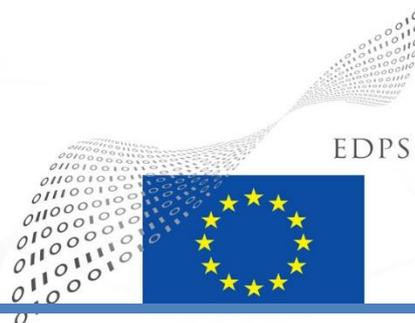


EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 3/2020

Stellungnahme des EDSB zur Europäischen Datenstrategie



16. Juni 2020

Zusammenfassung

Die Europäische Kommission hat am 19. Februar 2020 eine Mitteilung mit dem Titel „Eine Europäische Datenstrategie“ veröffentlicht. Diese ist Teil eines größeren Pakets strategischer Dokumente, das auch eine Mitteilung zur „Gestaltung der digitalen Zukunft Europas“ und ein Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen umfasst.

Ziel der Datenstrategie ist die Schaffung eines einheitlichen europäischen Datenraums, um auf diese Weise Unternehmen und Behörden den Zugang zu hochwertigen Daten zu erleichtern und damit das Wachstum und die Wertschöpfung zu steigern. Darüber hinaus soll sie „die EU in die Lage versetzen [...], zur attraktivsten, sichersten und dynamischsten datenagilen Wirtschaft der Welt zu werden.“ Ein wesentlicher Bestandteil der Datenstrategie ist die Entwicklung gemeinsamer europäischer Datenräume in strategischen Wirtschaftszweigen und Bereichen von öffentlichem Interesse, wie etwa der gemeinsame europäische Gesundheitsdatenraum.

In der vorliegenden Stellungnahme wird der Standpunkt des EDSB zur Datenstrategie insgesamt sowie zu bestimmten konkreten Aspekten dargelegt, etwa zum Begriff „öffentliches Wohl“, zu offenen Daten (*Open Data*), der Nutzung von Daten für die wissenschaftliche Forschung, Datenmittlern, Datenaltruismus, der internationalen gemeinsamen Datennutzung und andere.

Der EDSB versteht die zunehmende Bedeutung von Daten für Wirtschaft und Gesellschaft und unterstützt die umfassenderen strategischen Ziele der EU, etwa die Entwicklung eines digitalen Binnenmarktes und die technologische Souveränität der EU. Zugleich erinnert er daran, dass „*big data comes with big responsibility*“ (große Datenmengen mit einer großen Verantwortung verbunden sind), und daher müssen geeignete Datenschutzgarantien vorhanden sein.

Diesbezüglich beglückwünscht der EDSB die Kommission zu ihrer Zusage, dafür zu sorgen, dass europäische Grundrechte und grundlegende Werte, einschließlich des Rechts auf Schutz personenbezogener Daten, das Fundament aller Aspekte der Datenstrategie und ihrer Umsetzung bilden. Er würdigt insbesondere die Zusicherung, dass die Strategie in voller Übereinstimmung mit der Datenschutz-Grundverordnung ausgearbeitet werden soll, die nicht zuletzt aufgrund ihres in technologischer Hinsicht neutralen Ansatzes eine solide Grundlage bildet.

Der EDSB hebt hervor, dass eines der Ziele der Datenstrategie der Nachweis der Tragfähigkeit und Nachhaltigkeit eines alternativen Datenwirtschaftsmodells sein sollte – offen, fair und demokratisch. Im Unterschied zum derzeit vorherrschenden Geschäftsmodell, das von einer beispiellosen Konzentration von Daten bei einer Handvoll mächtiger Akteure sowie einer allgegenwärtigen Nachverfolgung geprägt ist, sollte der europäische Datenraum als Beispiel für Transparenz, eine effektive Rechenschaftspflicht und ein ausgewogenes Verhältnis zwischen den Interessen einzelner betroffener Personen und dem gemeinsamen Interesse der gesamten Gesellschaft dienen.

Ferner wird in dieser Stellungnahme der durch die Covid-19-Pandemie verursachten beispiellosen weltweiten Krise Rechnung getragen, die sich auf alle Aspekte unseres Lebens auswirkt. In diesem Zusammenhang bekräftigt der EDSB seine Auffassung, dass Datenschutz kein Problem, sondern Teil der Lösung ist. Daten und Technologie können bei der Bewältigung der Krise in Verbindung mit anderen Faktoren eine wichtige Rolle spielen, da es für etwas derart Komplexes kein „Patentrezept“ gibt.

Der EDSB steht der Kommission, dem Rat und dem Europäischen Parlament weiterhin zur Verfügung, um sie bei den nächsten Schritten der Umsetzung der Europäischen Datenstrategie sowohl hinsichtlich des rechtlichen Rahmens als auch praktischer Aspekte weiter zu beraten. Die Anmerkungen in dieser Stellungnahme lassen weitere Anmerkungen in Zukunft zu besonderen Themen und/oder dann, wenn weitere Informationen vorliegen, unberührt.

INHALTSVERZEICHNIS

1. EINLEITUNG UND HINTERGRUND	4
2. ALLGEMEINE KOMMENTARE.....	5
2.1. Anwendung der wesentlichen Datenschutzgrundsätze.....	5
2.2. Rechte betroffener Personen und die Rolle von Datenmittlern	6
2.3. Der Begriff des „öffentlichen Wohls“.....	7
2.4. Offene Daten	9
2.5. Personenbezogene und nicht personenbezogene Daten.....	9
2.6. Organe, Einrichtungen und Agenturen der Europäischen Union	10
3. DATEN FÜR DIE WISSENSCHAFTLICHE FORSCHUNG.....	10
4. GEMEINSAME EUROPÄISCHE DATENRÄUME	12
4.1. Allgemeine Kommentare zum Konzept	12
4.2. Zwingend vorgeschriebene gemeinsame Nutzung von Daten	13
4.3. Gemeinsamer europäischer Gesundheitsdatenraum.....	14
5. BESONDERE FRAGESTELLUNGEN.....	15
5.1. Governance-Rahmen für den Zugang und die Nutzung von Daten.....	15
5.2. Datenschutzgerechte Technologien (<i>privacy preserving technologies</i>).....	16
5.3. „Datenaltruismus“	16
5.4. Qualifikationen und Datenkompetenz	16
5.5. Internationaler Datenaustausch	17
6. SCHLUSSFOLGERUNGEN.....	17
Anmerkungen.....	19

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16, gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf die Artikel 7 und 8, gestützt auf die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)¹,

gestützt auf die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG², insbesondere Artikel 58 Absatz 3 Buchstabe c,

gestützt auf die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates³ –

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG UND HINTERGRUND

1. Die Europäische Kommission hat am 19. Februar 2020 eine Mitteilung mit dem Titel „Eine Europäische Datenstrategie“⁴ vorgelegt. Diese ist Teil eines größeren Pakets strategischer Dokumente, das auch eine Mitteilung zur „Gestaltung der digitalen Zukunft Europas“⁵ und ein Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen⁶ umfasst.
2. Ziel der Datenstrategie (im Folgenden „Datenstrategie“ oder „Strategie“) ist die Schaffung eines einheitlichen europäischen Datenraums, um auf diese Weise Unternehmen und Behörden den Zugang zu hochwertigen Daten zu erleichtern und damit das Wachstum und die Wertschöpfung zu steigern und zugleich die CO₂-Emissionen der EU-Wirtschaft zu verringern. Darüber hinaus soll sie eine Schlüsselrolle bei der Verwirklichung des Ziels der Kommission spielen, „die EU in die Lage [zu] versetzen [...], zur attraktivsten, sichersten und dynamischsten datenagilen Wirtschaft der Welt zu werden.“
3. Die europäische Datenstrategie ist Gegenstand einer öffentlichen Konsultation. Ziel der Konsultation ist es, Meinungen zur Datenstrategie insgesamt sowie zu bestimmten konkreten Aspekten zusammenzutragen. Eine ähnliche öffentliche Konsultation wurde zum Weißbuch zur Künstlichen Intelligenz eingeleitet.
4. Der EDSB wurde am 29. Januar 2020 informell von der Kommission zum ersten Entwurf der Datenstrategie konsultiert und legte vorläufige Kommentare vor. Der EDSB begrüßt es, dass seine Meinung zu einem sehr frühen Zeitpunkt des Verfahrens eingeholt wurde, und bestärkt die Kommission darin, auch in Zukunft an dieser bewährten Praxis festzuhalten.
5. In der vorliegenden Stellungnahme werden einige der informellen Kommentare weiter ausgeführt und angesichts der öffentlichen Konsultation gezieltere Beiträge geleistet. Diese Stellungnahme sollte grundsätzlich mit anderen einschlägigen Stellungnahmen des EDSB, auf die im Dokument

durchgängig verwiesen wird, gelesen werden, etwa die vorläufige Stellungnahme zur wissenschaftlichen Forschung⁷, die Stellungnahme zu offenen Daten⁸, die Stellungnahme zu Systemen für das Personal Information Management⁹ und andere. Darüber hinaus berührt diese Stellungnahme etwaige weitere Kommentare, die der EDSB aufgrund zusätzlicher, zu einem späteren Zeitpunkt vorliegender Informationen, einschließlich im Zusammenhang mit künftigen Konsultationen zu Gesetzesvorhaben in Bezug auf die in der Datenstrategie und im Arbeitsprogramm der Kommission vorgesehenen Rechtsakte vorlegen könnte, nicht.

