



**Gemeinsame
Stellungnahme 03/2021
des EDSA und des EDSB
zum Vorschlag für eine
Verordnung des
Europäischen Parlaments
und des Rates über
europäische Daten-
Governance
(Daten-Governance-Gesetz)**

Version 1.1

Versionsverlauf

Version 1.1	9. Juni 2021	Geringfügige redaktionelle Änderungen
Version 1.0	10. März 2021	Verabschiedung der gemeinsamen Stellungnahme

INHALTSVERZEICHNIS

1	HINTERGRUND	5
2	ANWENDUNGSBEREICH DER STELLUNGNAHME	6
3	BEWERTUNG	8
3.1	Allgemeine Bemerkungen.....	8
3.2	Allgemeine Aspekte zum Verhältnis des Vorschlags zum Unionsrecht im Bereich des Schutzes personenbezogener Daten.....	9
3.3	Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen 20	
3.3.1	Verhältnis des Vorschlags zur Richtlinie über offene Daten und zur DSGVO	20
3.3.2	Artikel 5: Bedingungen für die Weiterverwendung von Daten durch öffentliche Stellen 23	
3.3.3	Artikel 5 Absatz 11: Weiterverwendung „hochsensibler“ nicht personenbezogener Daten 29	
3.3.4	Artikel 6: Gebühren für die Weiterverwendung von Daten	30
3.3.5	Governance und institutionelle Aspekte: Artikel 7 (Zuständige Stellen). Artikel 8 (Zentrale Informationsstelle)	31
3.4	Anforderungen an Anbieter von Diensten für die gemeinsame Datennutzung.....	33
3.4.1	Datenmittler im Sinne des Artikels 9 Absatz 1 Buchstabe b: Vermittlungsdienste zwischen betroffenen Personen und potenziellen Datennutzern	37
3.4.2	Datenmittler nach Artikel 9 Absatz 1 Buchstabe c: „Datengenossenschaften“	39
3.4.3	Artikel 10: Anmeldeverordnung – allgemeine Voraussetzungen für die Zulassung zur Registrierung – Inhalt der Anmeldung; Ergebnis (und Fristen) der Anmeldung. Artikel 11: Bedingungen für die Erbringung von Diensten für die gemeinsame Datennutzung	40
3.4.4	Artikel 12 und 13: Zuständige Behörden und Überwachung der Einhaltung (der Artikel 10 und 11).....	44
3.5	Datenaltruismus.....	46
3.5.1	Zusammenspiel zwischen Datenaltruismus und Einwilligung nach der DSGVO	46
3.5.2	Artikel 16 und 17: Eintragungsregelung – allgemeine Eintragungsanforderungen – Inhalt der Eintragung; Ergebnis (und Fristen) der Eintragung	50
3.5.3	Artikel 18 und 19: Transparenzanforderungen und „besondere Anforderungen zum Schutz der Rechte und Interessen betroffener Personen und juristischer Personen im Hinblick auf ihre Daten“	52
3.5.4	Artikel 20 und 21: für die Eintragung zuständige Behörden und Überwachung der Einhaltung	54
3.5.5	Artikel 22: Europäisches Einwilligungsformular für Datenaltruismus	55

3.6	Internationale Datenübermittlungen: Artikel 5 Absätze 9 bis 13; Erwägungsgründe 17 und 19; Artikel 30	55
3.7	Horizontale Bestimmungen zu institutionellen Rahmenbedingungen; Beschwerden; Expertengruppe des Europäischen Dateninnovationsrats; delegierte Rechtsakte; Sanktionen, Bewertung und Überprüfung, Änderungen der Verordnung über ein einheitliches digitales Zugangstor, Übergangsmaßnahmen und Inkrafttreten	57
3.7.1	Artikel 23: Anforderungen an zuständige Behörden	57
3.7.2	Artikel 24: Beschwerden; Artikel 25: Recht auf wirksamen gerichtlichen Rechtsbehelf	58
3.7.3	Artikel 26 und 27: Zusammensetzung und Aufgaben der Expertengruppe des Europäischen Dateninnovationsrats	59
3.7.4	Artikel 31: anzuwendende Sanktionen bei Verstößen gegen die vorgeschlagene Verordnung	60
3.7.5	Artikel 33: Änderung der Verordnung (EU) 2018/1724	61

Der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte –

gestützt auf Artikel 42 Absatz 2 der 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/EG (im Folgenden „EU-DSVO“),

gestützt auf das Abkommen über den Europäischen Wirtschaftsraum, insbesondere auf Anhang XI und Protokoll 37 in der durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 geänderten Fassung –

HABEN FOLGENDE GEMEINSAME STELLUNGNAHME VERABSCHIEDET:

1 HINTERGRUND

1. Der Vorschlag für ein Daten-Governance-Gesetz (im Folgenden „Vorschlag“) wurde gemäß der Mitteilung „Eine europäische Datenstrategie“¹ (im Folgenden „Datenstrategie“) eingebracht.
2. Der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDSB) weisen darauf hin, dass für die Datenstrategie laut Kommission Folgendes gilt: *„Die Bürgerinnen und Bürger werden sich nur dann auf datengetriebene Innovationen einlassen und ihnen Vertrauen entgegenbringen, wenn sie zuversichtlich sind, dass bei jeder Weitergabe personenbezogener Daten in der EU die strengen EU-Datenschutzvorschriften strikt eingehalten werden.“*²
3. Wie in der Begründung ausgeführt, zielt der Vorschlag darauf ab, *„die Verfügbarkeit von Daten zur Nutzung zu fördern, indem das Vertrauen in die Datenmittler erhöht wird und die Mechanismen für die gemeinsame Datennutzung in der gesamten EU gestärkt werden. Das Instrument bezieht sich auf Folgendes:*
 - *Bereitstellung von Daten des öffentlichen Sektors zur Weiterverwendung in Fällen, in denen diese Daten den Rechten anderer unterliegen,*
 - *gemeinsame Datennutzung durch Unternehmen gegen Entgelt in jedweder Form,*
 - *Ermöglichung der Nutzung personenbezogener Daten mithilfe eines ‚Mittlers für die gemeinsame Nutzung personenbezogener Daten‘, der Einzelpersonen bei der Ausübung ihrer Rechte gemäß der Datenschutz-Grundverordnung (DSGVO) unterstützen soll,*

¹ Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie, COM(2020) 66 final vom 19.2.2020.

