

Erklärung



Erklärung 05/2021 zum Daten-Governance-Gesetz angesichts der gesetzgeberischen Entwicklungen

Angenommen 19. Mai 2021

Der Europäische Datenschutzausschuss (EDSA) hat folgende Erklärung angenommen:

Am 9. März 2021 haben der EDSB und der EDSA die gemeinsame Stellungnahme zum Vorschlag für ein Daten-Governance-Gesetz¹ angenommen, die auch im Europäischen Parlament bei der Anhörung des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) am 16. März 2021 vorgestellt wurde.²

Der EDSA verfolgt aufmerksam die Arbeit der Mitgesetzgeber an dieser wichtigen Gesetzgebungsinitiative, die – zur Erinnerung – Bestimmungen bezüglich der Verarbeitung von Daten, einschließlich personenbezogener Daten, im Zusammenhang mit der Weiterverwendung von Daten im Besitz öffentlicher Stellen, von „Diensten für die gemeinsame Datennutzung“ (zu denen auch sogenannte Datenmakler gehören würden), und im Zusammenhang mit der Verarbeitung von Daten (einschließlich personenbezogener Gesundheitsdaten) durch „datenaltruistische“ Organisationen enthält.

Das Daten-Governance-Gesetz wird schwerwiegende Auswirkungen auf die Rechte und Freiheiten des Einzelnen und der Zivilgesellschaft insgesamt in der gesamten EU haben. In den meisten Fällen wäre die Verarbeitung personenbezogener Daten tatsächlich die Kerntätigkeit der vorgenannten Einrichtungen³ und damit in Bezug auf die Grundrechten auf Schutz der Privatsphäre und der personenbezogenen Daten in Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (die

¹ Gemeinsame Stellungnahme vom EDSA und EDSB 03/2021 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz), abrufbar unter: [Gemeinsame Stellungnahme vom EDSA und EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance \(Daten-Governance-Gesetz\) | Europäischer Datenschutzbeauftragter \(europa.eu\)](#)

² Siehe Entwurf der Tagesordnung der Anhörung [hier](#).

³ Wenn es sich nicht um die ausschließliche Tätigkeit handelt, z. B. bei Anbietern von Diensten für die gemeinsame Datennutzung gemäß Artikel 9 Buchstabe b des Daten-Governance-Gesetzes, die sich ausschließlich auf personenbezogene Daten beziehen.

Charta) und in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) verankert. Diese Rechte sind ein wesentlicher Ausdruck der Werte der Europäischen Union.

Ohne solide Datenschutzgarantien besteht die Gefahr, dass (das Vertrauen in) die digitale Wirtschaft nicht nachhaltig sein würde. Anders gesagt kann die Weiterverwendung, gemeinsame Nutzung und Verfügbarkeit von Daten Vorteile, aber auch verschiedene Arten von Schadenrisiken für die betroffenen Personen und die Gesellschaft als Ganzes mit sich bringen, die sich aus wirtschaftlicher, politischer und sozialer Sicht auf den Einzelnen auswirken.⁴

Um diesen Risiken zu begegnen und sie zu minimieren sowie das Vertrauen des Einzelnen zu fördern, müssen Datenschutzgrundsätze und -garantien bereits ab dem frühen Entwurfsstadium der Datenverarbeitung umgesetzt werden, insbesondere dann, wenn diese personenbezogene Daten betrifft, die nicht direkt von der betroffenen natürlichen Person/Einzelperson erhoben wurden. Darüber hinaus muss das Daten-Governance-Gesetz nicht nur mit der DSGVO, sondern auch mit anderen Unions- und einzelstaatlichen Rechtsvorschriften, insbesondere der Richtlinie über offene Daten⁵, in Einklang stehen und somit auf den übergeordneten Grundsatz der Rechtsstaatlichkeit eingehen und Rechtssicherheit für betroffene öffentliche Verwaltungen, juristische Personen und Einzelpersonen bieten.