6. Und schließlich nimmt der EDSB die zur Zeit geführte Diskussion über das Ausmaß, in dem Daten und Technologie im Kampf gegen Covid-19 hilfreich sein könnten, zur Kenntnis. In diesem Zusammenhang möchte der EDSB an seinen Standpunkt erinnern, den auch die anderen Aufsichtsbehörden im Rahmen des Europäischen Datenschutzausschusses (EDSA)¹⁰ teilen, dass Datenschutzvorschriften nicht Maßnahmen im Wege stehen, die aufgrund der Coronavirus-Pandemie getroffen werden. Datenschutz ist kein Problem, sondern Teil der Lösung. Der EDSB vertritt die Auffassung, dass Daten und Technologie bei der Bewältigung der beispiellosen Krise, die sich auf alle Aspekte unseres Lebens auswirkt, eine wichtige Rolle spielen, sie jedoch keinesfalls eine „Patentlösung“ sind. Daten und Technologie können nur dann einen Beitrag zur Bekämpfung der Pandemie und anderen ähnlichen Bedrohungen leisten, wenn sie die Handlungskompetenz des Einzelnen stärken und mit geeigneten Garantien und anderen ganzheitlichen Maßnahmen einhergehen.

2. ALLGEMEINE KOMMENTARE

2.1. Anwendung der wesentlichen Datenschutzgrundsätze

7. Der EDSB begrüßt die im Rahmen der Datenstrategie eingegangene Verpflichtung, sicherzustellen, dass **europäische Grundrechte und grundlegende Werte**, einschließlich des Rechts auf Schutz personenbezogener Daten gemäß Artikel 8 der Charta der Grundrechte der Europäischen Union und Artikel 16 AEUV, bei allen aufgrund der Strategie getroffenen Maßnahmen vollumfänglich geachtet werden.
8. Der EDSB unterstützt insbesondere die Zusage der Kommission, die Strategie in voller Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO) auszuarbeiten. Er ist davon überzeugt, dass die **DSGVO** nicht zuletzt aufgrund ihres in technologischer Hinsicht neutralen Ansatzes **eine solide Grundlage** für die Entwicklung und Umsetzung der Strategie **bildet**.
9. Der EDSB erinnert daran, dass bei der Verarbeitung personenbezogener Daten gemäß Artikel 5 der DSGVO stets die **Grundsätze** der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz; Zweckbindung; Datenminimierung; Richtigkeit; Speicherbegrenzung; Integrität und Vertraulichkeit geachtet werden.
10. Diese Grundsätze gelten auch bei der Verarbeitung personenbezogener Daten für das „öffentliche Wohl“ weiter unverändert. **Zweckbindung** ist eine wesentliche Garantie, damit Personen Vertrauen haben können, dass die von ihnen zur Verfügung gestellten Daten nicht auf unerwartete Art und Weise gegen sie verwendet werden. Wie wichtig der Grundsatz der Zweckbindung ist, haben gerade die Maßnahmen, die zur Bekämpfung des Coronavirus in Erwägung gezogen werden, z. B. Gesundheitsdaten, die unter Aufsicht der Gesundheitsbehörden als Verantwortliche verarbeitet und nicht für gewerbliche oder andere, damit unvereinbare Zwecke verwendet werden sollen, klar gezeigt.

11. Ebenso bedeutend sind auch die Grundsätze der **Transparenz und der Rechenschaftspflicht**. Transparenz sollte als Verpflichtung verstanden werden, sowohl den Bürgerinnen und Bürgern/der Öffentlichkeit als auch Datenschutzbehörden klare, verständliche und leicht zugängliche Informationen zur Verfügung zu stellen. Darüber hinaus ist die Möglichkeit, die Verarbeitungsvorgänge unabhängig zu überprüfen und bei Bedarf Maßnahmen für ihre Durchsetzung zu ergreifen, ein wichtiger Aspekt der Rechenschaftspflicht und kann nicht allein durch Selbstregulierung ersetzt werden.
12. Im Zusammenhang mit dem vorgeschlagenen zukünftigen **Rechtsakt über Daten** empfiehlt der EDSB, Anforderungen für die Hersteller von Produkten, Dienstleistungen und Anwendungen festzulegen, die auf der Verarbeitung personenbezogener Daten beruhen oder personenbezogene Daten verarbeiten, damit diese auch den Rechtsvorschriften über den Datenschutz, insbesondere den Anforderungen des **Datenschutzes durch Technik (*data protection by design*) und durch datenschutzfreundliche Voreinstellungen (*data protection by default*)**, Genüge tun. Eine solche Verpflichtung sollte die bereits bestehenden Verpflichtungen von Verantwortlichen und Auftragsverarbeitern im Rahmen der DSGVO ergänzen und könnte Verantwortliche und Auftragsverarbeiter in erheblichem Maße dabei unterstützen, ihren Datenschutzverpflichtungen nachzukommen, etwa bei der Wahl geeigneter Hardware- oder Softwarelösungen.
13. Der EDSB erinnert daran, dass die Annahme der vorgeschlagenen **Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy-VO)**¹¹ für den Schutz der Grundrechte auf Privatsphäre und auf Schutz personenbezogener Daten im digitalen Zeitalter unerlässlich ist. Daher ist die Vervollständigung des rechtlichen Rahmens der EU für den Datenschutz und die Vertraulichkeit der Kommunikation eine wichtige Voraussetzung für den Erfolg der Datenstrategie.
14. Der EDSB stellt fest, dass die Umsetzung der Strategie unweigerlich damit verbunden sein wird, dass das Ausmaß und die Schwere von Risiken für den Datenschutz, einschließlich von **Sicherheitsrisiken**, zunehmen werden. So erhöht sich beispielsweise mit an das Internet der Dinge angeschlossenen Geräten die „Angriffsfläche“ für Cyberangriffe, und es werden dadurch neue, mögliche nachteilige Auswirkungen auf Einzelpersonen verstärkt oder verursacht. Dieses Problem sollte im Zusammenhang mit der Überarbeitung der Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) oder über neue Gesetzgebungsinitiativen angegangen und könnte auch mit dem Verbraucherschutzrecht und der Verbraucherpolitik der EU verknüpft werden, beispielsweise im Bereich der Produktsicherheit.

2.2. Rechte betroffener Personen und die Rolle von Datenmittlern

15. Der EDSB begrüßt das Ziel der Strategie, dafür zu sorgen, dass Einzelpersonen Kontrolle über ihre Daten ausüben können, u. a. durch Bereitstellung von Werkzeugen und Mitteln, mit deren Hilfe sie selbst detailliert darüber entscheiden können, was mit ihren Daten geschieht („persönliche Datenräume“). In diesem Zuge stellt die Strategie auf eine Stärkung des Rechts des Einzelnen auf Datenübertragbarkeit gemäß Artikel 20 der DSGVO ab.
16. Angesichts dessen, dass die Verknüpfung von Daten den Zugang durch viele verschiedene Akteure erleichtert, ist eine wichtige Voraussetzung dafür, dass Einzelpersonen ihre Rechte als betroffene Personen wirksam wahrnehmen können, die Fähigkeit, sich vergewissern zu können, was mit ihren Daten geschehen ist und durch wen. Daher läuft die gewöhnliche Herangehensweise an die Frage der Transparenz in längeren, abstrakt oder ambivalent formulierten Datenschutzhinweisen, die noch immer von manchen Verantwortlichen verwendet werden, den Anforderungen der DSGVO, Informationen „in präziser, transparenter,

verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“¹², zuwider. In diesem Zusammenhang und insbesondere angesichts der technologischen Entwicklungen erinnert der EDSB daran, dass die Informationen für betroffene Personen gemäß Artikel 12 Absatz 7 und 8 der DSGVO durch **standardisierte und maschinenlesbare Bildsymbole** bereitgestellt werden könnten, um einen leicht wahrnehmbaren, verständlichen und aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln. Die Kommission sollte bis 2022 anhand delegierter Rechtsakte festlegen, wie die erforderlichen Informationen durch solche standardisierten Bildsymbole präsentiert werden können.

