarbeitenden Gesundheitseinrichtungen bei den jeweils zuständigen Aufsichtsbehörden gestellt werden müssen. Zur Straffung und Verschlankung der Antragsverfahren nach § 25 Absatz 3 Satz 4 GDNG sollte daher vorgesehen werden, dass die Antragstellung durch alle beteiligten Stellen gemeinsam gegenüber einer der beteiligten Datenschutzaufsichtsbehörden zu erfolgen hat.

26 GDNG-E:

Ergänzend zur Stellungnahme der BfDI vom 29.04.2026 wird auf Folgendes hingewiesen:

Mit § 26 GDNG-E soll den Aufsichtsbehörden die Aufgabe übertragen werden, auf Antrag Verantwortlichen für Forschungsvorhaben die Genehmigung erteilen zu können, die für das jeweilige Forschungsvorhaben erforderlichen Gesundheitsdaten auch ohne Einwilligung der betroffenen Personen verarbeiten zu dürfen. Die Genehmigung soll nach Artikel 26 Abs. 4 GDNG-E nicht erteilt werden dürfen, soweit der Zugang zu den im Antrag genannten Daten abschließend spezialgesetzlich geregelt ist oder Zugang in angemessener Form auf Grund einer anderen Rechtsgrundlage möglich ist.

Die Regelung wird in der geplanten Fassung sowohl als rechtlich zweifelhaft als auch unpraktikabel bewertet.

So wird der sachliche Anwendungsbereich der Vorschrift durch § 26 Abs. 1 Satz 1 GDNG-E nur äußerst grob bestimmt („Forschungsvorhaben"). Auch aufgrund dieser äußerst weiten Formulierung der Vorschrift ist zweifelhaft, ob für eine solche Regelung im Bereich der Sekundärnutzung überhaupt eine hinreichende Kompetenz des Bundesgesetzgebers (z.B. nach Artikel 74 Abs. 1 Nr. 13, 19 oder 19a GG) besteht.

Bereits in dem am 5.3.2026 an das BMG gerichtete Schreiben des Co-Vorsitzes des AK Gesundheit und Soziales der DSK wurde das Einführen neuer Genehmigungsaufgaben kritisiert:

„Unabhängig von der Zuständigkeit sollte außerdem kritisch geprüft werden, ob die Genehmigung oder Freizeichnung durch Datenschutzaufsichtsbehörden als Tatbestandsvoraussetzung von Forschungsregelungen vorzusehen ist. Es handelt sich hierbei um eine spezifische Maßnahme zur Wahrung der Rechte und Freiheiten der betroffenen Person im Sinne des Artikel 9 Absatz 2 Buchstabe j DS-GVO, die der Absicherung eines ausreichenden Datenschutzniveaus dienen kann. Forschungsvorhaben müssten aber vorab ein zusätzliche[s] bürokratisches Prüfungsverfahren absolvieren. Die vorherige Genehmigung von Datenverarbeitungsvorgängen durch Aufsichtsbehörden ist bisher die Ausnahme und erfordert eine detaillierte Betrachtung der Verarbeitungsvorgänge (vergleichbar einer Zertifizierung nach Artikel 42 DS-GVO). Für ein schlankes und kurzes Verfahren müssten die Aufsichtsbehörden zudem mit den entsprechenden zusätzlichen personellen Ressourcen ausgestattet werden."

Die Ausführungen auf Seite 6 des Gesetzesentwurfs, wonach bei den Ländern keine Kosten entstehen, gehen somit fehl.

Wie von der BfDI in ihrer Stellungnahme vom 29.04.2026 ausgeführt, sieht ferner die DS-GVO nicht vor, dass datenschutzrechtliche Rechtsgrundlagen durch Genehmigungen von Datenschutzaufsichtsbehörden ersetzt werden.

Insoweit ist unverständlich, warum neben dem in § 25 Absatz 3 Satz 4 GDNG-E gewählten Ansatz einer „Zustimmung" durch die Datenschutzaufsichtsbehörde nun offenbar mit der „Genehmigung" ein weiterer neuer Typus einer ex ante-Entscheidung durch die Aufsichtsbehörden eingeführt werden soll. Insbesondere ist unklar, ob das Genehmigungsverfahren vom Zustimmungsverfahren nach § 25 Absatz 3 Satz 4 GDNG-E inhaltlich abweichen oder damit in der Sache dasselbe bezweckt werden soll.

Zudem ist das Verhältnis insbesondere zu den §§ 24, 25 GDNG-E und zu § 27 BDSG nicht geklärt.

