

Stellungnahme
der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes
und der Länder vom 12. Februar 2026

zum Referentenentwurf des
Bundesministeriums für Forschung, Technologie und Raumfahrt:

Entwurf eines Gesetzes zur verbesserten Nutzung von Daten für die Forschung
(Forschungsdatengesetz – FDG – Stand: 22.12.2025)

I. Einführung

Das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) hat am 15.01.2026 einen Referentenentwurf für ein Gesetz zur verbesserten Nutzung von Daten für die Forschung veröffentlicht.

Ein wesentlicher Bestandteil des Gesetzesentwurfs ist das Forschungsdatengesetz (FDG). Daneben enthält das Gesetz auch Änderungen des Bundesstatistikgesetzes und anderer Statistikgesetze.

Mit dem FDG soll der Zugang zu und die Zusammenführung von Daten für die öffentliche und private Forschung umfassend verbessert und vereinfacht werden. Außerdem soll die bereichsübergreifende Datenzusammenführung aus unterschiedlichen Quellen von Forschungsdaten, wie den Statistikämtern, Registern und akkreditierten Forschungsdatenzentren, ermöglicht werden. Hierzu soll ein Deutsches Zentrum für Mikrodaten beim Statistischen Bundesamt errichtet werden.

II. Hinweise der DSK

Der verbesserte Zugang zu Forschungsdaten für Forschende ist ein wichtiges Anliegen im Allgemeininteresse, und Forschungs- und Wissenschaftsfreiheit sind grundrechtlich geschützt. Bei diesem Vorhaben muss aber zugleich ein hohes Datenschutzniveau gewährleistet werden.

Für die Verarbeitung personenbezogener Daten zu Forschungszwecken muss ein Ausgleich zwischen den Forschungsinteressen (einschließlich der damit zugleich verfolgten Gemeininteressen) und dem Recht auf informationelle Selbstbestimmung der betroffenen Personen gefunden werden.

Der Referentenentwurf enthält zwar einige Schutzmaßnahmen, wie das voraussetzungslose Widerspruchsrecht der betroffenen Personen, Auskünfte zu Übermittlungen des Deutschen Zentrums für

Mikrodaten über ein Datenschutzcockpit und die Verfügbarmachung der Forschungsdaten ausschließlich in einer sicheren Verarbeitungsumgebung. Auch die Regelung eines Forschungsgeheimnisses und die Pseudonymisierung von Forschungsdaten durch eine Vertrauensstelle sind wertvolle datenschutzrechtliche Schutzmaßnahmen.

Im Hinblick auf die umfangreichen Regelungen zum Zugang zu personenbezogenen Daten und die Verknüpfung dieser Daten ist der Referentenentwurf aber aus datenschutzrechtlicher Sicht noch überarbeitungsbedürftig.

Die DSK weist in Anbetracht der kurzfristigen Gelegenheit zur Stellungnahme im Folgenden auf die wichtigsten Punkte hin und beschränkt sich hierbei auf das Forschungsdatengesetz (FDG).¹

1. Verhältnis zu anderen Normen aus dem Forschungsbereich – unklarer Anwendungsbereich

Nach § 1 Abs. 1 FDG-E dient das FDG der Verbesserung des Zugangs zu und der Nutzung von Daten zu Forschungszwecken. Es gilt nach § 1 Abs. 2 FDG-E nicht, soweit andere Gesetze die Verarbeitung zu Forschungszwecken ausdrücklich ausschließen.

Der Anwendungsbereich des Gesetzes wird durch diese Regelung im Verhältnis zu anderen Gesetzen, die auch Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zu Forschungszwecken enthalten, nicht ausreichend abgegrenzt.

In § 7 Abs. 3 FDG-E ist zwar geregelt, dass § 7 Abs. 1 FDG-E (Zugang zu Daten zu Forschungszwecken) nicht anwendbar ist, soweit ein anderes Gesetz den Zugang zu den Daten erlaubt oder Forschungsdatenzentren befugt sind, Forscherinnen und Forschern den Zugang zu den Daten auf der Grundlage einer Einwilligung der betroffenen Personen zu Forschungszwecken zu gewähren.