² Eine europäische Datenstrategie, Einleitung, Seite 1.

– Ermöglichung der Nutzung von Daten aus altruistischen Gründen.“³

4. Bei der Vorlage des Vorschlags hat die Kommission insbesondere Folgendes berücksichtigt: *„Mit der neuen Verordnung wird ein Rahmen für eine verantwortungsvolle Governance der gemeinsamen europäischen Datenräume geschaffen und dafür gesorgt, dass Dateninhaber ihre Daten freiwillig zur Verfügung stellen können. Sie wird die im Rahmen der Richtlinie über offene Daten noch zu erlassenden Vorschriften über hochwertige Datensätze ergänzen, die EU-weit den kostenlosen Zugang zu bestimmten Datensätzen in maschinenlesbarem Format und über genormte Anwendungsprogrammierschnittstellen (API) regeln sollen.“*⁴
5. In der Datenstrategie wird ferner Folgendes hervorgehoben: *„Die Verfügbarkeit von Daten ist eine wesentliche Voraussetzung für das Trainieren von Systemen der künstlichen Intelligenz. Dabei schreiten die Produkte und Dienste rasch von der Mustererkennung und Erkenntnisgenerierung zu ausgefeilteren Vorhersagetechniken voran und ermöglichen somit bessere Entscheidungen.“*⁵
6. Wie in der Begründung des Vorschlags anerkannt wird, *„ist das Zusammenspiel mit den Rechtsvorschriften über personenbezogene Daten besonders wichtig. Mit der Datenschutz-Grundverordnung (DSGVO) und der e-Datenschutzrichtlinie hat die EU einen soliden und vertrauenswürdigen Rechtsrahmen für den Schutz personenbezogener Daten und einen weltweiten Standard geschaffen.“*⁶
7. Der EDSA und der EDSB weisen auch darauf hin, dass der Vorschlag, wie es in der Begründung heißt, darauf abzielt, *„die gemeinsame Datennutzung zu erleichtern, u. a. durch die Stärkung des Vertrauens in die Mittler für die gemeinsame Datennutzung, die in den verschiedenen Datenräumen eingesetzt werden sollen. Er zielt nicht darauf ab, wesentliche Rechte auf den Zugang zu Daten und deren Nutzung zu gewähren, zu ändern oder zu beseitigen. Es ist geplant, diese Art von Maßnahmen in einen möglichen Rechtsakt über Daten (2021) aufzunehmen.“*⁷ Zum Zeitpunkt der Abfassung dieser gemeinsamen Stellungnahme liegen die Ziele und der Inhalt eines solchen Rechtsakts über Daten noch nicht vor.

2 ANWENDUNGSBEREICH DER STELLUNGNAHME

8. Am 25. November 2020 veröffentlichte die Kommission den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) (im Folgenden „Vorschlag“).
9. Am 25. November 2020 ersuchte die Kommission den EDSA und den EDSB auf der Grundlage des Artikels 42 Absatz 2 der Verordnung (EU) 2018/1725 (EU-DSVO) um eine gemeinsame Stellungnahme zu dem Vorschlag.

³ Begründung, Seite 1.

⁴ https://ec.europa.eu/commission/presscorner/detail/de/qanda_20_2103#European%20Data%20Spaces

⁵ Datenstrategie, Seiten 2 und 3.

⁶ Begründung, Seite 1.

⁷ Begründung, Seite 1.

10. **Der Vorschlag ist von besonderer Bedeutung für den Schutz der Rechte und Freiheiten des Einzelnen bei der Verarbeitung personenbezogener Daten. Der Anwendungsbereich dieser Stellungnahme beschränkt sich auf die Punkte des Vorschlags, die sich auf den Schutz personenbezogener Daten beziehen. Dies ist, wie festgestellt wurde, ein zentraler – wenn nicht sogar der wichtigste – Aspekt des Vorschlags.**
11. In diesem Zusammenhang weisen der EDSA und der EDSB auf folgenden Satz in Erwägungsgrund 3 hin: „Daher bleiben folgende Rechtsvorschriften von dieser Verordnung unberührt: Verordnung (EU) 2016/679“.
12. Der EDSA und der EDSB sind der Auffassung, dass das zugrunde liegende Ziel, das Vertrauen in Bezug auf die Erleichterung der Datenverfügbarkeit und den Nutzen für die digitale Wirtschaft in der EU zu stärken, tatsächlich **auf der Notwendigkeit beruht, die Einhaltung und Anwendung des EU-Besitzstands im Bereich des Schutzes personenbezogener Daten sicherzustellen und aufrechtzuerhalten**. Das geltende EU-Recht in diesem Bereich, insbesondere die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO), ist als Vorbedingung zu betrachten, auf der weitere Legislativvorschläge aufbauen können, ohne dass dabei die einschlägigen bestehenden Bestimmungen berührt oder beeinträchtigt werden. Das gilt auch, wenn es um die Zuständigkeit der Aufsichtsbehörden und andere Governance-Aspekte geht.⁸
13. Nach Ansicht des EDSA und des EDSB ist es daher wichtig, dass **im verfügbaren Teil des Vorschlags Unstimmigkeiten und mögliche Widersprüche zur DSGVO unbedingt vermieden werden**. Dies ist nicht nur aus Gründen der Rechtssicherheit von Bedeutung, sondern auch, um zu vermeiden, dass der Vorschlag das Grundrecht auf Schutz personenbezogener Daten, wie es in Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und Artikel 8 der Charta der Grundrechte der Europäischen Union verankert ist, direkt oder indirekt gefährdet.
14. Der EDSA und der EDSB weisen in dieser gemeinsamen Stellungnahme insbesondere auf Unstimmigkeiten mit der Datenschutzgesetzgebung der EU (sowie mit anderen EU-Rechtsvorschriften, wie der Richtlinie über offene Daten) und auf Probleme hin, die durch das Inkrafttreten des vorliegenden Vorschlags, z. B. in Bezug auf die Rechtssicherheit, entstehen würden.
15. Wie in dieser gemeinsamen Stellungnahme im Einzelnen dargelegt, wirft der Vorschlag eine beträchtliche Zahl schwerwiegender, oft miteinander verbundener Bedenken im Zusammenhang mit der Wahrung des Grundrechts auf Schutz personenbezogener Daten auf. **Es ist nicht das Ziel dieser gemeinsamen Stellungnahme, eine erschöpfende Liste der von den gesetzgebenden Organen zu behandelnden Punkte zu erstellen, und auch nicht in jedem Fall alternative Vorschläge oder Formulierungsvorschläge zu unterbreiten**. Stattdessen **soll mit dieser gemeinsamen Stellungnahme**

⁸ Siehe Stellungnahme 3/2020 des EDSB zur europäischen Datenstrategie, Rn. 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.“

auf die wichtigsten kritischen Punkte des Vorschlags eingegangen werden. Gleichzeitig stehen der EDSA und der EDSB für weitere Klarstellungen und den Austausch mit der Kommission zur Verfügung.