Laut Begründung des Daten-Governance-Gesetzes *„ist das Zusammenspiel mit den Rechtsvorschriften über personenbezogenen Daten besonders wichtig. Mit der Datenschutz-Grundverordnung (DSGVO) und der e-Datenschutz-Richtlinie hat die EU einen soliden und vertrauenswürdigen Rechtsrahmen für den Schutz personenbezogener Daten und einen weltweiten Standard geschaffen.“⁶*

Sicherstellung der Kohärenz zwischen dem Daten-Governance-Gesetz und dem EU-Datenschutz-Bestand

Wie in der Gemeinsamen Stellungnahme hervorgehoben wird, **bringt das Daten-Governance-Gesetz jedoch ungeachtet der Darstellung in der Erwägung, dass sie „unbeschadet“ der DSGVO gilt, mehrere erhebliche Unstimmigkeiten mit der DSGVO mit sich.⁷**

Der EDSA stellt fest, dass diese Unstimmigkeiten im ITRE-Berichtsentwurf vom 26. März 2021 bisher nicht angesprochen wurden.⁸ Der EDSA begrüßt jedoch, dass einige der in der gemeinsamen Stellungnahme angesprochenen kritischen Zustände im Kompromisstext des Ratsvorsitzes vom 30. März 2021⁹ angesprochen werden.

⁴ Beispielsweise könnten ohne angemessene Datenschutzgarantien die gesammelten Daten zur Erstellung ausführlicher Profile von Einzelpersonen verwendet und in einer Weise genutzt werden, die deren Interessen untergräbt (z. B. Preisdiskriminierung oder Manipulation im Rahmen von Wahlkämpfen). Siehe Fußnote 60 auf Seite 31 der Gemeinsamen Stellungnahme zur Gefahr der Verwendung personenbezogener Daten zu nicht im Zusammenhang stehenden Zwecken.

⁵ Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 172 vom 26.6.2019, S. 56).

⁶ Begründung, S. 1.

⁷ Siehe Absatz 3.2 der Gemeinsamen Stellungnahme.

⁸ Abrufbar [hier](#).

⁹ Abrufbar [hier](#).

Um diese Unstimmigkeiten anzusprechen, fordern wir die Mitgesetzgeber auf, folgende Punkte sorgfältig zu prüfen¹⁰:

- Erstens sollte das **„Zusammenspiel“ zwischen dem Daten-Governance-Gesetz und der DSGVO** gemäß Artikel 1 des Daten-Governance-Gesetzes geklärt werden, indem die DSGVO als eine Verordnung betrachtet wird, die die „Bausteine“ für einen soliden und vertrauenswürdigen Rechtsrahmen liefert.
- Zweitens müssen die im Daten-Governance-Gesetz verwendete(n) **Definitionen/Terminologie** integriert und geändert werden, um sie mit der DSGVO in Einklang zu bringen.
- Drittens sollte das **Daten-Governance-Gesetz unmissverständlich klarstellen, dass die Verarbeitung personenbezogener Daten immer auf einer angemessenen Rechtsgrundlage gemäß Artikel 6 der DSGVO** und auch auf einer spezifischen Ausnahmeregelung gemäß Artikel 9 im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten beruhen muss.
- Viertens sollten die **Bestimmungen des Daten-Governance-Gesetzes** als Voraussetzung für einen klaren Rechtsrahmen **angeben, ob sie sich auf nicht-personenbezogene Daten, personenbezogene Daten oder beides beziehen**, und auch festlegen, dass im Falle von **„gemischten Datensätzen“** die DSGVO gilt.¹¹
- Fünftens sollten die verfassungsrechtlichen Vorschriften (gemäß Artikel 16 Absatz 2 AEUV), wonach die **gemäß der DSGVO eingerichteten unabhängigen Aufsichtsbehörden (die Datenschutzbehörden) „die“ benannten Behörden sind, die für den Schutz personenbezogener Daten und die Erleichterung des freien Verkehrs personenbezogener Daten zuständig sind**, im Daten-Governance-Gesetz widerspiegelt werden.

Dies bedeutet, dass die **Datenschutzbehörden die wichtigsten zuständigen Behörden im Zusammenhang mit dem Daten-Governance-Gesetz und soweit personenbezogene Daten betroffen sind**, im Hinblick auf öffentliche Stellen, Weiterverwender, Anbieter von Diensten für die gemeinsame Datennutzung, Datennutzer und datenaltruistische Organisationen, die personenbezogene Daten verarbeiten, sowie für die Entwicklung von Leitlinien für Technologien zum Schutz der Privatsphäre oder für Managementsysteme für personenbezogene Informationen (PIMS) zur Förderung verantwortungsvoller Dateninnovation sein müssen.