Dieser tatbestandliche Ausschluss des Datenzugangs eignet sich aber nicht zu einer rechtsklaren Abgrenzung des Anwendungsbereichs, sondern führt zu Unklarheiten bei der Rechtsanwendung:

Denn grundsätzlich bleibt das FDG nach § 1 Abs. 1 FDG-E in solchen Fällen anwendbar und nur der Datenzugang nach § 7 FDG-E wird ausgeschlossen. Unklar ist, wie hierbei mit Konstellationen umgegangen wird, in denen andere Gesetze anwendbar sind, aber für das konkrete Forschungsvorhaben keinen Datenzugang „erlauben“ (z.B. aufgrund einer negativen Interessenabwägung nach einer spezialgesetzlichen Forschungsklausel). Da in diesem Fall die Verarbeitung durch ein anderes Spezialgesetz nicht im Sinne des § 1 Abs. 2 FDG-E ausdrücklich ausgeschlossen wäre, könnte § 7 FDG-E anwendbar sein und hierdurch die spezialgesetzlichen Einschränkungen unterlaufen werden.

Nach Anlage 1 Nr. 115 zum FDG-E gehören beispielsweise auch die Klinischen Krebsregister der Länder zu den Registern, zu deren Daten nach § 7 Abs. 4 Nr. 1 FDG-E ein Zugang beim Deutschen Zentrum für Mikrodaten beantragt werden kann. Nach dem Bundeskrebsregisterdatengesetz (BKRG) sammelt das Zentrum für Krebsregisterdaten die Daten der klinischen Krebsregister und stellt diese Forschenden zur Verfügung. Das BKRG enthält hierzu spezifische Vorschriften (§ 8 BKRG), die hier vorrangig anwendbar sein sollten, da sie auf die betroffenen besonders sensiblen Gesundheitsdaten zugeschnitten sind.

In § 1 FDG-E sollte der Anwendungsbereich des FDG daher klar beschrieben werden. Ein Ausschluss für den Bereich der Gesundheitsforschung, der im FDG-Referentenentwurf 2024 noch vorgesehen war, erscheint im Hinblick auf den besonderen Schutzbedarf dieser Daten geboten.

¹ Die Abkürzung „FDG-E“ ohne Angabe des Artikels bezeichnet im Folgenden Artikel 1 des Referentenentwurfs.

2. Unabhängigkeit des Deutschen Zentrums für Mikrodaten und Wahrung des Abschottungs- und Trennungsgebotes

Nach § 3 Abs. 1 FDG-E soll beim Statistischen Bundesamt als vom Verwaltungsbereich des Statistischen Bundesamtes zu trennende, eigene und unabhängige Organisationseinheit ein Deutsches Zentrum für Mikrodaten eingerichtet werden, das aus einer Forschungsstelle und einer Vertrauensstelle bestehen soll. Dabei soll das Deutsche Zentrum für Mikrodaten nach dem Wortlaut des Entwurfs uneingeschränkt der Rechts- und Fachaufsicht des Bundesministeriums für Forschung, Technologie und Raumfahrt unterstehen. Nach § 3 Abs. 2 FDG-E sind die Forschungsstelle und die Vertrauensstelle räumlich, organisatorisch und technisch voneinander zu trennen.

Wenn der Gesetzgeber das Deutsche Zentrum für Mikrodaten beim Statistischen Bundesamt ansiedelt, muss durch konkrete gesetzliche Vorgaben sichergestellt werden, dass das Deutsche Zentrum für Mikrodaten unabhängig ist und klar vom Statistikbereich des Bundesamts abgeschottet wird. Das gilt im besonderen Maße für die Vertrauensstelle. Die Vertrauensstelle muss zwingend unabhängig, eigenverantwortlich und damit weisungsfrei ausgestaltet sein, um ihre Funktion der Gewährleistung einer „informationellen Gewaltenteilung“ erfüllen zu können. Zudem muss die Vertrauensstelle entsprechend dem für den Statistikbereich verfassungsrechtlich geltenden Abschottungs- und Trennungsgebot auch von der Forschungsstelle durch eine „Mauer der Geheimhaltung“ streng abgeschottet werden.