17. Es entstehen **Systeme für das Personal Information Management (PIMS)** als vielversprechende Plattformen, um betroffenen Personen eine bessere Kontrolle über ihre personenbezogenen Daten zu bieten. Außerdem könnten einige PIMS-Modelle als Treiber für die Datenübertragbarkeit gesehen werden, da sie als zentrale Dateninfrastruktur fungieren können und Einzelpersonen die Möglichkeit bieten, ihre personenbezogenen Daten zu verwalten. Der EDSB hat bereits eine Stellungnahme zu Systemen für das Personal Information Management veröffentlicht¹³. Darin verweist der EDSB auf die Notwendigkeit, technische Werkzeuge und Standards, die die Wahrnehmung der Rechte betroffener Personen einfach machen (z. B. mit Datenschutzkonsolen), als wichtige Möglichkeit zu entwickeln, Einzelpersonen in die Lage zu versetzen, ihre Daten zu verwalten. In seiner Stellungnahme zu PIMS hat der EDSB darüber hinaus auch insbesondere darauf verwiesen, dass derartige Systeme gegenüber den Nutzern völlig transparent sein und eine echte Nutzerkontrolle gewährleisten müssen.
18. Der EDSB stellt fest, dass es andere Arten von **Datenmittlern** gibt, etwa Datentreuhänder und Genossenschaften, Daten-Marktplätze, Datenmakler usw. Diesbezüglich betont der EDSB, dass klar unterschieden werden muss zwischen Datenmittlern, die sich ausschließlich mit personenbezogenen Daten befassen und versuchen, ihr individuelles Handeln zu stärken, einerseits und denjenigen, die durch wirtschaftliche Anreize angetrieben werden und versuchen, hauptsächlich den Datenaustausch zwischen Unternehmen (Business-to-Business – B2) zu fördern, andererseits.
19. Der EDSB ist der Auffassung, dass Vermittler, die versuchen, betroffene Personen mithilfe von technischen und anderen Werkzeugen in die Lage zu versetzen, die Nutzung ihrer Daten zu verwalten, Beachtung, **weitere Forschung und wirksame Unterstützung** verdienen, da sie zu einer nachhaltigen und ethischen Nutzung von Daten in Einklang mit den Grundsätzen der DSGVO beitragen.
20. Zugleich unterstreicht der EDSB, dass im Hinblick auf die Rolle von **Datenmaklern**, die aktiv große Datenmengen erheben, einschließlich personenbezogener Daten aus unterschiedlichen Quellen, mit Bedacht vorgegangen werden sollte. Sie ziehen eine Vielzahl von Datenquellen heran, die für datenbezogenen Dienstleistungen genutzt werden, wie etwa Daten, die für andere Zwecke, die damit nicht in Zusammenhang stehen, weitergegeben werden, Daten aus öffentlichen Registern (offene Daten) sowie Daten, die beim „Durchforsten“ des Internet und von sozialen Medien erhoben werden, und dabei verletzen sie häufig die Rechtsvorschriften zum Datenschutz. In diesem Zusammenhang stellt der EDSB fest, dass die Tätigkeiten von Datenmaklern, die große Datenmengen erheben, einer immer intensiveren Untersuchung durch eine Reihe nationaler Datenschutzbehörden unterzogen werden¹⁴.

2.3. Der Begriff des „öffentlichen Wohls“

21. In der Datenstrategie wird ein besonderes Augenmerk auf die „**Verfügbarkeit von Daten für das öffentliche Wohl**“ gelegt, was im weiteren Sinne zu verstehen ist – von Gesundheitsversorgung und Umweltschutz bis zur Verbrechensbekämpfung. Der EDSB begrüßt

die Zielvorstellung der Kommission, die Nutzung von Daten für das „öffentliche Wohl“ zu fördern. Der EDSB erinnert an einen der übergreifenden Grundsätze der DSGVO, wonach die Verarbeitung personenbezogener Daten im Dienste der Menschheit stehen sollte.¹⁵

22. Der EDSB stellt weiterhin fest, dass sich die Strategie in gleicher Weise auf den Begriff des „**öffentlichen Interesses**“ bezieht und diesen abwechselnd mit dem Begriff „Wohl der Allgemeinheit“ verwendet. „Öffentliches Interesse“ kann als Grundlage für die rechtmäßige Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe e der DSGVO dienen und hinreichende Gewähr für die Verarbeitung besonderer Kategorien von Daten (z. B. Gesundheitsdaten) im Sinne von Artikel 9 Absatz 2 Buchstabe g und i der DSGVO bieten. Gemäß Artikel 6 Absatz 3 der DSGVO wird die Rechtsgrundlage für die Verarbeitung personenbezogener Daten, die zur Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist, durch Unionsrecht oder das Recht der Mitgliedstaaten festgelegt. Daher dient die Verarbeitung personenbezogener Daten für das „öffentliche Wohl“ denselben wichtigen, in der DSGVO als „öffentliches Interesse“ bezeichneten Zielen, und es sollten dieselben Anforderungen für sie gelten.
23. In diesem Zusammenhang stellt der EDSB fest, dass insbesondere Informationen des öffentlichen Sektors eine Schlüsselrolle im digitalen Binnenmarkt spielen könnten. Darüber hinaus kann von der intelligenten Nutzung von Daten, einschließlich ihrer Verarbeitung durch Künstliche Intelligenz, eine transformative Wirkung auf verschiedene Wirtschaftszweige ausgehen. Der EDSB verweist zugleich darauf, dass für die gemeinsame Nutzung von Daten für soziale oder andere gemeinsame Bedürfnisse **geeignete Datenschutzgarantien** in Einklang mit den Grundsätzen der **Erforderlichkeit und Verhältnismäßigkeit** gelten sollten.
24. Die Nutzung von Daten für das öffentliche Wohl/öffentliches Interesse kann eine Verarbeitung in großem Umfang erforderlich machen, wobei Daten aus unterschiedlichen Quellen kombiniert werden, was möglicherweise besondere Kategorien von Daten und/oder personenbezogene Daten gefährdeter Gruppen von betroffenen Personen umfasst. Sofern dies zutrifft, bringt eine solche Verarbeitung wahrscheinlich ein hohes Risiko mit sich, und Verantwortliche müssen **Datenschutz-Folgenabschätzungen** gemäß Artikel 35 der DSGVO durchführen¹⁶. Des Weiteren empfiehlt der EDSB, die Ergebnisse solcher Folgenabschätzungen, sofern dies möglich ist, als vertrauensbildende und Transparenz fördernde Maßnahme zu veröffentlichen,
25. Die Weiterverwendung von Daten, die für das öffentliche Wohl/für eine im öffentlichen Interesse liegende Funktion erhoben und/oder gemeinsam genutzt werden (z. B. zur Verbesserung des Verkehrs/der Mobilität oder zur Abwehr von ernststen grenzübergreifenden Bedrohungen für die Gesundheit), für gewerbliche gewinnorientierte Zwecke (etwa Versicherung, Marketing usw.) sollte vermieden werden. Eine solche **schleichende Ausweitung der Zweckbestimmung** dürfte nicht nur einen Verstoß gegen die Datenschutzgrundsätze gemäß Artikel 5 der DSGVO darstellen, sondern könnte auch das Vertrauen der Bürgerinnen und Bürger, ein wesentlicher Bestandteil der Strategie, untergraben.
26. Ebenso wichtig ist, dass bei der Verarbeitung von Daten für das öffentliche Wohl **kein Datenoligopol entstehen oder verstärkt werden sollte** (Abhängigkeit des öffentlichen Sektors, von KMU usw. von einigen wenigen mächtigen IT-Unternehmen, so genannten „Big Tech“)¹⁷. Dies ist auch aus Sicht des Datenschutzes von Belang, da Monopole und Oligopole zu einer Anbieterbindung der Nutzer führen und letztlich die Möglichkeit für den Einzelnen, seine Rechte wirksam wahrzunehmen, einschränken.