16. Der EDSA und der EDSB sind sich zugleich bewusst, dass das Gesetzgebungsverfahren zu dem Vorschlag noch nicht abgeschlossen ist, und möchten besonders darauf hinweisen, dass sie **den beiden gesetzgebenden Organen zur Verfügung stehen, um während dieses Verfahrens weitere Ratschläge und Empfehlungen zu geben**, damit vor allem Folgendes gewährleistet ist: Rechtssicherheit für natürliche Personen, Wirtschaft und Staat, ein angemessener Schutz personenbezogener Daten für betroffene Personen im Einklang mit dem AEUV, der Charta der Grundrechte der EU und dem Besitzstand der Union im Bereich des Datenschutzes, ein nachhaltiges digitales Umfeld einschließlich der erforderlichen „Kontrolle und Gegenkontrolle“.
17. Wegen der möglichen wichtigen Verbindungen zu dem Vorschlag⁹ bezieht sich diese Aufforderung zur Einbeziehung der Datenschutzbehörden auch auf einen künftigen Vorschlag für einen europäischen Rechtsakt über Daten.

3 BEWERTUNG

3.1 Allgemeine Bemerkungen

18. Der EDSA und der EDSB erkennen das legitime Ziel an, die Verfügbarkeit von Daten zur Nutzung zu fördern, indem das Vertrauen in die Datenmittler erhöht wird und die Mechanismen für die gemeinsame Datennutzung in der gesamten EU gestärkt werden. Sie betonen gleichzeitig, dass der Schutz personenbezogener Daten ein wesentlicher und integraler Bestandteil des Vertrauens ist, das Einzelpersonen und Organisationen in die Entwicklung der digitalen Wirtschaft haben sollten. Der Vorschlag für eine Verordnung über europäische Daten-Governance (Daten-Governance-Gesetz) ist auch vor dem Hintergrund der zunehmenden Abhängigkeit der digitalen Wirtschaft von der Verarbeitung personenbezogener Daten und der Entwicklung neuer Technologien – beispielsweise zur Analyse großer Datensätze und künstliche Intelligenz – zu prüfen.
19. Der EDSA und der EDSB betonen, dass bei der DSGVO die Notwendigkeit zugrunde lag, das Grundrecht auf Datenschutz zu stärken, der Schwerpunkt des Vorschlags hingegen eindeutig auf der Freisetzung des wirtschaftlichen Potenzials der Weiterverwendung und der gemeinsamen Nutzung von Daten liegt. Demnach beabsichtigt der Vorschlag, „die Bedingungen für die gemeinsame Datennutzung im Binnenmarkt zu verbessern“, wie es in Erwägungsgrund 3 heißt. **Der EDSA und der EDSB weisen jedoch darauf hin, dass die im EU-Recht vorgesehene nötige Sicherstellung und Gewährleistung des**

⁹ In der Folgenabschätzung zu dem Vorschlag, SWD(2020) 295 final, heißt es auf Seite 6 (Fettdruck hinzugefügt): „Diese Initiative ist ein **erster Schritt des aus zwei Schritten bestehenden Ansatzes**, der in der europäischen Datenstrategie angekündigt wurde. **Die Initiative** wird sich mit der dringenden Notwendigkeit befassen, die gemeinsame Datennutzung durch einen angemessenen **Governance-Rahmen** zu erleichtern. **In einem zweiten Schritt** wird sich die Kommission damit befassen, **wer die Daten kontrolliert oder ‚besitzt‘, d. h. mit den materiellen Rechten in Bezug auf die Frage, wer unter welchen Umständen auf welche Daten zugreifen und sie nutzen kann.** **Die Einführung solcher Rechte** wird im Zusammenhang mit dem **Rechtsakt über Daten (2021)** untersucht werden. Unterschiedliche Interessen der Interessenträger und unterschiedliche Ansichten darüber, was in dieser Hinsicht fair ist, machen diese Fragen zu einem Gegenstand intensiver Debatten und würden mehr zeitlichen Spielraum rechtfertigen.“

Schutzniveaus personenbezogener Daten in dem Vorschlag – auch in Bezug auf die ihm beigefügte Folgenabschätzung – nicht gebührend berücksichtigt ist. Der EDSA und der EDSB sind der Ansicht, dass dieser politische Trend hin zu einem datengesteuerten wirtschaftlichen Rahmen ohne ausreichende Berücksichtigung der Aspekte des Schutzes personenbezogener Daten aus der Sicht der Grundrechte ernsthafte Bedenken aufwirft. In diesem Zusammenhang betonen der EDSA und der EDSB, dass jeder Vorschlag, einschließlich künftiger datenbezogener Initiativen, die Auswirkungen auf die Verarbeitung personenbezogener Daten haben können (wie z. B. der europäische Rechtsakt über Daten), die Einhaltung und Anwendung des EU-Besitzstands im Bereich des Schutzes personenbezogener Daten gewährleisten und aufrechterhalten muss.

20. **Der EDSA und der EDSB weisen darüber hinaus darauf hin, dass das Modell der Europäischen Union auf der durchgängigen Berücksichtigung ihrer Werte und Grundrechte bei den Entwicklungen ihrer Politik beruht und dass die DSGVO als Grundlage betrachtet werden muss, auf der ein europäisches Daten-Governance-Modell aufzubauen ist. Wie bereits in verschiedenen politischen Kontexten, z. B. bei der Bekämpfung der COVID-19-Pandemie, festgestellt wurde, ist der EU-Rechtsrahmen im Bereich des Schutzes personenbezogener Daten als treibende Kraft und nicht als Hindernis für die Entwicklung einer Datenwirtschaft zu betrachten, die den Werten und Grundsätzen der Union entspricht.**
21. Der EDSA und der EDSB sind zuversichtlich, dass die beiden gesetzgebenden Organe über diese gemeinsame Stellungnahme zu Erkenntnissen gelangen, die dafür sorgen, dass ein voll mit dem EU-Besitzstand im Bereich des Schutzes personenbezogener Daten im Einklang stehender Rechtsakt erlassen wird. Auch würde damit das Vertrauen gestärkt, indem das vom EU-Recht vorgesehene Schutzniveau unter der Aufsicht der nach Artikel 16 Absatz 2 AEUV eingerichteten unabhängigen Datenschutzbehörden aufrechterhalten wird.