Wie in der gemeinsamen Stellungnahme¹² in Erinnerung gerufen wird, „verfügen die Datenschutzbehörden aufgrund ihrer Zuständigkeiten und Aufgaben gemäß DSGVO bereits über besondere Fachkenntnisse bei der Überwachung der Einhaltung der Vorschriften für die Datenverarbeitung, bei der Prüfung bestimmter Datenverarbeitungstätigkeiten und der gemeinsamen

¹⁰ Siehe Absatz 3.2 der Gemeinsamen Stellungnahme, die an diese kritischen Aspekte zu Beginn als Punkte erinnert, die in der Gemeinsamen Stellungnahme weiterentwickelt werden.

¹¹ Wenn **Datensätze sowohl personenbezogene als auch nicht-personenbezogene Daten verbinden**, hebt die Mitteilung der Kommission an das Europäische Parlament und den Rat, *Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union*, COM/2019/250 final, hervor, dass, „falls die nicht-personenbezogenen Daten und die personenbezogenen Daten „untrennbar miteinander verbunden“ sind, die Datenschutzrechte und -pflichten aus der Datenschutz-Grundverordnung in vollem Umfang für den gesamten gemischten Datensatz gelten, und zwar auch dann, wenn die personenbezogenen Daten nur einen kleinen Teil des Datensatzes ausmachen.“

¹² Siehe Absatz 153 der Gemeinsamen Stellungnahme.

Nutzung von Daten, bei der Bewertung der angemessenen Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus für die Speicherung und Übermittlung personenbezogener Daten sowie bei der Förderung des Bewusstseins der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter für ihre Verpflichtung im Zusammenhang mit der Verarbeitung personenbezogener Daten.“ Natürlich erfordert die wirksame Erfüllung der neuen Aufgaben gemäß dem Daten-Governance-Gesetz, die in erster Linie den unabhängigen Datenschutzbehörden und dem Europäischen Datenschutzausschuss gemäß Artikel 16 Absatz 2 AEUV übertragen werden sollen, die Bereitstellung angemessener personeller, finanzieller und informationstechnischer Ressourcen.

Der EDSA begrüßt in diesem Zusammenhang die zusätzliche Formulierung in Artikel 1 Absatz 3 des Kompromisstextes des Rates und den ausdrücklichen Hinweis auf die Befugnisse der Aufsichtsbehörden. Aus Gründen der Klarheit und im Bewusstsein des Ermessensspielraums der Mitgesetzgeber empfiehlt der EDSA, in den Rechtstext des Daten-Governance-Gesetzes (Artikel 1) den folgenden Wortlaut von Artikel 1 Absatz 3 des Kompromissvorschlags des Rates einzufügen (fett gedruckte Worte hinzugefügt: „**Zuständigkeiten und**“):

*„Die Unions- und einzelstaatlichen Rechtsvorschriften über den Schutz personenbezogener Daten gelten für alle personenbezogenen Daten, die im Zusammenhang mit dieser Verordnung verarbeitet werden. Insbesondere lässt diese Verordnung die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG, einschließlich der **Zuständigkeiten und Befugnisse der Aufsichtsbehörden**, unberührt. Im Falle von Widersprüchen zwischen den Bestimmungen dieser Verordnung und dem Unionsrecht betreffend den Schutz personenbezogener Daten ist letzteres maßgeblich. Diese Verordnung schafft keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten.“*

Der EDSA fordert die Mitgesetzgeber außerdem auf, dafür zu sorgen, dass seine Gesamtempfehlung in Bezug auf die benannten zuständigen Behörden und die Governance auf Unionsebene bei der Ausarbeitung ihrer jeweiligen Positionen zum Kommissionsvorschlag widergespiegelt und somit ausdrücklich in den Rechtstext des Daten-Governance-Gesetzes aufgenommen wird.

Insbesondere unter Berücksichtigung der im Daten-Governance-Gesetz festgelegten Definitionen.

In der gemeinsamen Stellungnahme wird darauf hingewiesen, dass **die in der DSGVO vorgesehenen Definitionen gelten und nicht implizit durch das Daten-Governance-Gesetz geändert oder aufgehoben werden sollten, da dies die Definitionen beider Rechtsrahmen verwischen und somit Rechtsunsicherheit schaffen würde.**¹³ Darüber hinaus sollten die neuen Definitionen, die im Daten-Governance-Gesetz eingeführt werden, soweit sie sich auf die Verarbeitung personenbezogener Daten beziehen, eigentlich keine „Vorschriften“ enthalten, die mit der DSGVO unvereinbar sind.¹⁴ Dies ist in der Tat ein entscheidender Punkt, auf den der EDSA die Aufmerksamkeit der Mitgesetzgeber dringend lenken möchte.