Hierfür genügt die im Entwurf erwähnte räumliche, organisatorische und technische Trennung allein nicht. Im Gesetz zu ergänzen ist insbesondere noch die personelle Trennung, da es ansonsten zu Überschneidungen bei der Aufgabenwahrnehmung und damit Interessenkonflikten von Beschäftigten, die für beide Stellen tätig sind, kommen könnte. Die personelle Trennung dient auch der Verhinderung einer unzulässigen Verbindung der Datensätze, weswegen sie auch über den jeweiligen Beschäftigungszeitraum hinaus fortgelten sollte. Ein Unterlaufen der Trennung bzw. deren Missachtung sollte außerdem sanktioniert sein. Auch bei der gesetzlichen Ausgestaltung von Aufsichtsbefugnissen sind die notwendige Unabhängigkeit des Deutschen Zentrums für Mikrodaten und die gebotene Abschottung der Vertrauensstelle zu wahren.

Das Pseudonymisierungsverfahren ist insgesamt zu ungenau beschrieben. Es fehlen normenklare Definitionen insbesondere der „identifizierenden“ und der „fachlichen“ Daten. Die wesentlichen Regelungen sind aber insoweit im Parlamentsgesetz zu regeln. Eine Weitergabe von identifizierenden Daten an die Forschungsstelle (vgl. § 5 Absatz 2 Satz 3 letzter Halbsatz FDG-E) widerspricht der Festlegung, dass in dieser nur pseudonymisierte Datensätze verarbeitet werden dürfen (§ 4 Nr. 4 FDG-E). Diese Festlegung ist allerdings eine der wesentlichen Schutzmechanismen, an denen zum Schutz der von der Datenverarbeitung betroffenen Personen zwingend festzuhalten ist.

3. Verantwortlichkeit

Der Gesetzentwurf berücksichtigt bislang nicht ausreichend, dass Zurechnungssubjekt für datenschutzrechtliche Rechte und Pflichten nach Art. 4 Nr. 7 DS-GVO der jeweils datenschutzrechtlich Verantwortliche ist. Dieser muss beispielsweise einen Rechtsgrund für die von ihm vorgenommene Verarbeitung personenbezogener Daten haben, technisch-organisatorische Maßnahmen treffen und Informationspflichten sowie Betroffenenrechte erfüllen. Die Frage, wer der jeweils für die Datenverarbeitung Verantwortliche ist, ist daher datenschutzrechtlich stets im Auge zu behalten und in Gesetzgebungsverfahren möglichst normenklar zu regeln.

Dem wird der Gesetzentwurf bislang an vielen Stellen nicht gerecht. Beispielsweise finden sich in § 2 Nr. 13 und 14 sowie 15 FDG-E Definitionen der neu eingeführten Begrifflichkeiten „datenhaltende

Stelle“ und „daten anbietende Stelle“, ohne dass klar würde, wie sich das zum Begriff des datenschutzrechtlich Verantwortlichen verhält.

Dasselbe gilt für den dort verwendeten Begriff der „hinter der datenhaltenden [bzw. daten anbietenden] Stelle stehenden Einheit, die Träger von Rechten und Pflichten sein kann“. Der Gesetzentwurf spricht vielfach von der Überlassung von Daten an „Forscherinnen und Forscher“, also natürliche Personen, die „Forschungseinrichtungen angehören“. Das greift datenschutzrechtlich zu kurz. Datenschutzrechtlich dürfte eine Übermittlung an die jeweils Verantwortlichen vorliegen, wobei diese sicherzustellen haben, dass nur die Forscherinnen und Forscher Zugriff auf die personenbezogenen Daten haben.

Bei § 5 FDG-E wird nicht klar, wer für die Pseudonymisierung der an die Forschungsstelle übermittelten Daten die datenschutzrechtliche Verantwortung trägt, die daten anbietenden bzw. datenhaltenden Stellen oder die Vertrauensstelle? Auch übersieht die Regelung in § 7 Abs. 7 FDG-E, dass Maßnahmen der Datenschutzaufsichtsbehörde sich typischerweise an den Verantwortlichen und nicht an einzelne Forscherinnen und Forscher richten. Zudem lässt der Referentenentwurf bislang leider auch die datenschutzrechtliche Verantwortung beim Deutschen Zentrum für Mikrodaten offen, insbesondere bleibt unklar, ob hier die Vertrauensstelle und die Forschungsstelle zwei verschiedene Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO darstellen, was mit Blick auf die erforderliche Trennung erforderlich sein dürfte, und wie sich dies zur datenschutzrechtlichen Verantwortung des Statistischen Bundesamts im Übrigen verhält.