3.2 Allgemeine Aspekte zum Verhältnis des Vorschlags zum Unionsrecht im Bereich des Schutzes personenbezogener Daten

22. Der Vorschlag enthält mehrere Verweise auf die Einhaltung der DSGVO, in der die Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr personenbezogener Daten festgelegt sind (siehe u. a. Erwägungsgrund 3 und Erwägungsgrund 28 des Vorschlags: *„Handelt es sich bei den Anbietern von Diensten für die gemeinsame Datennutzung um für die Verarbeitung Verantwortliche oder Auftragsverarbeiter im Sinne der Verordnung (EU) 2016/679, so sind sie an die Bestimmungen der genannten Verordnung gebunden.“*).
23. Der EDSA und der EDSB sind der Ansicht, dass angesichts des Anwendungsbereichs der Verarbeitung personenbezogener Daten, auf die in dem Vorschlag Bezug genommen wird, in Erwägungsgrund 3 auch ein Verweis auf die Richtlinie 2002/58/EG („e-Datenschutzrichtlinie“) aufgenommen werden sollte, da sie ebenfalls Teil des EU-Besitzstands im Bereich des Schutzes personenbezogener Daten ist, mit dem der Vorschlag im Einklang stehen muss.
24. Ganz allgemein sind der EDSA und der EDSB der Ansicht, dass **Sinn und Wortlaut des Vorschlags das Schutzniveau nicht untergraben dürfen und die vollständige Kohärenz mit allen Grundsätzen und Vorschriften** der DSGVO gewährleisten müssen, um die Grundrechte auf Schutz personenbezogener Daten nach Artikel 8 der Charta und Artikel 16 AEUV wirksam zu garantieren.

25. In Anbetracht der vorstehenden Ausführungen, auf die in den folgenden Absätzen dieser gemeinsamen Stellungnahme Bezug genommen wird, sind der EDSA und der EDSB der Ansicht, dass **der Vorschlag wesentliche Unstimmigkeiten mit der DSGVO** sowie mit anderem Unionsrecht¹⁰ aufweist, insbesondere in Bezug auf die folgenden fünf Aspekte:
- a) Gegenstand und Anwendungsbereich des Vorschlags,
 - b) im Vorschlag verwendete Begriffsbestimmungen/Terminologie,
 - c) Rechtsgrundlage für die Verarbeitung personenbezogener Daten,
 - d) verschwommene Unterscheidung zwischen (der Verarbeitung von) personenbezogenen und nicht personenbezogenen Daten (und unklares Verhältnis des Vorschlags zur Verordnung über den freien Verkehr nicht personenbezogener Daten),
 - e) Governance/Aufgaben und Befugnisse der nach dem Vorschlag zu benennenden zuständigen Stellen und Behörden unter Berücksichtigung der Aufgaben und Befugnisse der Datenschutzbehörden, die für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten sowie für die Erleichterung des freien Verkehrs personenbezogener Daten in der Union zuständig sind.

A. Gegenstand und Anwendungsbereich

26. In Artikel 1 Absatz 2 des Vorschlags heißt es: *„Die besonderen Bestimmungen anderer Rechtsakte der Union über den Zugang zu bestimmten Kategorien von Daten oder deren Weiterverwendung sowie die*
-

¹⁰ Obwohl sich diese Einschätzung nicht strikt auf die Verarbeitung personenbezogener Daten bezieht, sehen der EDSA und der EDSB auch die Möglichkeit zu Verwirrung und Unklarheit in der Frage, wie der Vorschlag zusammen mit der **Verordnung (EU) 2018/1807 über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union** zur Anwendung gelangt. In diesem Zusammenhang ist darauf hinzuweisen, dass die Begriffsbestimmungen für „Verarbeitung“, „Nutzer“, „beruflicher Nutzer“ und „Datenlokalisierungsaufgabe“ sowie andere Bestimmungen der Verordnung über nicht personenbezogene Daten (siehe z. B. Artikel 6, Übertragung von Daten) nicht mit den Begriffsbestimmungen und den anderen Bestimmungen des Vorschlags **übereinstimmen** oder sich überschneiden könnten. Außerdem ist im Hinblick auf die Weiterverwendung von Daten im Besitz öffentlicher Stellen, die aus Gründen der statistischen Geheimhaltung geschützt sind, darauf hinzuweisen, dass trotz des in Artikel 3 Absatz 3 des Vorschlags genannten Grundsatzes die in Artikel 5 Absätze 3 und 4 festgelegten Bedingungen für die Weiterverwendung nicht mit den auf EU-Ebene festgelegten sektorspezifischen Vorschriften für den Schutz vertraulicher Daten, die für statistische Zwecke verwendet werden, übereinstimmen (siehe die Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates vom 11. März 2009 über europäische Statistiken und zur Aufhebung der Verordnung (EG, Euratom) Nr. 1101/2008 des Europäischen Parlaments und des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften, der Verordnung (EG) Nr. 322/97 des Rates über die Gemeinschaftsstatistiken und des Beschlusses 89/382/EWG, Euratom des Rates zur Einsetzung eines Ausschusses für das Statistische Programm der Europäischen Gemeinschaften sowie die Verordnung (EU) Nr. 557/2013 der Kommission vom 17. Juni 2013 zur Durchführung der Verordnung (EG) Nr. 223/2009 des Europäischen Parlaments und des Rates über europäische Statistiken in Bezug auf den Zugang zu vertraulichen Daten für wissenschaftliche Zwecke und zur Aufhebung der Verordnung (EG) Nr. 831/2002 der Kommission).

Anforderungen in Bezug auf die Verarbeitung personenbezogener oder nicht personenbezogener Daten bleiben von dieser Verordnung unberührt.