Einerseits sollte das Daten-Governance-Gesetz die Definitionen von „personenbezogenen Daten“, „betroffene Person“, „Einwilligung“ und „Verarbeitung“ enthalten, die sich auf die Definitionen in der DSGVO¹⁵ beziehen; andererseits sollten die Definitionen von „Metadaten“, „Dateninhaber“,

¹³ Siehe Unterabsatz 3.2.B. der Gemeinsamen Stellungnahme.

¹⁴ Siehe auch Punkt 44 der Gemeinsamen Stellungnahme.

¹⁵ Siehe in diesem Zusammenhang Kompromisstext des Rates vom 30. März 2021.

„Datennutzer“, „gemeinsame Nutzung von Daten“ und „Datenaltruismus“ im Daten-Governance-Gesetz geändert werden, um Unstimmigkeiten und Rechtsunsicherheit zu vermeiden und der „Natur der zu achtenden Rechte“ zu entsprechen, nämlich dem persönlichen Charakter des Rechts auf Schutz personenbezogener Daten als Recht, das sich auf jede Person¹⁶ bezieht, und als unveräußerliches Recht, auf das „nicht verzichtet werden kann“ und das nicht zum Gegenstand von Eigentumsrechten gemacht werden kann.¹⁷

In diesem Zusammenhang bedauert der EDSA den Verweis auf den „Austausch, die Bündelung oder den Handel mit Daten“, wie er im Kompromisstext des Rates in Bezug auf die Definition des „Anbieters von Diensten für die gemeinsame Datennutzung“ hinzugefügt wurde, da er, soweit es sich um personenbezogene Daten handelt, den Gedanken nahelegt, deren Handel zu legitimieren, und somit nicht mit dem persönlichen Charakter des Rechts auf Schutz personenbezogener Daten vereinbar ist. Da Datenschutz sogar ein Grundrecht ist, das in Artikel 8 der Charta garantiert wird, und unter Berücksichtigung der Tatsache, dass eines der Hauptziele der DSGVO darin besteht, betroffenen Personen die Kontrolle über die sie betreffenden personenbezogenen Daten zu verschaffen, **wiederholt der EDSA, dass personenbezogene Daten nicht als „handelbarer Rohstoff“ betrachtet werden können. Eine wichtige Folge daraus ist, dass der Betroffene, auch wenn er in die Verarbeitung seiner personenbezogenen Daten einwilligen kann, nicht auf seine Grundrechte verzichten kann.**¹⁸ Infolgedessen ist der für die Verarbeitung Verantwortliche, dem die betroffene Person ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten erteilt hat, nicht berechtigt, personenbezogene Daten (als so genannten „Rohstoff“) in einer Weise zu „tauschen“ oder zu „handeln“, die nicht im Einklang mit allen geltenden Datenschutzgrundsätzen und -garantien steht.

Als Beispiel für eine Bestimmung, die Anlass zu einer Auslegung geben könnte, die nicht im Einklang mit dem oben genannten „persönlichen Charakter“ steht, definiert Artikel 2 Absatz 5 des Daten-Governance-Gesetzes den „Dateninhaber“ (einschließlich juristischer Personen) unter anderem als denjenigen, der das Recht hat, Zugang zu den unter seiner Kontrolle stehenden personenbezogenen Daten zu gewähren oder diese weiterzugeben.¹⁹ In diesem Zusammenhang merkt der EDSA an, dass die DSGVO jedem Einzelnen das Recht auf den Schutz personenbezogener Daten garantiert, indem sie ein System von Kontrollen und Abwägungen einführt, um den Einzelnen zu schützen, wenn seine personenbezogenen Daten verarbeitet werden.²⁰ Die Verarbeitung personenbezogener Daten muss den Grundsätzen (u. a. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz,

¹⁶ Siehe Punkt 34 der Gemeinsamen Stellungnahme, der sich auf Artikel 8 der Charta bezieht: „1. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. 2. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden.“

¹⁷ Siehe Punkt 118 der Gemeinsamen Stellungnahme: „Der klare Anreiz zur „Monetarisierung“ personenbezogener Daten erhöht auch die Bedeutung der Einhaltung des Datenschutzes“, und Fußnote 54: „In diesem Zusammenhang entwickelt der EDSA Leitlinien zur Erhebung und Verwendung personenbezogener Daten gegen finanzielle Vergütung.“ Siehe auch Fußnote 61 auf S. 30 der Gemeinsamen Stellungnahme.