Die DSK empfiehlt daher dringend, den Referentenentwurf insgesamt dahingehend zu überarbeiten, dass klar wird, wer wofür datenschutzrechtlich verantwortlich sein soll.

4. Datenzugangsverfahren

Für die Prüfung der Anträge auf Zugang zu Forschungsdaten sieht § 7 FDG-E einige datenschutzrechtliche Prüfkriterien vor, wie die Erforderlichkeit der Daten, das öffentliche Interesse an dem Forschungsvorhaben und die Berücksichtigung des Schutzes personenbezogener Daten.

Der Datenzugang von Forschenden ist dabei zwar tatbestandlich auf die in § 7 Abs. 4 FDG-E bezeichneten Daten beschränkt. Die konkreten Grenzen der tatsächlichen erfassten personenbezogenen Daten bleiben allerdings zum Teil unbestimmt. Vor diesem Hintergrund können Reichweite der Datenverarbeitung und die damit verbundenen Auswirkungen auf die Datenschutzrechte betroffener Personen schwerlich abschließend beurteilt werden. So ist etwa nicht ohne Weiteres nachvollziehbar, welche Daten nach § 7 Abs. 4 Nr. 1 FDG-E von den in Anlage 1 genannten 117 „Registern“ erfasst bzw. nicht erfasst sein sollen, die dort „zum Zwecke der Registerführung eingetragen sind“. Dies gilt umso mehr, als dass laut Gesetzesbegründung der Begriff „Register“ hier „untechnisch und weit“ zu verstehen sein soll. Auch sollte klargestellt werden, was konkret von dem Begriff „systematisch geführte personenbezogene Datenbestände“ (s. etwa Ziff. 11, 25, 33 der Anlage 1) oder „Datenbestände“ (s. etwa Ziff. 88 der Anlage 1)“ erfasst sein soll.

Die vorgenannten Prüfkriterien sollten noch um Angaben zu den technischen und organisatorischen Maßnahmen (TOM), die für das konkrete Forschungsprojekt getroffen werden, ergänzt werden. Diese Maßnahmen sind vom Deutschen Zentrum für Mikrodaten ohnehin für die Interessenabwägung nach § 7 Abs. 1 Nr. 4 FDG-E von Bedeutung, da hierbei Maßnahmen zur Minimierung von Risiken berücksichtigt werden. Die TOM müssen zudem geeignet sein, um die Grundsätze für die Verarbeitung nach Art. 5 DS-GVO umzusetzen und notwendige Garantien aufzunehmen, um allen Anforderungen der DS-GVO zu genügen und die Rechte der betroffenen Personen zu schützen (Art. 25 DS-GVO).

Zudem bestehen inhaltliche Bedenken gegen § 5 Abs. 6 FDG-E. Danach darf die Forschungsstelle pseudonymisierte Datensätze nach Abschluss des Forschungsvorhabens für [weitere] zehn Jahre speichern, wenn die Daten zur Erfüllung weiterer Zugangs- und Zusammenführungsbegehren von Forscherinnen und Forschern erforderlich sind. Neben der aufgrund des Grundsatzes der Datenminimierung problematischen pauschalen Erweiterung für zehn Jahre (statt „bis zu zehn Jahre“) ist dafür kein konkretes Forschungsbegehren nötig. Laut Begründung des Gesetzesentwurfs trifft die Forschungsstelle die Entscheidung über diese Speicherung auf Grundlage ihrer Erwartung über besonders nachgefragte Datensätze. Eine solch abstrakte Prognoseentscheidung der Forschungsstelle ohne weitere Voraussetzungen oder Maßnahmen liefe ebenfalls dem Grundsatz der Datenminimierung zuwider.

Im Verfahren zur Akkreditierung von Forschungseinrichtungen werden nach § 8 Abs. 2 Nr. 3 FDG-E die Erfüllung der datenschutzrechtlichen Anforderungen und damit ggfs. auch die TOM geprüft. Die Akkreditierung wird aber unabhängig von konkreten Forschungsvorhaben für 5 Jahre gewährt. Je nach Sensibilität der Daten sind für unterschiedliche Forschungsvorhaben jedoch unterschiedliche TOM angemessen, so dass eine einrichtungsbezogene Betrachtung nicht ausreicht, sondern eine vorhabenbezogene Betrachtung der TOM erfolgen muss.