Müssen öffentliche Stellen, Anbieter von Diensten für die gemeinsame Datennutzung oder eingetragene Einrichtungen, die Datenaltruismus-Dienste erbringen, aufgrund sektorspezifischer Unionsvorschriften bestimmte zusätzliche technische, administrative oder organisatorische Bestimmungen einhalten, etwa im Rahmen von Genehmigungs- oder Zertifizierungsverfahren, so finden auch diese Bestimmungen der sektorspezifischen Unionsvorschriften Anwendung.“

27. **Im Interesse der Klarheit empfehlen der EDSA und der EDSB, in Artikel 1 des Vorschlags eine Bestimmung aufzunehmen, die klar und eindeutig besagt, dass der Vorschlag das Schutzniveau für den Einzelnen in Bezug auf die Verarbeitung personenbezogener Daten nach den Bestimmungen des Unionsrechts und des nationalen Rechts unberührt lässt und in keiner Weise beeinträchtigt und dass der Vorschlag keine in den Datenschutzvorschriften festgelegten Pflichten und Rechte ändert. Dieser Zusatz würde für mehr Rechtssicherheit sorgen und gewährleisten, dass das Grundrecht auf Schutz personenbezogener Daten nicht untergraben wird.**
28. Diesbezüglich ist unklar, warum eine ähnliche Präzisierung in Artikel 9 Absatz 2 des Vorschlags enthalten ist, der sich auf Anbieter von Diensten für die gemeinsame Datennutzung bezieht¹¹, statt (mit den nötigen Abänderungen, d. h. mit Bezug auch auf öffentliche Stellen, Weiterverwender und datenaltruistische Organisationen) als horizontale Bestimmung in Artikel 1 des Vorschlags enthalten zu sein.

B. Die Begriffsbestimmungen des Vorschlags stimmen nicht mit den Begriffsbestimmungen und Schlüsselbegriffen der DSGVO überein und müssen daher geändert oder deutlicher formuliert werden.

29. Die in Artikel 2 Nummer 5 des Vorschlags enthaltene Begriffsbestimmung zum „Dateninhaber“ lautet: „eine juristische Person oder eine betroffene Person, die nach geltendem Unionsrecht oder geltendem nationalen Recht berechtigt ist, Zugang zu bestimmten, unter ihrer Kontrolle befindlichen personenbezogenen oder nicht personenbezogenen Daten zu gewähren oder diese Daten weiterzugeben“. Sie steht nicht im Einklang mit den übergreifenden Grundsätzen der DSGVO sowie mit dem Wortlaut der DSGVO.
30. In diesem Zusammenhang merken der EDSA und der EDSB an, dass sich Rechtsunsicherheiten aus der Tatsache ergeben können, dass in der DSGVO das Recht der betroffenen Person, Zugang zu ihren personenbezogenen Daten zu gewähren oder diese an Dritte weiterzugeben, nicht erwähnt wird. Auch findet kein entsprechendes Recht einer juristischen Person Erwähnung, wie sich dies aus der Definition des Begriffs „Dateninhaber“ offensichtlich ableiten ließe. Vielmehr bescheinigt die DSGVO jeder natürlichen Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten, was

¹¹ In Artikel 9 Absatz 2 heißt es: „Die Anwendung anderen Unionsrechts und nationalen Rechts auf die Anbieter von Diensten für die gemeinsame Datennutzung ebenso wie die Befugnisse der Aufsichtsbehörden zur Gewährleistung der Einhaltung des geltenden Rechts, insbesondere in Bezug auf den Schutz personenbezogener Daten und das Wettbewerbsrecht, bleiben von diesem Kapitel unberührt.“

sich auf eine umfassende Reihe von Vorschriften für die Verarbeitung personenbezogener Daten bezieht, die für jede Stelle verbindlich sind, die die Daten verarbeitet (Verantwortlicher/gemeinsam Verantwortlicher) oder die Daten im Auftrag des Verantwortlichen (Auftragsverarbeiter) verarbeitet.¹²

31. **Der EDSA und der EDSB sind diesbezüglich der Ansicht, dass es statt der Formulierung, eine juristische Person habe das Recht, Zugang zu personenbezogenen Daten zu gewähren oder diese weiterzugeben, angemessener wäre, darauf zu verweisen, ob und unter welchen Voraussetzungen eine bestimmte Verarbeitung personenbezogener Daten durchgeführt werden kann oder nicht.**
32. Der EDSA und der EDSB möchten klarstellen, dass sowohl der Zugang zu personenbezogenen Daten als auch der Austausch personenbezogener Daten eine Verarbeitung personenbezogener Daten im Sinne des Artikels 4 Nummer 2 DSGVO darstellen.
33. Nach der Datenschutzgesetzgebung ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn die betroffene Person (die identifizierte oder identifizierbare natürliche Person, auf die sich die personenbezogenen Daten beziehen) in die Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt hat oder wenn eine andere geeignete Rechtsgrundlage nach Artikel 6 DSGVO wirksam angewendet werden kann.
34. Die vorstehenden Erwägungen werden insbesondere unter Berücksichtigung des Artikels 8 der Charta vorgebracht: *„(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.“*
35. Der EDSA und der EDSB haben auch Bedenken hinsichtlich des Wortlauts von Erwägungsgrund 14 des Vorschlags (Unterstreichung hinzugefügt): *„Juristische und natürliche Personen sollten darauf vertrauen können, dass die Weiterverwendung von geschützten Daten bestimmter Kategorien, die sich im Besitz des öffentlichen Sektors befinden, in einer Art und Weise erfolgt, die ihre Rechte und Interessen wahrt.“* Gleiches gilt für Artikel 11 Nummer 6 in Bezug auf *„Garantien, die sicherstellen, dass Dateninhaber und Datennutzer im Insolvenzfall Zugang zu ihren Daten erhalten“*, sowie für Artikel 19 *„Besondere Anforderungen zum Schutz der Rechte und Interessen betroffener Personen und juristischer Personen im Hinblick auf ihre Daten“*, wo es in Artikel 19 Absatz 1 Buchstabe a heißt: *„die Zwecke von allgemeinem Interesse, für die sie [die im Register der anerkannten datenaltruistischen*

¹² Siehe auch die Erwägungsgründe 6 und 7 der DSGVO (Fettdruck hinzugefügt):

„(6) Rasche technologische Entwicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. Zunehmend machen auch natürliche Personen Informationen öffentlich weltweit zugänglich. Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert und dürfte den Verkehr personenbezogener Daten innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen noch weiter erleichtern, wobei ein **hohes Datenschutzniveau** zu gewährleisten ist.