¹⁸ Siehe EDSA-Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, abrufbar unter: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_de.pdf

¹⁹ Siehe auch Punkte 29-31 der Gemeinsamen Stellungnahme. Siehe auch die unklare Bezugnahme auf „ihre“ Daten in Artikel 11 Absatz 6, Artikel 19 und Artikel 19 Absatz 1 Buchstabe a, die ebenfalls in der gemeinsamen Stellungnahme hervorgehoben wird.

²⁰ Siehe Punkt 29 ff der Gemeinsamen Stellungnahme.

Zweckbindung, Datenminimierung, Richtigkeit) und Vorschriften entsprechen, einschließlich der Rechte der Betroffenen (beispielsweise das Recht auf Information, auch über das ihn oder sie betreffende Profiling; das Recht auf Auskunft; auf Berichtigung; auf Löschung; darauf, nicht einer vollautomatisierten Entscheidungsfindung unterworfen zu werden, die sie oder ihn erheblich beeinträchtigt), auf die der Betroffene nicht verzichten kann. In diesem Zusammenhang stellt der EDSA fest, dass sich die Definition des Dateninhabers, wenn sie überhaupt beibehalten wird, anstatt sich auf eine juristische Person zu beziehen, die „das Recht hat, Zugang zu personenbezogenen Daten zu gewähren oder diese weiterzugeben“, auf die Verarbeitung personenbezogener Daten und die Bedingungen dafür in Übereinstimmung mit dem geltenden Datenschutzrecht beziehen sollte.²¹

Wie im vorgeschlagenen Wortlaut für Artikel 1 des Daten-Governance-Gesetzes dargelegt ist, soweit personenbezogene Daten betroffen sind, das Datenschutzrecht maßgeblich (bei widersprüchlichen Vorschriften).²² Dennoch **ist es wesentlich, im gesamten Verordnungstext widersprüchliche Vorschriften oder Auslegungen zu vermeiden, auch um die umgehende Verständlichkeit des Gesetzestextes zu verbessern.**

In diesem Sinne sollte eine Definition des Begriffs „Erlaubnis“ (von Rechtspersonen zur Weiterverwendung von Daten) eingeführt werden, um unmissverständlich klarzustellen, auf welche (Art von Daten) er sich genau bezieht. Wie in der gemeinsamen Stellungnahme dargelegt, sind wir der Ansicht, dass sich der Begriff aus Gründen der Klarheit nur auf nicht-personenbezogene Daten beziehen sollte.²³

Bedenken im Zusammenhang mit den Abschnittskapiteln des Daten-Governance-Gesetzes

Der EDSA hat auch erhebliche Bedenken hinsichtlich der „Abschnittskapitel“ des Daten-Governance-Gesetzes (II, III und IV) und möchte im Folgenden einige davon in Erinnerung rufen:

- In Bezug auf Kapitel II des Daten-Governance-Gesetzes erinnern wir daran, dass die gemeinsame Stellungnahme empfiehlt, **in den inhaltlichen Teil des Daten-Governance-Gesetzes die Präzisierung in Erwägungsgrund 7 aufzunehmen**, dass „[...] personenbezogene Daten außerhalb des Anwendungsbereiches der Richtlinie (EU) 2019/1024 [unsere Anmerkung: und in den Anwendungsbereich des Daten-Governance-Gesetzes] fallen, sofern die Zugangsregelung den Zugang zu diesen Daten aus Gründen des Schutzes der Privatsphäre und der Integrität des Einzelnen ausschließt oder einschränkt, insbesondere in Übereinstimmung mit den Datenschutzvorschriften“.²⁴

Dies bedeutet, dass das Daten-Governance-Gesetz insbesondere für den von der Richtlinie über offene Daten gemäß Artikel 1 Absatz 2 Buchstabe h abgegrenzten Bereich gelten würde, d. h.:

²¹ Siehe auch Punkt 31 der Gemeinsamen Stellungnahme.