Außerdem sollte für die Prüfung der Anträge auf Datenzugang durch das Deutsche Zentrum für Mikrodaten auch die Einbindung eines unabhängigen Gremiums vorgesehen sein. Ein solches Gremium kann die für die Prüfung notwendige unabhängige Expertise aus unterschiedlichen Bereichen (wissenschaftlich-fachlich, ethisch, datenschutzrechtlich etc.) einbringen und sollte zu jedem Antrag ein Votum abgeben, das vom Deutschen Zentrum für Mikrodaten berücksichtigt werden muss.

In anderen Forschungsdatenzugangsökosystemen sind diese Gremien beispielsweise als „Use-and-Access-Committee“ oder „Data Governance Board“ vorgesehen.

5. Zusammenführung von Daten

Der datenschutzrechtliche Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b) DS-GVO steht der Verknüpfung von Datensätzen grundsätzlich entgegen. In Anwendung des Grundsatzes der Datenminimierung nach Art. 5 Abs. 1 lit. c) DS-GVO sind personenbezogene Daten vorrangig zu anonymisieren. Nur in Ausnahmefällen kommt eine Nutzung pseudonymisierter Daten in Betracht. Sofern für Zwecke der wissenschaftlichen Forschung Datensätze ausnahmsweise verknüpft werden sollen, bedarf es im Hinblick auf das Grundrecht auf Datenschutz und das Grundrecht auf informationelle Selbstbestimmung einer besonderen Rechtfertigung, die sich in der Regel aus einem öffentlichen Interesse und einem gesellschaftlichen Nutzen ergeben soll.²

Aufgrund des erhöhten Risikos durch die Zusammenführung für die Rechte und Freiheiten natürlicher Personen bedarf es hier neben einer Erforderlichkeitsprüfung in jedem Fall gesteigerter technischer und organisatorischer Schutzanforderungen in Gestalt von Garantien.

In diesem Zusammenhang sollte eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO vor der Verknüpfung gesetzlich verpflichtend sein und klar geregelt werden, wer diese durchführen muss.

Nach § 9 Abs. 1 S. 2 FDG-E darf das Deutsche Zentrum für Mikrodaten zum Zweck der Zusammenführung bereichsspezifische oder eindeutige bereichsübergreifende Personenkennzeichen wie die Identifikationsnummer nach § 139b der Abgabenordnung („Steuer-ID“) verwenden.

² vgl. DSK-Entschließung vom 22./23. November 2023, Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register, https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_medRegister.pdf, S. 5.

Die Verwendung von eindeutigen bereichsübergreifenden Personenkennzeichen, wie der Steuer-ID, ist aber verfassungs- und datenschutzrechtlich bedenklich.³ Von der Verwendung sollte daher abgesehen werden.

Im Übrigen ist im Hinblick auf die bereichsspezifischen Personenkennzeichen wie z.B. der Sozialversicherungsnummer fraglich, ob die jeweiligen spezialgesetzlichen Zweckbestimmungen und Verarbeitungsbeschränkungen, durch eine zweckändernde Generalklausel aufgehoben werden können.

Nach der Gesetzesbegründung (S. 65) sollen außerdem auch KI-Anwendungen zur Zusammenführung von Daten genutzt werden. Hierfür sollte das FDG-E um eine spezifische gesetzliche Regelung ergänzt werden, die ausreichende Schutzmaßnahmen mit Blick auf die hierdurch entstehenden zusätzlichen Risiken vorsieht.

6. Widerspruch und Betroffenenrechte

Gemäß § 11 Abs. 3 FDG-E können die betroffenen Personen der Verarbeitung von personenbezogenen Daten nach §§ 7 und 9 FDG im FDG-Datenschutzcockpit jederzeit widersprechen.

Dieses Widerspruchsrecht muss aber so ausgestaltet werden, dass betroffene Personen vor der tatsächlichen Verarbeitung ihrer personenbezogenen Daten effektiv über die Verwendung ihrer Daten mitbestimmen können.