2.4. Offene Daten

27. Im Hinblick auf die in der Strategie vorgesehene Weiterverwendung von Daten des öffentlichen Sektors durch Unternehmen („Government-to-Business“ – G2B), genauer gesagt der Zugang und die Verarbeitung von Daten im Besitz von Behörden im Sinne der „PSI-Richtlinie“¹⁸, geändert durch die Richtlinie 2019/1024/EU (im Folgenden „**Richtlinie über offene Daten**“)¹⁹, hat der EDSB eine Stellungnahme²⁰ abgegeben, in der er sich auf die folgenden zentralen Grundsätze berief:
- (i) **Transparenz und Einbeziehung der Gesellschaft** beim Zweck der Weiterverwendung gegenüber den Bürgerinnen und Bürgern/betroffenen Personen sowie **Transparenz und eindeutige Festlegung des Zwecks** zwischen dem Lizenzgeber (der Behörde) und Lizenznehmern;
 - (ii) **Datenschutz-Folgenabschätzung** bei der Verarbeitung von Daten im Sinne von Artikel 35 Absatz 3 der DSGVO, um die Risiken und die geeigneten Datenschutzgarantien zur Bewältigung dieser Risiken aufzuzeigen, bevor die Daten weiterverwendet werden.
28. Der EDSB merkt an, dass aufgrund der technologischen, wirtschaftlichen und rechtlichen Besonderheiten eines jeden „Sektors“ (so unterscheidet sich beispielsweise die Verarbeitung von Gesundheitsdaten für Forschungszwecke von der Verarbeitung von intelligenten Energiedaten zur Umsetzung eines „grünen Geschäftsmodells“)²¹ ein „**sektorspezifischer**“ **Ansatz**, der u. a. eine „sektorbezogene“ Datenschutz-Folgenabschätzung erfordert, notwendig sein könnte.
29. Aus Sicht der Informationstechnologie begrüßt es der EDSB, dass die Strategie darauf abzielt, die Weiterverwendung von Informationen des öffentlichen Sektors zu fördern, und zwar durch Abbau der Hindernisse für den Marktzugang, insbesondere für kleine und mittlere Unternehmen, durch Verminderung des Risikos überzogener Vorreitervorteile, die vor allem Großunternehmen zugutekommen und deshalb die Zahl potenzieller Weiterverwender der betreffenden Daten begrenzen, sowie durch Verbesserung der Geschäftsmöglichkeiten durch Förderung der Veröffentlichung dynamischer Daten und Einführung von Anwendungsprogrammierschnittstellen (API).

2.5. Personenbezogene und nicht personenbezogene Daten

30. Der EDSB stellt fest, dass in der Strategie zwischen **drei Kategorien von Daten** unterschieden wird, und zwar nicht personenbezogene Daten, personenbezogene Daten und gemischte Datensätze. In diesem Zusammenhang möchte der EDSB daran erinnern, dass in der Praxis bei einer Kombination aus nicht personenbezogenen Daten der Rückschluss auf personenbezogene Daten möglich ist bzw. solche personenbezogenen Daten erzeugt werden könnten, d. h. Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.
31. In der Strategie wird außerdem auf „**anonymisierte**“ und „**aggregierte**“ Daten verwiesen, und an einer Stelle wird behauptet, dass aggregierte Daten dasselbe sein könnten wie anonymisierte Daten.²² Hier möchte der EDSB darauf hinweisen, dass aggregierte Daten nicht unbedingt nicht personenbezogene Daten sind, da aggregierte Daten sich nach wie vor auf eine identifizierte oder identifizierbare natürliche Person beziehen können. Diesbezüglich erinnert der EDSB daran, dass in Einklang mit Erwägungsgrund 26 der DSGVO und der Rechtsprechung des EuGH²³ alle objektiven Faktoren, einschließlich der Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, gebührend herangezogen werden sollten, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie zu berücksichtigen ist, ebenso die rechtlichen und sonstigen Mittel für den Zugriff auf weitere Daten über die Person.

32. Hinzu kommt, dass Anonymisierungsverfahren nicht unkompliziert sind²⁴. Je vielfältiger die Daten, desto schwieriger ist es, sie zu anonymisieren und dabei das Risiko einer Reidentifizierung auf ein akzeptables Maß zu reduzieren. Die praktischen Schwierigkeiten in Verbindung mit einer robusten Anonymisierung könnten Verantwortliche, insbesondere KMU, davon abhalten, nützliche Daten auszutauschen. Um den erforderlichen Aufwand zu verringern und zugleich zu gewährleisten, dass Daten angemessen anonymisiert werden, empfiehlt der EDSB der Kommission, in gute Anonymisierungsverfahren und Anonymisierungsstandards zu investieren und diese weiter zu unterstützen und zu fördern.
33. Diesbezüglich möchte der EDSB außerdem auf eine Reihe bewährter Verfahren in Bezug auf die Weiterverwendung anonymisierter Daten im öffentlichen Sektor verweisen, etwa die von der Europäischen Arzneimittel-Agentur (EMA) entwickelten ausführlichen Leitlinien für die Industrie, die die Einhaltung dieser Grundsätze erleichtern sollen²⁵, oder die Bereitstellung der Statistiken des Europäischen Statistischen Systems (ESS) als ein hochwertiges „öffentliches Gut“²⁶.

2.6. Organe, Einrichtungen und Agenturen der Europäischen Union

34. Der EDSB stellt fest, dass in der Strategie nicht ausdrücklich auf die Rolle und die geltenden Vorschriften für die Organe, Einrichtungen und Agenturen der Europäischen Union eingegangen wird. Zwar sind die für sie geltenden Datenschutzvorschriften, insbesondere die Verordnung (EU) 2018/1725, weitgehend an die DSGVO und die Richtlinie (EU) 2016/680 angeglichen, und daher sind alle diese Rechtsakte einheitlich auszulegen²⁷. Zugleich sind die Organe und anderen Einrichtungen der Union wichtige eigenständige Akteure in der datengesteuerten Wirtschaft – als Datenanbieter (z. B. über das offene Datenportal der EU), als Nutzer von Daten (z. B. für eine bessere Politikgestaltung) oder als Diensteanbieter (z. B. die digitale eHealth-Diensteinfrastruktur (eHDSI²⁸)).
35. Daher ist der EDSB als Aufsichtsbehörde, die die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Union beaufsichtigt, davon überzeugt, dass die Datenstrategie und die zugehörigen Rechtsakte und nicht bindenden Akte zu ihrer Durchführung der besonderen Rolle der Organe, Einrichtungen und Agenturen der Europäischen Union gebührend Rechnung tragen sollte. Auf diese Weise wird die Union nicht nur für die notwendige Transparenz und Rechtssicherheit sorgen, sondern auch das von der Kommission in der Strategie gegebene Versprechen „mit gutem Beispiel voran“ einlösen²⁹.

3. DATEN FÜR DIE WISSENSCHAFTLICHE FORSCHUNG

36. Der EDSB nimmt den Plan der Kommission zur Kenntnis, die Menge und die Arten von Daten für die wissenschaftliche Forschung gemäß dem Grundsatz „so offen wie möglich, so geschlossen wie nötig“ zu erhöhen. Eine der wichtigsten Initiativen zur Erleichterung der Erhebung, gemeinsamen Nutzung, des Zugangs und der Weiterverwendung von Daten und Dienstleistungen durch Wissenschaftler ist die **Europäische Cloud für offene Wissenschaft**. Letztere dient auch als Modell für die Schaffung der künftigen gemeinsamen europäischen Datenräume.
37. Sowohl in der Vorläufigen Stellungnahme zum Datenschutz und zur wissenschaftlichen Forschung³⁰ als auch in den Leitlinien des EDSA für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch³¹ wird hervorgehoben, dass **Datenschutzvorschriften wie die DSGVO mit echter wissenschaftlicher Forschung voll und ganz in Einklang stehen und sie nicht behindern**. Zugleich ist die Weitergabe personenbezogener Daten immer mit einem gewissen Risiko für betroffene Personen verbunden, auch dann, wenn der Zweck die wissenschaftliche Forschung ist, insbesondere in

Fällen sensibler Daten. Datenschutzvorschriften sollen als robustes Sicherheitsnetz für Personen dienen, deren Daten für die Forschung benötigt werden, sowie als Gerüst, das Wissenschaftler dazu bringt, sich mit Innovationen zu befassen, die den europäischen Werten Rechnung tragen.