²² Im gleichen Sinne siehe Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. L 136, 22.5.2019, S. 1, Artikel 3 Absatz 8: „Das Unionsrecht betreffend den Schutz personenbezogener Daten gilt für alle personenbezogenen Daten, die im Zusammenhang mit Verträgen gemäß Absatz 1 verarbeitet werden. Insbesondere lässt diese Richtlinie die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG unberührt. Im Fall von Widersprüchen zwischen Bestimmungen dieser Richtlinie und dem Unionsrecht zum Schutz personenbezogener Daten ist letzteres maßgeblich.“

²³ Siehe Punkt 47 ff der Gemeinsamen Stellungnahme.

²⁴ Siehe auch Punkt 69 der Gemeinsamen Stellungnahme.

„Dokumente, die nach den Zugangsregelungen der Mitgliedstaaten aus Gründen des Schutzes personenbezogener Daten nicht oder nur eingeschränkt zugänglich sind, und Teile von Dokumenten, die nach diesen Regelungen zugänglich sind, wenn sie personenbezogene Daten enthalten, deren Weiterverwendung gesetzlich nicht mit dem Recht über den Schutz natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten vereinbar ist oder gesetzlich als Beeinträchtigung des Schutzes der Privatsphäre und der Integrität der betroffenen Personen definiert ist, insbesondere im Einklang mit dem Unionsrecht oder dem nationalen Recht im Hinblick auf den Schutz personenbezogener Daten“. Angesichts der Sensibilität der zu achtenden personenbezogenen Daten, und um sicherzustellen, dass das Schutzniveau personenbezogener Daten in der EU nicht gesenkt wird, sowie aus Gründen der Rechtssicherheit empfiehlt die gemeinsame Stellungnahme, **Kapitel II des Vorschlags an die in der DSGVO niedergelegten bestehenden Vorschriften zum Schutz personenbezogener Daten und an die Richtlinie über offene Daten anzugleichen**. Alternativ werden die Mitgesetzgeber in der gemeinsamen Stellungnahme aufgefordert, in Erwägung zu ziehen, **personenbezogene Daten** aus dem Anwendungsbereich dieses Kapitels **auszuschließen**.²⁵

Aufgrund der Tatsache, dass die Einwilligung der betroffenen Person aufgrund des Machtungleichgewichts, das häufig in der Beziehung zwischen der betroffenen Person und den Behörden besteht, möglicherweise nicht als frei gegeben angesehen werden kann, äußert die gemeinsame Stellungnahme Bedenken zu Artikel 5 Absatz 6 des Daten-Governance-Gesetzes²⁶ und fordert die Mitgesetzgeber im weiteren Sinne auf, **in dem Vorschlag eindeutig angemessene Modelle der „Bürgerbeteiligung“ zu definieren, durch die Einzelpersonen in offener und kooperativer Weise an dem Prozess der Festlegung der Szenarien, die die Weiterverwendung ihrer personenbezogenen Daten ermöglichen, teilnehmen können, und zwar nach einem Bottom-up-Ansatz für offene Datenprojekte**.

In der Gemeinsamen Stellungnahme wird außerdem empfohlen, **das Daten-Governance-Gesetz zu ändern, um klarzustellen, dass die Weiterverwendung personenbezogener Daten, die sich im Besitz öffentlicher Stellen befinden, nur dann zulässig ist, wenn sie durch Unionsrecht oder das Recht der Mitgliedstaaten begründet ist**, das eine Liste eindeutiger, miteinander vereinbar Zwecke enthält, für die die Weiterverarbeitung rechtmäßig genehmigt werden kann, oder wenn sie in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zur Wahrung der in Artikel 23 der DSGVO ²⁷genannten Ziele darstellt.

Der EDSA weist ferner darauf hin, dass die Aufnahme von Daten im Besitz öffentlicher Stellen, die aus Gründen der statistischen Geheimhaltung geschützt sind, in den Anwendungsbereich von Kapitel II des Daten-Governance-Gesetzes gemäß Artikel 3 Absatz 1 Buchstabe b dem Grundsatz zu widersprechen droht, wonach personenbezogene Daten, die zu statistischen Zwecken erhoben

²⁵ Siehe auch Punkt 71 der Gemeinsamen Stellungnahme.