(7) Diese Entwicklungen erfordern einen **soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes** in der Union, da es von großer Wichtigkeit ist, eine **Vertrauensbasis** zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. **Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen.** Natürliche Personen, Wirtschaft und Staat sollten **in rechtlicher und praktischer Hinsicht über mehr Sicherheit** verfügen.“

Organisationen eingetragenen Einrichtungen] die Verarbeitung ihrer Daten [der Dateninhaber] durch einen Datennutzer erlaubt“.

36. Der EDSA und der EDSB merken diesbezüglich an, dass die Rechte und Interessen der betroffenen Person in Bezug auf ihre personenbezogenen Daten einerseits und die Rechte und Interessen juristischer Personen in Bezug auf die sie betreffenden Informationen andererseits nicht von derselben Art sind (Letztere betreffen nicht die Menschenwürde oder das Recht auf Privatsphäre und Datenschutz, sondern vielmehr gewerbliche Schutzrechte wie Geschäftsgeheimnisse, Patente und Marken). Angesichts dieser Heterogenität wären die genannten Bestimmungen daher konzeptionell nicht „stichhaltig“. Darüber hinaus wären sie auch schwer anwendbar und würden zu Rechtsunsicherheiten führen. So würden sich beispielsweise im Insolvenzfall (auf den in Artikel 11 Nummer 6 Bezug genommen wird) die Garantien, die den Dateninhabern den Zugang zu nicht personenbezogenen Daten ermöglichen, in der Praxis erheblich von den Bedingungen und Beschränkungen für die kontinuierliche Verarbeitung personenbezogener Daten unterscheiden. Es handelt sich um unterschiedliche Fragen, die unterschiedliche Lösungen erfordern¹³, und wenn im Rahmen der Verpflichtung des Anbieters von Diensten für die gemeinsame Datennutzung, die Kontinuität der Erbringung seiner Dienste (einschließlich der gemeinsamen Nutzung personenbezogener Daten) zu gewährleisten, auf beides zugleich verwiesen wird, ist dies auf jeden Fall verwirrend, wenn nicht sogar eindeutig unvereinbar mit der DSGVO.
37. Die Begriffsbestimmung für „Datennutzer“¹⁴ in Artikel 2 Nummer 6 ist ebenfalls eine neue, mit dem Vorschlag eingeführte Begriffsbestimmung, bei der – im Falle personenbezogener Daten – unklar ist, welches Zusammenspiel sich daraus mit der Begriffsbestimmung für „Empfänger“¹⁵ in Artikel 4 Nummer 9 DSGVO ergibt. Wir merken in diesem Zusammenhang an, dass in Artikel 11 Nummer 1 des Vorschlags festgelegt ist, dass „der Anbieter ... die Daten, für die er Dienste erbringt, für keine anderen Zwecke verwenden [darf], als sie den Datennutzern zur Verfügung zu stellen“. Diese Bestimmung führt in Verbindung mit der Begriffsbestimmung für „Datennutzer“ zu Rechtsunsicherheit, da der Begriff „Empfänger“ in der DSGVO und der Begriff „Datennutzer“ im Vorschlag unterschiedlich definiert werden, was zu Schwierigkeiten bei der praktischen Anwendung führen würde. Außerdem könnte die Begriffsbestimmung in Artikel 2 Nummer 6 irreführend sein, wenn sie so ausgelegt wird, dass sie sich auf eine natürliche oder juristische Person bezieht, die berechtigt ist (das Recht hat?), personenbezogene Daten für kommerzielle und nichtkommerzielle Zwecke zu nutzen. Der Verweis auf

¹³ Im Insolvenzfall ist beispielsweise darauf zu achten, dass es dadurch zu einer Veränderung in der Verantwortlichkeit für die Datenverarbeitung kommt. Der neue Verantwortliche muss insbesondere festlegen, welche Daten verarbeitet werden können, die Zwecke ermitteln, für die die Daten ursprünglich eingeholt wurden, die rechtmäßige Grundlage für die gemeinsame Nutzung der Daten festlegen, die Einhaltung der Datenschutzgrundsätze, insbesondere von Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz, sicherstellen und die betroffenen Personen über Änderungen im Zusammenhang mit der Verarbeitung ihrer Daten informieren sowie berücksichtigen, dass die betroffenen Personen ihr Widerspruchsrecht ausüben können.

¹⁴ Nach Artikel 2 Nummer 6 des Vorschlags bezeichnet der Ausdruck „**Datennutzer**“ eine natürliche oder juristische Person, die rechtmäßig Zugang zu bestimmten Daten hat und berechtigt ist, diese Daten für kommerzielle oder nichtkommerzielle Zwecke zu nutzen“.

¹⁵ Nach der Begriffsbestimmung in Artikel 4 Nummer 9 DSGVO bezeichnet der Ausdruck „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht“.

und die Bedeutung einer solchen „Berechtigung“ (d. h. ihre Rechtsquelle und Wirkung) sind ebenfalls unklar.