38. Es wird allgemein davon ausgegangen, dass wissenschaftliche Forschung der gesamten Gesellschaft zugutekommt und dass wissenschaftliche Erkenntnisse ein öffentliches Gut sind, das es zu fördern und zu unterstützen gilt. Zwar teilt der EDSB im Allgemeinen diese Ansicht, doch darf die Ausübung einer Tätigkeit, die als Forschung gilt, keine *carte blanche* sein, um unverantwortliche Risiken in Bezug auf die Grundrechte einzugehen. Aus Datenschutzsicht sind die Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung von zentraler Bedeutung. Wie bereits in der Vorläufigen Stellungnahme zum Datenschutz und zur wissenschaftlichen Forschung dargelegt, haben Datenschutzbehörden, Ethikausschüsse und die Forschungsgemeinschaft ein gemeinsames Interesse daran zusammenzuarbeiten, um neue Erkenntnisse zu gewinnen und zugleich sicherzustellen, dass Menschen nicht als reine Datensätze behandelt werden.
39. Während eine besondere Datenschutzregelung der wissenschaftlichen Forschung zugutekommt, möchte der EDSB die Kommission und Wissenschaftler, die auf die gemeinsamen Datenräume angewiesen sind, daran erinnern, dass jeder der Grundsätze gemäß Artikel 5 der DSGVO (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz; Zweckbindung; Datenminimierung; Richtigkeit; Speicherbegrenzung; Integrität und Vertraulichkeit; und Rechenschaftspflicht) bei jedem Verarbeitungsvorgang personenbezogener Daten für Forschungszwecke uneingeschränkt zur Anwendung gelangt.
40. Die wissenschaftliche Forschung ist häufig mit der Verarbeitung und gemeinsamen Nutzung besonderer Kategorien personenbezogener Daten der Beteiligten verbunden und könnte daher in bestimmten Fällen als Datenverarbeitung mit einem hohen Risiko im Sinne der DSGVO angesehen werden. Daher empfiehlt der EDSB, dass **geeignete Garantien** vorgesehen werden und der Zugang zu den in den Datenräumen gespeicherten Daten anhand verschiedener Faktoren gewährleistet wird, wie z. B. eine Zugriffsanfrage durch den Akteur, der Zweck der Verarbeitung und das entsprechende Risikoniveau, das Vorhandensein von Rahmenvereinbarungen über gegenseitige Rechenschaft und von Garantien usw. Darüber hinaus sollten dann, wenn in der Forschung mit sensiblen Daten gearbeitet wird, Datenschutz-Folgenabschätzungen unter Beteiligung der jeweiligen Datenschutzbeauftragten (DSB) und von Ausschüssen für Ethikprüfungen durchgeführt werden.
41. Die DSGVO sieht Ausnahmen von bestimmten Verpflichtungen (d. h. das Auskunftsrecht der betroffenen Person (Artikel 15), das Recht auf Berichtigung (Artikel 16), das Recht auf Einschränkung der Verarbeitung (Artikel 18) und das Widerspruchsrecht (Artikel 21)) für Zwecke der wissenschaftlichen Forschung vor, sofern die Verarbeitung in einem angemessenen Verhältnis zum angestrebten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz achtet und geeignete und spezifische Maßnahmen zum Schutz der Grundrechte und der Interessen der betroffenen Person vorsieht. Gleichwohl kann diese besondere Regelung nicht so angewandt werden, dass der Wesensgehalt des Rechts auf Datenschutz beeinträchtigt wird. Daher muss jede Ausnahme von diesen Rechten betroffener Personen besonders gründlich geprüft werden. Hierfür sind eine Einzelfallprüfung, bei der die zu wahren Interessen und Rechte in ein ausgewogenes Verhältnis gebracht werden, sowie eine flexible Bewertung, bei der vielen Faktoren Rechnung zu tragen ist, erforderlich. Jede Beschränkung von Grundrechten im Gesetz ist restriktiv auszulegen und sollte nicht missbraucht werden. Darüber hinaus können Ausnahmen gemäß Artikel 89 Absatz 2 der DSGVO nur „insoweit“ zugelassen werden, als Ausnahmen von diesen Rechten „voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind“.

42. Es gibt keine allgemeingültige Definition von Forschung oder wissenschaftlicher Forschung. Darüber hinaus verschwimmen die Grenzen zwischen öffentlichem Interesse, Freiheit der Lehre und privatem Vorteil inzwischen so sehr wie noch nie. Durch diese Ungewissheit könnten Lücken im Schutz der Grundrechte, einschließlich des Rechts auf Privatsphäre und auf Schutz personenbezogener Daten, entstehen. Daher empfiehlt der EDSB dringend, dass in der Strategie und den geplanten Rechtsvorschriften konkret auf die Definitionen und den Geltungsbereich von Schlüsselbegriffen wie wissenschaftliche Forschung, Innovation oder öffentliches Interesse eingegangen wird, um eine mangelnde Einheitlichkeit in Bezug auf die Begriffe in der DSGVO zu vermeiden³².

4. GEMEINSAME EUROPÄISCHE DATENRÄUME

4.1. Allgemeine Kommentare zum Konzept

43. Ein wesentlicher Bestandteil der Datenstrategie ist die Entwicklung gemeinsamer europäischer Datenräume in strategischen Wirtschaftszweigen und Bereichen von öffentlichem Interesse. In den Datenräumen sollen große Datenbestände, technische Werkzeuge und Infrastrukturen, die für die Nutzung und den Austausch von Daten erforderlich sind, sowie Governance-Mechanismen verknüpft werden. Sie sollen auf einer horizontalen Regelung beruhen, die gegebenenfalls durch sektorspezifische Rechtsvorschriften für den Zugang und die Nutzung von Daten ergänzt wird.
44. Die gemeinsamen europäischen Datenräume stehen in Einklang mit den umfassenderen strategischen Zielen der EU und fördern diese, wie die Entwicklung eines fairen und wettbewerbsfähigen **digitalen Binnenmarktes**, die Übernahme neuer Technologien wie Künstliche Intelligenz und insbesondere maschinelles Lernen sowie die Bewahrung der **digitalen Souveränität der EU**.
45. Der EDSB begrüßt die Zusage in der Strategie, dass gemeinsame europäische Datenräume „**unter uneingeschränkter Einhaltung der Datenschutzvorschriften und nach den höchsten bestehenden Cybersicherheitsstandards**“ entwickelt werden, und freut sich auf die Prüfung der konkreten Vorschläge und Initiativen zur Umsetzung dieser Zusage.
46. Der EDSB begrüßt die Absicht der Kommission, die Annahme von sektorspezifischen Rechtsvorschriften flankierend zur Schaffung bestimmter gemeinsamer europäischer Datenräume in Erwägung zu ziehen. Der europäische Gesetzgeber ist dafür verantwortlich, in Konstellationen, in denen die Strategie zu einer gesteigerten Verfügbarkeit und Weiterverwendung personenbezogener Daten führen würde, zusätzliche Rechtsgarantien zu schaffen. In Bezug auf die gemeinsame Nutzung von Gesundheitsdaten und für die wissenschaftliche Forschung im Allgemeinen bedarf es offenbar besonders dringend einer weiteren Präzisierung und Detailschilderung der in der DSGVO enthaltenen allgemeinen Regelungen auf EU-Ebene. Zugleich kann eine solche Präzisierung, durch die die Vorschriften über die Verarbeitung personenbezogener Daten insbesondere für die wissenschaftliche Forschung soweit wie möglich harmonisiert werden sollen, die gemeinsame Nutzung von Daten weiter fördern.
47. Neben dem horizontalen Datenschutz und den Cybersicherheitsstandards sollte die Kommission auch in die weitere Förderung der **Interoperabilität**, auch im Zusammenhang mit der Datenübertragbarkeit, investieren. Auf diese Weise könnten aufgrund gemeinsamer Datenräume mehr datenschutzkonforme Geschäftsmodelle entstehen und sich erfolgreich durchsetzen.