²⁶ Artikel 5 Absatz 6: „Wenn die Weiterverwendung von Daten nicht gemäß den in den Absätzen 3 bis 5 festgelegten Verpflichtungen erlaubt werden kann und es keine andere Rechtsgrundlage für die Übermittlung der Daten gemäß der Verordnung (EU) 2016/679 gibt, **unterstützt die öffentliche Stelle die Weiterverwender bei der Einholung der Einwilligung der betroffenen Personen** und/oder der Erlaubnis der Rechtsträger, deren Rechte und Interessen durch eine solche Weiterverwendung beeinträchtigt werden könnten, sofern dies ohne unverhältnismäßig hohe Kosten für den öffentlichen Sektor machbar ist. Dabei können sie von den in Artikel 7 Absatz 1 genannten zuständigen Stellen unterstützt werden.“

²⁷ Siehe auch Punkt 77 der Gemeinsamen Stellungnahme. Siehe ebenso Punkt 75 und Punkt 76 der Gemeinsamen Stellungnahme.

werden, nur zu diesem Zweck verwendet werden dürfen.²⁸ Die Einhaltung dieses Grundsatzes ist entscheidend, um das Vertrauen der betroffenen Person nicht zu untergraben, wenn sie ihre personenbezogenen Daten für statistische Zwecke zur Verfügung stellt.²⁹

- In Bezug auf Kapitel III sollte das Daten-Governance-Gesetz als eine der Bedingungen für das Anbieten von Diensten für die gemeinsame Datennutzung festlegen, dass der Anbieter über Verfahren verfügt, um die Einhaltung des Unionsrechts und des nationalen Rechts zum Schutz personenbezogener Daten zu gewährleisten, einschließlich Verfahren zur Sicherstellung der Ausübung der Rechte der betroffenen Personen. Insbesondere muss der Anbieter der betroffenen Person leicht zugängliche Instrumente zur Verfügung stellen, die es ihr ermöglichen, ihre Einwilligung nicht nur zu erteilen, sondern auch zu *widerrufen*; und er muss Instrumente bereitstellen, die einen umfassenden Überblick darüber geben, wie und zu welchem konkreten Zweck ihre personenbezogenen Daten weitergegeben werden.³⁰

Darüber hinaus erinnert das Daten-Governance-Gesetz an die **Verpflichtung, ggf. eine Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO durchzuführen** und bei verbleibenden hohen Risiken für die betroffenen Personen die Datenschutzbehörde vor der Verarbeitung gemäß Artikel 36 DSGVO zu konsultieren.³¹

- Die gleichen Anforderungen sollten durch das Daten-Governance-Gesetz in Bezug auf datenaltruistische Organisationen festgelegt werden.³² Diese Datenschutzgarantien müssen in das Daten-Governance-Gesetz aufgenommen werden, auch aufgrund der Kennzeichnung – als Anbieter von Diensten für die gemeinsame Datennutzung oder als „in der Union anerkannte datenaltruistische Organisation“ –, die von diesen juristischen Personen genutzt werden würde, um die Einwilligung der betroffenen Person zur Verarbeitung ihrer personenbezogenen Daten zu erhalten, die davon ausgehen würde, dass ein hohes Schutzniveau für diese Daten gewährleistet ist.

In Anbetracht dessen ist der EDSA, wie in der gemeinsamen Stellungnahme angemerkt, der Ansicht, dass die im Daten-Governance-Gesetz vorgesehene Melde-/Registrierungsregelung für Anbieter von Diensten für die gemeinsame Datennutzung bzw. für datenaltruistische Organisationen in Anbetracht der möglichen Auswirkungen der von solchen Einrichtungen vorgenommenen Verarbeitung personenbezogener Daten auf die betroffenen Personen kein ausreichend strenges Prüfverfahren vorsieht. Daher empfiehlt der EDSA, alternative Verfahren zu prüfen, die insbesondere eine systematischere Einbeziehung von Rechenschafts- und Compliance-Instrumenten für die Verarbeitung personenbezogener Daten gemäß DSGVO berücksichtigen sollten, insbesondere die Einhaltung eines Verhaltenskodex oder eines Zertifizierungsmechanismus.³³

²⁸ Siehe Erwägungsgrund 27 der Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates vom 11. März 2009 über europäische Statistiken; sowie Artikel 4 Absatz 1 und Artikel 4 Absatz 2 der Empfehlung des Europarats Nr. R (97)18 zum Schutz der für statistische Zwecke erhobenen und verarbeiteten personenbezogenen Daten.

²⁹ Siehe auch Fußnote 36 der Gemeinsamen Stellungnahme.

³⁰ Siehe Unterabsatz 3.4.1. und Punkt 147 der Gemeinsamen Stellungnahme.

³¹ Siehe Punkt 147 der Gemeinsamen Stellungnahme.