38. Darüber hinaus ist das Zusammenspiel zwischen dem Begriff des Datennutzers als „natürliche oder juristische Person [die berechtigt ist, Daten für kommerzielle und nichtkommerzielle Zwecke zu nutzen]“ und den Begriffen „Verantwortlicher“, „gemeinsam Verantwortlicher“ oder „Auftragsverarbeiter“ nach der DSGVO ebenfalls unklar. Des Weiteren verweist der Vorschlag auf eine mögliche Qualifizierung der Anbieter von Diensten für die gemeinsame Datennutzung als Verantwortliche oder Auftragsverarbeiter sowie deren Pflichten nach der DSGVO¹⁶, sieht dies aber nicht für den Datennutzer oder für datenaltruistische Organisationen vor (obwohl Letztere nach der DSGVO ebenfalls Verantwortliche, gemeinsam Verantwortliche oder Auftragsverarbeiter sein können).
39. **Generell betonen der EDSA und der EDSB, dass in dem Vorschlag die Rollen der einzelnen „Akteure“ (Anbieter von Diensten für die gemeinsame Datennutzung, datenaltruistische Organisation, Datennutzer) in Bezug auf die Rechtsvorschriften zum Schutz personenbezogener Daten (als für die Verarbeitung Verantwortlicher, Auftragsverarbeiter oder gemeinsam für die Verarbeitung Verantwortlicher) definiert werden sollten, nicht nur, um Unklarheiten über die geltenden Verpflichtungen nach der DSGVO zu vermeiden, sondern auch, um die Lesbarkeit des verfügbaren Teils zu verbessern.**
40. Ähnliche Probleme, nämlich das **unklare Verhältnis zu den Begriffsbestimmungen und Vorschriften der DSGVO**, betreffen die Begriffsbestimmung für „gemeinsame Datennutzung“ in Artikel 2 Nummer 7 des Vorschlags (in der u. a. auf „eine gemeinschaftliche oder individuelle Nutzung der geteilten Daten“ verwiesen wird). Soweit es sich um personenbezogene Daten handelt, ist auch die gemeinsame Nutzung personenbezogener Daten (sowohl durch den Dateninhaber, die juristische Person, als auch durch einen Datennutzer) direkt oder über einen Vermittler auf jeden Fall verwirrend.
41. Ähnliche Bedenken – wie nachstehend näher ausgeführt – bestehen in Bezug auf den Begriff „Erlaubnis [der juristischen Personen zur Weiterverwendung von Daten]“, für den im Vorschlag jedoch keine Definition vorgesehen ist.
42. Die Begriffsbestimmung für „Metadaten“ in Artikel 2 Nummer 4 ist unter dem Gesichtspunkt des Schutzes personenbezogener Daten ebenfalls problematisch, denn sie bezieht sich auf „Daten, die in Bezug auf Tätigkeiten einer natürlichen oder juristischen Person zwecks Erbringung eines Dienstes für die gemeinsame Datennutzung erfasst werden; dazu gehören Datum, Uhrzeit und Geolokalisierungsdaten, Dauer der Tätigkeit sowie Verbindungen zu anderen natürlichen oder juristischen Personen, die von der den Dienst nutzenden Person hergestellt werden“. Solche Daten können personenbezogene Daten enthalten.
43. Wie in dieser gemeinsamen Stellungnahme weiter ausgeführt, kann der Vorschlag in Bezug auf Artikel 11 Nummer 2 so ausgelegt werden, dass er eine Rechtsgrundlage für die Verarbeitung von Metadaten schafft. In Artikel 11 des Vorschlags wird offenbar festgelegt, dass der Anbieter als Voraussetzung für die Erbringung des Dienstes für die gemeinsame Datennutzung die besagten

¹⁶ Siehe Erwägungsgrund 28: „Handelt es sich bei den Anbietern von Diensten für die gemeinsame Datennutzung um für die Verarbeitung Verantwortliche oder Auftragsverarbeiter im Sinne der Verordnung (EU) 2016/679, so sind sie an die Bestimmungen der genannten Verordnung gebunden.“

Metadaten „für die Entwicklung dieses Dienstes [für die gemeinsame Datennutzung]“ tatsächlich verwenden darf. Der verfügbare Teil enthält keinen Verweis darauf, dass sich der Anbieter von Diensten für die gemeinsame Datennutzung unter anderem auf eine geeignete Rechtsgrundlage für die Verarbeitung personenbezogener Daten nach Artikel 6 Absatz 1 DSGVO stützen muss.

44. **Da der Vorschlag, wie darin selbst ausdrücklich erwähnt, die DSGVO unberührt lässt, sind der EDSA und der EDSB generell der Ansicht, dass die in der DSGVO vorgesehenen Begriffsbestimmungen gelten und diese nicht implizit durch den Vorschlag geändert oder aufgehoben werden sollten. Die neuen Begriffsbestimmungen sollten, soweit sie sich auf die Verarbeitung personenbezogener Daten beziehen, nicht wie selbstverständlich „Vorschriften“ enthalten, die mit dem Sinn und dem Wortlaut der DSGVO unvereinbar sind.**
45. Diese Präzisierung ist gerade deshalb von Bedeutung, da sich die Unklarheiten und Rechtsunsicherheiten, die sich aus dem Vorschlag ergeben, häufen können, wenn mehr als eine unklare Definition in derselben Bestimmung enthalten ist (siehe z. B. Artikel 7 Absatz 2 Buchstabe c des Vorschlags, der sich auf die „Einholung der Einwilligung oder Erlaubnis zur Weiterverwendung für altruistische und andere Zwecke durch die Weiterverwender entsprechend den besonderen Festlegungen der Dateninhaber“ bezieht).
46. **In Anbetracht der obigen Ausführungen empfehlen der EDSA und der EDSB, den Vorschlag genauer zu formulieren und zu ändern, um sicherzustellen, dass – soweit personenbezogene Daten betroffen sind – keine Unstimmigkeiten mit den Begriffsbestimmungen und Konzepten der DSGVO bestehen.**

C. In dem Vorschlag sollte die anzuwendende Rechtsgrundlage in der DSGVO für die Verarbeitung personenbezogener Daten genauer angegeben werden, um Rechtsunsicherheiten zu vermeiden.

47. Der EDSA und der EDSB merken an, dass im Vorschlag in mehreren Bestimmungen auf die „Erlaubnis der Dateninhaber“ für die Verwendung von Daten Bezug genommen wird:
 - Artikel 5 Absatz 6: *„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“, wie in Erwägungsgrund 11 präzisiert: „Öffentliche Stellen sollten gegebenenfalls die Weiterverwendung von Daten auf der Grundlage der Einwilligung bzw. Erlaubnis der betroffenen natürlichen und juristischen Personen zur Weiterverwendung ihrer Daten mit geeigneten technischen Mitteln erleichtern.“*
 - Artikel 7 Absatz 2 Buchstabe c: *„gegebenenfalls Unterstützung der öffentlichen Stellen bei der Einholung der Einwilligung oder Erlaubnis zur Weiterverwendung für altruistische und andere Zwecke durch die Weiterverwender entsprechend den besonderen Festlegungen der Dateninhaber“*
 - Artikel 11 Nummer 11: *„stellt ein Anbieter Werkzeuge zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von juristischen Personen zur Verfügung gestellten Daten bereit“*
 - Artikel 19 Absatz 3: *„Stellt eine im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung Werkzeuge zur Einholung der Einwilligung betroffener Personen oder der Erlaubnis zur Verarbeitung der von juristischen Personen zur Verfügung gestellten Daten bereit“, wie*

in Erwägungsgrund 36 präzisiert: „Juristische Personen könnten die Verarbeitung ihrer nicht personenbezogenen Daten für eine Reihe von Zwecken erlauben, die zum Zeitpunkt der Erteilung der Erlaubnis noch nicht festgelegt waren.“