48. Zwar teilt der EDSB die Ansicht, dass ein Pauschalansatz möglicherweise nicht geeignet ist, doch empfiehlt er der Kommission trotz alledem, weiter zu präzisieren, dass die gemeinsamen europäischen Datenräume nur mit personenbezogenen Daten bestückt werden sollten, die nachweislich in Einklang mit den Rechtsvorschriften zum Datenschutz gewonnen wurden, einschließlich insbesondere mit den Grundsätzen der Rechtmäßigkeit, Zweckbindung und Datenminimierung.
49. Der Strategie zufolge werden Datenräume für vielerlei Zwecke genutzt. Daher sollte von Anfang an für jeden Datenraum genau festgelegt werden, welche Zwecke zulässig sind (d. h. Forschungs- und nichtforschungsbezogene Zwecke usw.). Darüber hinaus ist eine klare Einschränkung der kontextübergreifenden Nutzung von Daten, einschließlich von **Verboten der Nutzung sensibler personenbezogener Daten für andere Zwecke** (beispielsweise die Nutzung genetischer Daten für Versicherungszwecke) aufgrund des Schutzes der Grundrechte auf Privatsphäre und auf den Schutz personenbezogener Daten und des Wertes der Menschenwürde, der das Fundament dieser Grundrechte bildet, in bestimmten Fällen gerechtfertigt. Dies ist für die sektorübergreifende Nutzung personenbezogener Daten im Zusammenhang mit dem Internet der Dinge besonders wichtig.
50. Die gemeinsamen europäischen Datenräume, die auf den europäischen Werten und Grundrechten beruhen, in deren Mittelpunkt der Mensch steht, könnten aber auch als Beweis für die **Funktionsfähigkeit alternativer Modelle** zur derzeitigen Konzentration von Daten bei einer Handvoll mächtiger Privatunternehmen außerhalb der EU dienen, die die Rolle selbst ernannter Gatekeeper im Internet übernehmen, oder großer Anbieter von IT-Lösungen. Daher könnten die geplanten europäischen Datenräume im Hinblick auf **Transparenz, effektive Rechenschaftspflicht und ein ausgewogenes Verhältnis** zwischen den Interessen betroffener Personen und dem gemeinsamen Interesse der Gesellschaft insgesamt eine Vorbildfunktion übernehmen.
51. Der Erfolg der gemeinsamen europäischen Datenräume und der Strategie insgesamt hängt weitgehend von der Fähigkeit ab, eine verlässliche **Vertrauensgrundlage** zwischen den verschiedenen Interessenträgern – betroffene Personen, Regierungen, Privatunternehmen, wissenschaftliche Forschungsgemeinschaft und zivilgesellschaftliche Organisationen sowie Datenschutzbehörden und andere einschlägige Regulierungsstellen – zu schaffen. Hierzu sollte sich das Governance-Modell speziell mit der Einbindung der Bürgerinnen und Bürger und der Zivilgesellschaft befassen.

4.2. Zwingend vorgeschriebene gemeinsame Nutzung von Daten

52. Der EDSB nimmt zur Kenntnis, dass die Kommission beabsichtigt, die **gemeinsame Nutzung von Daten unter bestimmten Umständen zwingend vorzuschreiben**. In letzter Zeit wurde mehrfach der Ruf nach einem geregelten Zugang zu im privaten Besitz befindlichen personenbezogenen Daten für Forschungszwecke, die dem öffentlichen Interesse dienen, laut, etwa die Verbesserung der Gesundheitsversorgung und die Bewältigung der Klimakrise³³. Es wird erwartet, dass solche Initiativen im Zusammenhang mit der Covid-19-Pandemie noch mehr an Bedeutung gewinnen. Darüber hinaus hat der EDSB in seiner Vorläufigen Stellungnahme zur wissenschaftlichen Forschung die Frage von Geschäftsgeheimnissen, insbesondere im Technologiesektor, in dem einige der wertvollsten Daten kontrolliert werden, als größtes Hindernis für die sozialwissenschaftliche Forschung hervorgehoben.
53. Eine mögliche Grundlage für eine Weitergabe von Daten im öffentlichen Interesse im Rahmen des Datenschutzrechts muss im Recht der EU bzw. der Mitgliedstaaten klar formuliert und niedergelegt und durch eine strenge Verhältnismäßigkeitsprüfung und geeignete Garantien zum

Schutz vor Missbrauch und unrechtmäßigem Zugriff flankiert werden. Der EDSB empfiehlt daher eine **offene und umfassende Debatte** über diese Frage, an der sich sämtliche Interessenträger beteiligen sollten, etwa die Forschungsgemeinschaft, Technologieunternehmen, Bürgerrechtsgruppen, Aufsichtsbehörden usw.

54. Und schließlich fordert der EDSB eine behutsame Vorgehensweise bei Initiativen für einen obligatorischen **Zugang zu personenbezogenen Daten im Wettbewerbsumfeld**, d. h. Zugang zu personenbezogenen Daten im Besitz des marktbeherrschenden Unternehmens für seine Mitbewerber. Ein solcher Austausch und Zugang zu Daten unter Mitbewerbern muss gegen andere politische Anliegen, insbesondere Datenschutz, abgewogen werden. Jeder Austausch oder Zugang zu personenbezogenen Daten muss hinsichtlich des Umfangs und Zwecks streng abgegrenzt und in voller Übereinstimmung mit der DSGVO unter Berücksichtigung der Anforderungen an Rechtmäßigkeit und Zweckbindung und der legitimen Erwartungen der Nutzer erfolgen.

4.3. Gemeinsamer europäischer Gesundheitsdatenraum

55. Einer der neun strategischen Bereiche, in denen die Kommission aus der Zusammenführung von Daten und technischen Ressourcen einen klaren Mehrwert für die Union sieht, ist das **Gesundheitswesen**. Ziel des vorgeschlagenen gemeinsamen europäischen Gesundheitsdatenraums ist die Verbesserung des Zugangs und der Qualität der Gesundheitsversorgung, die Förderung der wissenschaftlichen Forschung und die Unterstützung der zuständigen Behörden bei fundierten politischen Entscheidungen.
56. Angesichts der erheblichen Auswirkungen und des sensiblen Charakters des grenzübergreifenden Austauschs von Gesundheitsdaten möchte der EDSB hervorheben, dass für alle Verarbeitungsvorgänge, die sich aus der Schaffung eines gemeinsamen europäischen Gesundheitsdatenraums ergeben könnten, eine **robuste Rechtsgrundlage** in Einklang mit den EU-Datenschutzvorschriften erforderlich ist. In diesem Zusammenhang weist er außerdem darauf hin, dass eine **weitere Harmonisierung der für Gesundheitsdaten geltenden Datenschutzvorschriften** zwischen den Mitgliedstaaten erforderlich ist. Darüber hinaus könnte ein europäischer Verhaltenskodex über die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke ein wirksamer Wegbereiter für einen stärkeren grenzüberschreitenden Austausch von Gesundheitsdaten innerhalb der EU sein.
57. Der Austausch von Gesundheitsdaten könnte eine wichtige Rolle bei der Lösung wichtiger individueller und gesellschaftlicher Probleme spielen, wenn er durch geeignete Datenschutzgarantien flankiert wird. Der Ausbruch von COVID-19, der unser Leben auf beispiellose Weise beeinflusst, hat dies äußerst überzeugend vor Augen geführt. In diesem Zusammenhang erkennt der EDSB an, dass der Austausch von Daten wesentlich zur Bewältigung der aktuellen Krise und ihrer langfristigen Folgen beitragen und der EU bei der Vorbereitung auf mögliche künftige ähnlich geartete Krisen helfen könnte.
58. Der EDSB möchte auf die unlängst erlassenen Leitlinien des EDSA für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch verweisen, in denen die wesentlichen Anforderungen an den Datenschutz hervorgehoben und näher erläutert werden, insbesondere Rechtmäßigkeit, Transparenz, Erforderlichkeit und Verhältnismäßigkeit sowie Integrität und Vertraulichkeit. Personenbezogene Daten können nur für ganz bestimmte rechtmäßige Zwecke verarbeitet werden, wenn sie für diese Zwecke erforderlich sind, und dürfen nicht auf eine Art und Weise verwendet werden, die mit diesen Zwecken nicht vereinbar ist.