³² Siehe Unterabsatz 3.5.1. der Gemeinsamen Stellungnahme.

³³ Siehe Punkt 140 und Punkt 180 der Gemeinsamen Stellungnahme.

Der EDSA bedauert, dass im Kompromisstext des Rates vom 30.03.2021 nun (ausdrücklich) vorgesehen ist, dass die Registrierung als anerkannte datenaltruistische Organisation keine Voraussetzung für die Ausübung datenaltruistischer Tätigkeiten ist und damit die Kontrollen und Garantien für die Betroffenen im Hinblick auf die entscheidend wichtigen Datenschutzaspekte weiter geschwächt werden. Diese Garantien sind auch aufgrund der unklaren Definition von „Datenaltruismus“ im Rahmen des Daten-Governance-Gesetzes besonders wichtig.

Darüber hinaus **sollte das Daten-Governance-Gesetz eine genaue Definition der „Zwecke von allgemeinem Interesse“ liefern, die von den datenaltruistischen Organisationen verfolgt werden würden.**³⁴ Außerdem sollte das „Europäische Einwilligungsförmular für Datenaltruismus“ für die Verarbeitung personenbezogener Daten durch datenaltruistische Organisationen in Absprache mit dem EDSA und nicht mit dem (noch zu gründenden) Dateninnovationsrat entwickelt werden.³⁵

In der gemeinsamen Stellungnahme wurde auf das Erfordernis der „Unabhängigkeit“ der Anbieter von Diensten für die gemeinsame Datennutzung sowie der „Unabhängigkeit“ von datenaltruistischen Organisationen in der DGA hingewiesen. In Bezug auf datenaltruistische Organisationen empfiehlt die gemeinsame Stellungnahme, **die Unabhängigkeit der datenaltruistischen Organisationen von den gewinnorientierten Einrichtungen zu klären (z. B. rechtlich, organisatorisch, wirtschaftlich).**³⁶ Im Hinblick auf die Anbieter von Diensten für die gemeinsame Datennutzung möchte der EDSA nun auf Erwägungsgrund 22 des Daten-Governance-Gesetzes hinweisen: „[...] *Spezialisierte Datenmittler, die sowohl von Dateninhabern als auch von Datennutzern unabhängig sind, können bei der Entstehung neuer von etwaigen Akteuren mit beträchtlicher Marktmacht unabhängiger datengetriebener Ökosysteme eine unterstützende Rolle spielen. [...]*“ Der EDSA unterstreicht, dass diese Art der Unabhängigkeit der Anbieter von Diensten für die gemeinsame Datennutzung sowohl unter Wettbewerbs- als auch unter Datenschutzgesichtspunkten von zentraler Bedeutung ist.³⁷

Schlussfolgerung

Abschließend fordert der EDSA die Mitgesetzgeber dringend auf, die in der Gemeinsamen Stellungnahme erläuterten wichtigen kritischen Zustände zu berücksichtigen und so zu vermeiden, dass das Daten-Governance-Gesetz ein paralleles Regelwerk schafft, das weder mit der DSGVO noch mit anderem Unionsrecht vereinbar ist, was zu unzureichenden Garantien für die betroffenen Personen und Schwierigkeiten bei der praktischen Anwendung führen würde.

Diese Erklärung, die einige der wichtigsten Punkte der Gemeinsamen Stellungnahme in Erinnerung ruft, berührt nicht eine mögliche künftige ausführlichere Erklärung oder Stellungnahme zu den künftigen Positionen der Mitgesetzgeber.

³⁴ Siehe Punkte 159-160 und 170-171 der Gemeinsamen Stellungnahme.

³⁵ Siehe Unterabsatz 3.5.5 der Gemeinsamen Stellungnahme.

³⁶ Siehe auch Punkt 78 der Gemeinsamen Stellungnahme.

³⁷ Siehe insbesondere: Erklärung des Europäischen Datenschutzausschusses zu den datenschutzbezogenen Auswirkungen von Unternehmenszusammenschlüssen, angenommen am 27. August 2018; „Die zunehmende Marktkonzentration auf den digitalen Märkten hat das Potenzial, das Niveau des Datenschutzes und die Freiheit der Verbraucher digitaler Dienste zu bedrohen“; Erklärung des EDSA zu den Auswirkungen von Unternehmenszusammenschlüssen auf den Datenschutz, angenommen am 19. Februar 2020.

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)