Eine angemessene „Sperrfrist“ muss daher sicherstellen, dass betroffene Personen tatsächlich hinreichend Gelegenheit haben, ihr Widerspruchsrecht zur Kenntnis zu nehmen und ausüben zu können, bevor Daten den Forschenden bereitgestellt werden.

Es muss außerdem eine gesetzliche Klarstellung erfolgen, wie die Informationspflichten aus Art. 13, 14 DS-GVO erfüllt werden und welche Rolle das Datenschutzcockpit dabei spielt. Der datenschutzrechtliche Grundsatz der Transparenz ist gerade für den Forschungsbereich von besonderer Bedeutung, um das Vertrauen der betroffenen Personen zu erhalten.

7. Forschungsgeheimnis

In § 12 FDG-E ist eine strafbewehrte Geheimhaltungspflicht für Forscherinnen und Forscher, die Hilfspersonen und Beschäftigten der Vertrauensstelle sowie ein Verbot der zweckwidrigen Nutzung und der Herstellung eines Personenbezugs vorgesehen.

Diese Regelung sollte noch um ein Beschlagnahmeverbot und ein Zeugnisverweigerungsrecht für diesen Personenkreis ergänzt werden.⁴

Dadurch kann das Vertrauen in die Forschung gestärkt und der Schutz der betroffenen Personen erhöht werden.

³ Die DSK hat im Zusammenhang mit dem Registermodernisierungsgesetz bereits mehrfach darauf hingewiesen, dass die Nutzung der Steuer-ID als übergreifendes Ordnungsmerkmal verfassungsrechtlich bedenklich ist, https://www.datenschutzkonferenz-online.de/media/en/20200828_entschlie%C3%9Fung_pkz_final_1.pdf.

⁴ vgl. DSK Petersberger Erklärung, S. 11, https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

Die Beschlagnahme von Forschungsdaten durch Strafverfolgungsbehörden ist ein ernstzunehmendes Risiko für die Forschungsfreiheit, wie der Beschluss des BVerfG vom 25. September 2023 (Az. 1 BvR 2219/20) zeigt.

8. Datenschutzaufsicht

Für länderübergreifende Forschungsvorhaben soll in § 14 FDG-E eine federführende und eine alleinige Datenschutzaufsicht eingeführt werden. Diese Regelungen orientieren sich sehr stark an § 5 GDNG.⁵

Die Festlegung einer (alleinigen oder federführenden) Aufsichtsbehörde für länderübergreifende Datenverarbeitungen nichtöffentlicher Stellen kann eine geeignete Maßnahme sein, um die einheitliche und effektive Durchsetzung des Datenschutzes in Deutschland zu stärken.

Die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO ist schlecht geeignet, als Abgrenzungskriterium zwischen der federführenden Aufsichtszuständigkeit nach § 14 Abs. 1 FDG-E und der alleinigen Aufsichtszuständigkeit nach § 14 Abs. 4 FDG-E zu dienen. In der Praxis ist die Reichweite gemeinsamer Verantwortlichkeit immer wieder im Einzelnen umstritten. Es bedarf daher zumindest einer vorge-schalteten Prüfung durch die beteiligten Aufsichtsbehörden, inwieweit eine gemeinsame Verantwortlichkeit gegeben ist.

Soweit der Entwurf eine Bündelung der Aufsichtszuständigkeit über öffentliche Stellen der Länder bei einer einzelnen Aufsichtsbehörde vorsieht, fehlt eine Gesetzgebungskompetenz des Bundes. Von der alleinigen Aufsicht nach § 5 Abs. 4 GDNG sind dementsprechend nur nicht-öffentliche Stellen erfasst. Dies muss in § 14 Abs. 4 FDG-E entsprechend angepasst werden.

Mit dem FDG wird ein neues und übergreifendes Forschungsökosystem geschaffen. Die DSK spricht sich daher dafür aus, dass eine Evaluierung des Gesetzes im FDG-E aufgenommen wird.

⁵ Zu § 5 GDNG hat die DSK jüngst eine Orientierungshilfe veröffentlicht, https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_Zusammenarbeit_mehrerer_Aufsichtsbehoerden_GDNG.pdf