Unklar ist ferner, ob mit dem Begriff der „Verarbeitung" nur die sog. Eigenverarbeitung oder auch die Übermittlung an Dritte zu den gesetzlichen Zwecken gemeint ist. Bereits im jetzigen § 6 GDNG (§ 25 GDNG-E) wird angesichts der höheren Eingriffstiefen insoweit stets deutlich differenziert, was angesichts der höheren Eingriffstiefe einer Übermittlung im Vergleich zur lediglich zweckändernden Eigennutzung auch als verfassungsrechtlich geboten angesehen wird. Es ist unklar, wie die Datenschutzaufsichtsbehörden den methodischen Ansatz der Datenverarbeitung -§ 26 Absatz 1 Nummer 4 GDNG-E - als Tatbestandsmerkmal für die Genehmigungserteilung überprüfen sollen.

Die inhaltlichen Anforderungen für eine Genehmigung nach § 26 GDNG-E werden derzeit als deutlich unzureichend angesehen.

Nach § 26 Absatz 3 Satz 1 GDNG-E kann die Genehmigung erteilt werden, wenn die Verarbeitung für das Forschungsvorhaben erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen. Für sich genommen erscheint die Absenkung von einem „erheblichen Überwiegen“ (wie etwa in § 27 BDSG oder vielfach im Landesrecht) auf ein einfaches Überwiegen durchaus möglich, da Artikel 9 Absatz 2 Buchstabe j DS-GVO diese hohe Schwelle nicht zwingend voraussetzt. Unverständlich ist jedoch, warum § 26 Absatz 3 GDNG-E die ausdrückliche unionsrechtliche Anforderung, angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person zu treffen (Artikel 9 Absatz 2 Buchstabe j DS-GVO) übergeht und nur eine Genehmigung durch die Datenschutzaufsicht vorsieht. Die Unionsrechtswidrigkeit der Vorschrift erscheint damit offenkundig.
Das Verhältnis zu § 25 GDNG-E sowie zu sonstigen Rechtsgrundlagen des Landes- oder Bundesrechts bleibt mit der Regelung des § 26 Absatz 4 GDNG-E (wonach eine Genehmigung nicht erteilt werden darf, „soweit der Zugang zu den im Antrag genannten Daten abschließend spezialgesetzlich geregelt ist oder der Zugang in angemessener Form auf Grund einer anderen Rechtsgrundlage möglich ist“) im Wesentlichen unklar. Bereits bestehende Verarbeitungsbefugnisse werden in vielen Fällen nicht hinreichend deutlich erkennen lassen, dass sie eine „abschließende“ Regelung bezwecken (§ 26 Absatz 4 Variante 1 GDNG-E). Unklar ist darüber hinaus aber auch, wann ein „Zugang in angemessener Form“ aufgrund einer anderweitigen Rechtsgrundlage bestehen würde (§ 26 Absatz 4 Variante 2 GDNG-E). Aufgrund des äußerst weiten sachlichen Anwendungsbereichs (s.o.) dürfte § 26 GDNG-E damit dazu führen, dass die bestehenden bereichsspezifischen Regelungen in vielen Fällen durch diese weitgehend unbestimmte Vorschrift überlagert und inhaltlich aufgeweicht werden. Auch die Bedeutung des § 25 GDNG-E wäre damit in Frage gestellt.

Die angeordnete Geltung des Bundes-Verwaltungsverfahrensgesetzes (VwVfG) nach § 1 Absatz 5 GDNG-E erscheint zumindest im Hinblick auf §§ 25 und 26 GDNG-E unverständlich. Soweit – wie wohl regelmäßig der Fall – die Zuständigkeit für eine „Zustimmung“ (§ 25 Absatz 3 Satz 4- 6 - GDNG-E) oder eine „Genehmigung“ (§ 26 GDNG-E) bei den Landesaufsichtsbehörden liegt, kommt das Verwaltungsverfahrensrecht der Länder zur Anwendung (vgl. auch § 1 Absatz 3 Bundes-VwVfG). Die Vorschrift des § 26 Absatz 3 Satz 2 GDNG-E, wonach die Genehmigung jederzeit ganz oder teilweise zurückgenommen, widerrufen oder mit Nebenbestimmungen verbunden werden, erscheint äußerst weitgehend, nicht zuletzt auch im Hinblick auf die wohl anzunehmenden Erwartungen eventueller Antragsteller, und wird auch wegen des Grundrechts auf Forschung gemäß EU-Grundrechtecharta und aus verfassungs- und verwaltungsrechtlichen Gründen als rechtlich bedenklich bewertet.
Es sollte daher geprüft werden, ob diese Abweichung von den allgemeinen verwaltungsrechtlichen Regeln (vgl. §§ 36, 48, 49 Bundes-VwVfG) tatsächlich erforderlich ist.
Wie bereits § 6 GDNG/§ 25 GDNG-E trifft auch § 26 GDNG-E im Ergebnis keine sachgerechten Vorkehrungen für ein praxistaugliches und möglichst bürokratiearmes Antragsverfahren.
Insoweit bedürfte die geplante Regelung des § 26 GDNG-E einer erheblichen Überarbeitung oder aber wäre insgesamt zu streichen.

Sollte an der Regelung festgehalten werden wird für §§ 25, 26 GDNG-E die Einführung einer Evaluationsklausel angeregt.