59. Und schließlich ersucht der EDSB die Kommission, Überlegungen über die mögliche Funktion des geplanten europäischen Gesundheitsdatenraums als Instrument für eine **bessere Vorsorge, Reaktion und Bewältigung künftiger Krisen im Gesundheitsbereich** zusammen mit der digitalen eHealth-Diensteinfrastruktur (eHDSI) und anderen einschlägigen Strukturen und Initiativen der EU anzustellen, wobei ihm die Grenzen der Zuständigkeit der Union im Gesundheitsbereich gemäß den Verträgen durchaus bewusst sind.

5. BESONDERE FRAGESTELLUNGEN

5.1. Governance-Rahmen für den Zugang und die Nutzung von Daten

60. Der EDSB teilt die Auffassung der Kommission, dass die Schaffung eines **Rechtsrahmens für die Governance** als Voraussetzung eine Priorität bei der Umsetzung der Datenstrategie und ihres Kernstücks – den gemeinsamen europäischen Datenräumen – ist. Dieser sollte die Rechtssicherheit und die Übereinstimmung mit anderen geltenden Rechtsrahmen gewährleisten, insbesondere für den Datenschutz, indem er darauf aufbaut und diese verstärkt.
61. Der EDSB erwartet, zu den künftigen Legislativvorschlägen wie z. B. dem geplanten Rechtsakt über Daten gemäß Artikel 42 der Verordnung 2018/1725 konsultiert zu werden. Unbeschadet seiner künftigen Stellungnahme(n) sollen mit der vorliegenden Stellungnahme zur Datenstrategie einige vorläufige Kommentare und Empfehlungen in Verbindung mit dem Governance-Rahmen abgegeben werden.
62. Je nach den Risiken, der Art, dem Umfang, dem Zusammenhang und den Zwecken der Verarbeitung könnte eine Art formale „**Sicherheitsüberprüfung**“ von Organisationen, die Zugang zu den gemeinsamen europäischen Datenräumen beantragen, gerechtfertigt sein, beispielsweise in Form eines Clearinghouse. Darüber hinaus sollten Organisationen, die an der Zusammenführung von Daten beteiligt sind oder Vereinbarungen weitergeben, bestimmte gemeinsame Standards einhalten, und zwar nicht nur im Hinblick auf Interoperabilität, sondern auch darauf, die Rechtmäßigkeit der Verarbeitung und die Förderung der Rechte betroffener Personen (etwa über Vereinbarungen über gemeinsam für die Verarbeitung Verantwortliche gemäß Artikel 26 der DSGVO) zu gewährleisten.
63. Anschließend sollte der Governance-Rahmen im Hinblick auf die Rechenschaftspflicht des Verantwortlichen Anforderungen an die **Rückverfolgbarkeit der Daten** umfassen. Dies ist für die gemeinsamen europäischen Datenräume, bei denen Daten aus verschiedenen Mitgliedstaaten und aus unterschiedlichen Quellen sowohl öffentlicher als auch privater Natur kombiniert werden, besonders wichtig.
64. Abschließend hebt der EDSB hervor, dass die Zuständigkeiten der **unabhängigen Aufsichtsbehörden für den Datenschutz** im Zusammenhang mit künftigen Governance-Mechanismen genau beachtet werden müssen. Außerdem wird es für die Umsetzung der Strategie, die zu einer verstärkten Nutzung von Daten führen wird, erforderlich sein, die Ressourcen für Datenschutz-Aufsichtsbehörden und andere öffentliche Aufsichtsstellen erheblich aufzustocken, insbesondere im Hinblick auf technisches Know-how und Fähigkeiten. Die Zusammenarbeit und gemeinsame Untersuchungen zwischen allen einschlägigen öffentlichen Aufsichtsbehörden, einschließlich von Datenschutz-Aufsichtsbehörden, sollten gefördert werden.

5.2. Datenschutzgerechte Technologien (*privacy preserving technologies*)

65. Der EDSB begrüßt, dass in der Strategie datenschutzgerechte Technologien (*privacy preserving technologies*) aufgezeigt werden, die „für die nächsten Phasen der Datenwirtschaft von entscheidender Bedeutung“ sind. Im gleichen Sinne verweist der EDSB auf das Potenzial von **Technologien zum Schutz der Privatsphäre** (*privacy enhancing technologies*, PET) als Voraussetzung für die gemeinsame Nutzung von Daten, die sowohl datenschutzfreundlich als auch sozial tragfähig sind.
66. Es gibt eine Reihe vielversprechender technologischer Lösungen, etwa die Nutzung von **synthetischen Daten**, die u. a. den Zugang zu Trainingsdaten für maschinelles Lernen erleichtern. Zwar herrscht nach wie vor Unsicherheit in Bezug auf die mögliche Realisierbarkeit und die Effizienz solcher Lösungen zur Eindämmung von Datenschutzrisiken, und es gibt noch offene Fragen dazu, doch ersucht der EDSB die Kommission, in weitere Forschung und Tests zu investieren.
67. Darüber hinaus unterstreicht der EDSB zur Optimierung der Vorteile der verschiedenen datenschutzgerechten Technologien, wie wichtig ihre **Standardisierung und Interoperabilität** sind. Hierzu begrüßt er die Zusage in der Strategie, die Entwicklung gemeinsamer europäischer Standards und Anforderungen an die Vergabe öffentlicher Aufträge für Datenverarbeitungsdienste zu erleichtern, und ersucht die Kommission, dieses Ziel weiter zu verfolgen.

5.3. „Datenaltruismus“

68. In der Strategie verpflichtet sich die Kommission zur „Erleichterung für Einzelpersonen, im Einklang mit der Datenschutz-Grundverordnung die Nutzung der von ihnen erzeugten Daten zum Wohl der Allgemeinheit zu gestatten, wenn sie dies wünschen („Datenaltruismus“)“. In Bezug auf das Konzept des „Datenaltruismus“, der auch als „Datenspende“ bezeichnet wird, ist der EDSB der Auffassung, dass der Mehrwert dieses Begriffs nicht ganz klar ist, wenn man berücksichtigt, dass ein solcher „Datenaltruismus“ darauf angewiesen ist, dass die betroffene Person ihre Einwilligung erteilt und dass die DSGVO bereits Grundsätze und Vorschriften für die Einwilligung vorsieht. Daher ersucht der EDSB die Kommission, den Umfang, einschließlich möglicher Zwecke, eines solchen „Datenaltruismus“ genauer zu definieren und festzulegen (beispielsweise Datenaltruismus für die wissenschaftliche Forschung im Gesundheitswesen).
69. Der EDSB möchte außerdem erneut bekräftigen, dass die betroffene Einzelperson in gar keinem Fall auf das Grundrecht auf Schutz personenbezogener Daten „verzichten“ kann, sei es durch eine „Spende“ oder durch den „Verkauf“ personenbezogener Daten. Der Verantwortliche unterliegt weiterhin uneingeschränkt den Vorschriften und Grundsätzen für personenbezogene Daten, auch wenn er Daten verarbeitet, die „gespendet“ wurden, d. h. wenn die betroffene Person ihre Einwilligung in die Verarbeitung erteilt hat.

5.4. Qualifikationen und Datenkompetenz

70. Der EDSB begrüßt die Zusage der Kommission, **in Qualifikationen und allgemeine Datenkompetenz zu investieren**. In diesem Zusammenhang möchte er hervorheben, dass Datenschutzkompetenz für Einzelpersonen wichtig ist, damit sie ihre Rechte im Allgemeinen kennen und fundierte Entscheidungen darüber treffen können, ob sie bestimmte Arten der Nutzung ihrer Daten gestatten oder nicht. Dies gilt vor allem für Jugendliche, die zu den aktivsten Nutzern digitaler Dienste gehören.

71. Sensibilisierung für den Datenschutz ist eine *conditio sine qua non*, damit gewährleistet werden kann, dass die Einwilligung von Einzelpersonen auch einen Sinn ergibt. Außerdem würden Personen, die sich der Bedeutung des Datenschutzes bewusst sind, ihre Rechte als betroffene Personen besser nutzen und damit alle Akteure im Datenökosystem dazu veranlassen, dem Geist und Buchstaben der DSGVO zu entsprechen.

5.5. Internationaler Datenaustausch

72. Der EDSB begrüßt die klare Zusage, dass alle Unternehmen und sonstigen Organisationen, die in Verbindung mit der datengesteuerten Wirtschaft in Europa Waren verkaufen oder Dienstleistungen erbringen, die europäische Rechtsvorschriften achten müssen, und dies sollte nicht durch Forderungen von Ländern außerhalb von Europa gefährdet werden.
73. Der EDSB möchte daran erinnern, dass alle **Übermittlungen personenbezogener Daten an Drittländer oder internationale Organisationen** in Einklang mit Kapitel V und den übrigen einschlägigen Bestimmungen der DSGVO bzw. im Fall von Organen und Einrichtungen der Union mit der Verordnung (EU) 2018/1725 erfolgen müssen. Diese Verpflichtung gilt uneingeschränkt für **Cloud-Computing**, wie aus den Leitlinien des EDSB zur Nutzung von Cloud-Computing-Diensten durch die Organe und Einrichtungen der EU³⁴ und der Gründung des Haager Forums – des ersten EU-Kundenrates der Software- und Cloud-Anbieter³⁵ – hervorgeht
74. Der EDSB teilt voll und ganz die Auffassung der Kommission, dass die internationale Zusammenarbeit auf einem Konzept beruhen muss, das die Grundrechte der EU fördert, einschließlich des Schutzes der Privatsphäre und personenbezogener Daten. Auch bei seiner Zusammenarbeit mit anderen Partnerorganisationen und innerhalb internationaler Foren wie *Global Privacy Assembly* lässt sich der EDSB von diesem Konzept leiten.

6. SCHLUSSFOLGERUNGEN

75. Der EDSB versteht die zunehmende Bedeutung von Daten für die Wirtschaft und Gesellschaft und unterstützt die Bestrebungen, die Europäische Union „die EU in die Lage [zu] versetzen [...], zur attraktivsten, sichersten und dynamischsten datenagilen Wirtschaft der Welt zu werden.“ Zugleich erinnert er daran, dass „*big data comes with big responsibility*“ (große Datenmengen mit einer großen Verantwortung verbunden sind), und daher müssen geeignete Datenschutzgarantien vorhanden sein und effektiv angewandt werden.
76. Der EDSB beglückwünscht die Kommission zu ihrer Zusage, dafür zu sorgen, dass europäische Grundrechte und grundlegende Werte, einschließlich des Rechts auf Schutz personenbezogener Daten, das Fundament aller Aspekte der Datenstrategie und ihrer Umsetzung bilden. Er würdigt insbesondere die Zusicherung, dass die Strategie in voller Übereinstimmung mit der Datenschutz-Grundverordnung ausgearbeitet werden soll, die nicht zuletzt aufgrund ihres in technologischer Hinsicht neutralen Ansatzes eine solide Grundlage bildet.
77. Heute ist das vorherrschende Geschäftsmodell der digitalen Wirtschaft von einer beispiellosen Konzentration von Daten bei einer Handvoll mächtiger Akteure außerhalb der EU sowie einer allgegenwärtigen Nachverfolgung im großen Maßstab geprägt. Der EDSB ist der festen Überzeugung, dass eines der wichtigsten Ziele der Datenstrategie der Nachweis der Tragfähigkeit und Nachhaltigkeit **eines alternativen Datenwirtschaftsmodells** sein sollte – offen, fair und demokratisch. Daher sollten die geplanten gemeinsamen europäischen Datenräume im Hinblick auf Transparenz, effektive Rechenschaftspflicht und ein ausgewogenes Verhältnis zwischen den Interessen betroffener Personen und dem gemeinsamen Interesse der Gesellschaft insgesamt eine Vorbildfunktion übernehmen.

78. Der EDSB erwartet, zu legislativen Folgemaßnahmen zur Datenstrategie, die sich auf den Datenschutz auswirken, wie vorstehend dargelegt, gemäß Artikel 42 der Verordnung 2018/1725 konsultiert zu werden, und steht der Kommission, dem Rat und dem Europäischen Parlament weiterhin zur Verfügung, um sie bei den nächsten Schritten der Umsetzung der Europäischen Datenstrategie sowohl hinsichtlich des rechtlichen Rahmens als auch praktischer Aspekte weiter zu beraten. Die Anmerkungen in dieser Stellungnahme lassen weitere Anmerkungen in Zukunft zu besonderen Themen und/oder dann, wenn weitere Informationen vorliegen, unberührt.

Brüssel, 16. Juni 2020

Wojciech Rafał WIEWIÓROWSKI

Anmerkungen

¹ ABl. L 119 vom 4.5.2016, S. 1.

² ABl. L 295 vom 21.11.2018, S. 39.

³ ABl. L 119 vom 4.5.2016, S. 89.

⁴ COM (2020) 66 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de

⁵ COM(2020) 67 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_de

⁶ COM (2020) 65 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de

⁷ https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

⁸ https://edps.europa.eu/sites/edp/files/publication/2018-0246_psi_directive_opinion_en_de.pdf

⁹ https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf

¹⁰ Weitere Informationen sind abrufbar unter: https://edps.europa.eu/data-protection/our-work/subjects/covid-19_de

¹¹ COM (2017) 10 final, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)

¹² Siehe Artikel 29-Datenschutzgruppe, Leitlinien zur Transparenz gemäß Verordnung (EU) 2016/679 (wp260rev.01) https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP260_LeitlinienFuerDieTransparenz.html

¹³ https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf

¹⁴ <https://privacyinternational.org/legal-action/challenge-hidden-data-ecosystem>

¹⁵ Vgl. Erwägungsgrund 4 DSGVO.

¹⁶ Siehe Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA):

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

¹⁷ Diesbezüglich ist grundsätzlich in Artikel 12 Absatz 1 der Richtlinie über offene Daten vorbehaltlich der beschränkten Ausnahme gemäß Artikel 12 Absatz 2 geregelt wie folgt: „Die Weiterverwendung von Dokumenten steht allen potenziellen Marktteilnehmern offen, selbst wenn auf diesen Dokumenten beruhende Mehrwertprodukte bereits von einem oder mehreren Marktteilnehmern genutzt werden. Verträge oder sonstige Vereinbarungen zwischen den öffentlichen Stellen, die im Besitz der Dokumente sind, und Dritten dürfen keine ausschließlichen Rechte gewähren.“

¹⁸ Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 345 vom 31.12.2003, S. 90).

¹⁹ 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. 56-83).

²⁰ EDSB Stellungnahme 5/2018, Stellungnahme zu dem Vorschlag für eine Neufassung der Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI), abrufbar unter:

https://edps.europa.eu/sites/edp/files/publication/2018-0246_psi_directive_opinion_en_de.pdf

²¹ Siehe beispielsweise die Datenschutz-Folgenabschätzung für intelligente Stromnetze und intelligente Verbrauchsmessung, abrufbar unter: <https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment> Letztere könnte auch durchgeführt werden, um bei der Suche nach Energiesparlösungen der Weiterverwendung von Daten Rechnung zu tragen.

²² Siehe Seite 8 der Strategie unter Hinweis auf „die Verwendung aggregierter und anonymisierter Daten aus den sozialen Medien“.

²³ Siehe Rechtssache C-582/14 Patrick Breyer gegen Bundesrepublik Deutschland, ECLI:EU:C:2016:779

²⁴ Siehe Artikel-29-Arbeitsgruppe, Stellungnahme 05/2014 zu Anonymisierungstechniken:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

²⁵ <https://www.ema.europa.eu/en/human-regulatory/marketing-authorisation/clinical-data-publication/support-industry-clinical-data-publication>

²⁶ <https://ec.europa.eu/eurostat/web/european-statistical-system/reuse-ess-statistics>

²⁷ Siehe Erwägungsgrund 5 der Verordnung (EU) 2018/1725.

²⁸ Siehe Gemeinsame Stellungnahme des EDSA und des EDSB 1/2019 zur Verarbeitung von Patientendaten und zur Rolle der Europäischen Kommission in der digitalen eHealth-Dienstinfrastruktur (eHDSI):

https://edps.europa.eu/sites/edp/files/publication/19-07-15_edpb_edps_joint_opinion_ehealth_de.pdf

²⁹ Siehe Seite 15 der Datenstrategie.

³⁰ https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

³¹ https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_de

³² Mehr dazu ist der Vorläufigen Stellungnahme des EDSB zum Datenschutz und zur wissenschaftlichen Forschung zu entnehmen.

³³ Siehe beispielsweise das Gutachten der deutschen Datenethikkommission aus dem Jahr 2019, Empfehlungen 16-23.

³⁴ https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_de.pdf

³⁵ Für weitere Informationen siehe: https://edps.europa.eu/press-publications/press-news/press-releases/2019/edps-investigation-it-contracts-stronger_en