48. Der EDSA und der EDSB stellen in diesem Zusammenhang fest, dass es in den meisten Fällen unklar ist, ob sich die Erlaubnis auf die Weiterverwendung von personenbezogenen Daten oder nicht personenbezogenen Daten oder auf beides bezieht.
49. Der EDSA und der EDSB merken außerdem an, dass im Falle der Verarbeitung personenbezogener Daten **die im Vorschlag genannte „Erlaubnis“ nicht das in Artikel 6 Absatz 1 DSGVO festgelegte Erfordernis einer geeigneten Rechtsgrundlage für die rechtmäßige Verarbeitung personenbezogener Daten ersetzen kann.** Mit anderen Worten: Nach der DSGVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn und soweit mindestens eine der Rechtsgrundlagen nach Artikel 6 Absatz 1 DSGVO gegeben ist. Im Vorschlag sollte dieser Punkt deutlich formuliert werden, um jegliche Unklarheit zu vermeiden.
50. Tatsächlich ist sogar bei der Auslegung des Begriffs „Erlaubnis“ (die jedoch im verfügenden Teil des Vorschlags zu definieren ist) als „eine Entscheidung (eine geschäftliche Entscheidung) einer juristischen Person, die Verarbeitung personenbezogener Daten zu erlauben, wenn diese juristische Person eine Rechtsgrundlage für die Erlaubnis für diese Verarbeitung nach Artikel 6 Absatz 1 DSGVO hat“ darauf hinzuweisen, dass die wörtliche Auslegung einiger Bestimmungen des Vorschlags diese DSGVO-konforme Auslegung nicht zu unterstützen scheint, denn dort heißt es beispielsweise: „*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*“ (Artikel 5 Absatz 6 des Vorschlags).¹⁷ In diesen Fällen scheint die „Erlaubnis“ eine Alternative zu mindestens einer der in Artikel 6 DSGVO vorgesehenen Rechtsgrundlagen (Einwilligung der betroffenen Person) zu sein.
51. Erwägungsgrund 6 des Vorschlags führt ebenfalls zu Unklarheiten im Hinblick auf die geeignete Rechtsgrundlage für die Verarbeitung personenbezogener Daten, da darin auf die „allgemein“ bestehende Verpflichtung verwiesen wird, sich bei der Verarbeitung personenbezogener Daten auf eine Rechtsgrundlage nach Artikel 6 DSGVO zu stützen.¹⁸
52. Im Übrigen, wie in dieser Stellungnahme weiter ausgeführt, merken der EDSA und der EDSB an, dass **das Verhältnis zwischen den verschiedenen, im Rahmen des Vorschlags vorgesehen Szenarien und Artikel 6 Absatz 4 DSGVO geklärt werden muss**, um den Fall zu regeln, dass die Verarbeitung personenbezogener Daten für einen anderen Zweck als den, für den die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person beruht.

¹⁷ Siehe auch Artikel 7 Absatz 2 Buchstabe c, Artikel 11 Nummer 11 und Artikel 19 Absatz 3 des Vorschlags, auf die oben Bezug genommen wurde.

¹⁸ Konkret heißt es in Erwägungsgrund 6 des Vorschlags (Fettdruck hinzugefügt): „**Allgemein** sollte die Verarbeitung personenbezogener Daten stets auf einem der Rechtsgründe beruhen, die in Artikel 6 der Verordnung (EU) 2016/679 aufgeführt sind.“

53. **Dementsprechend und angesichts des Ziels und Inhalts des Vorschlags sind der EDSA und der EDSB der Ansicht, dass der Vorschlag nicht als Unionsrecht, das in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 DSGVO genannten Ziele darstellt, geltend gemacht werden kann, um eine Rechtsgrundlage für die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, zu bieten, wenn diese Verarbeitung nicht auf der Einwilligung der betroffenen Person im Sinne des Artikels 6 Absatz 4 DSGVO beruht.**
54. **Gleichfalls in Anbetracht der obigen Ausführungen empfehlen der EDSA und der EDSB, im verfügbaren Teil des Vorschlags festzulegen, dass bei personenbezogenen Daten die Verarbeitung dieser Daten stets auf einer geeigneten Rechtsgrundlage nach Artikel 6 DSGVO beruhen muss.**
55. Als Beispiel für eine mögliche Unstimmigkeit in Bezug auf die Rechtsgrundlage für die Verarbeitung personenbezogener Daten sei auf die Bestimmung in Artikel 11 Nummer 2 des Vorschlags hingewiesen, dass *„die Metadaten, die bei der Erbringung des Dienstes für die gemeinsame Datennutzung erfasst werden, ... [nur] für die Entwicklung dieses Dienstes verwendet werden“* dürfen. In diesem Zusammenhang erinnern wir daran, dass die im Vorschlag genannten Metadaten¹⁹ Informationen über eine identifizierte oder identifizierbare natürliche Person darstellen können und in diesem Fall im Einklang mit den Datenschutzvorschriften und insbesondere mit den Vorschriften der Rechtsgrundlage für die Verarbeitung verarbeitet werden müssen. Wie schon unter Randnummer 51 erwähnt, wird dieser wesentliche Aspekt in dem Vorschlag jedoch nicht berücksichtigt.
56. **Diesbezüglich teilen der EDSA und der EDSB die weitergehende Betrachtung, dass die genannte Bestimmung sowie die übrigen Bestimmungen des Vorschlags keine eigenständige Rechtsgrundlage für die Weiterverwendung personenbezogener Daten durch Datennutzer oder für Verarbeitungsvorgänge von Anbietern von Diensten für die gemeinsame Datennutzung oder von datenaltruistischen Organisationen darstellen, da sie nicht die Kriterien nach Artikel 6 Absatz 3 für eine Verarbeitung gemäß Artikel 6 Absatz 1 Buchstaben c und e²⁰ DSGVO erfüllen.**

¹⁹ Nach Artikel 2 Nummer 4 des Vorschlags bezeichnet der Ausdruck „Metadaten“ Daten, die in Bezug auf Tätigkeiten einer natürlichen oder juristischen Person zwecks Erbringung eines Dienstes für die gemeinsame Datennutzung erfasst werden; dazu gehören Datum, Uhrzeit und Geolokalisierungsdaten, Dauer der Tätigkeit sowie Verbindungen zu anderen natürlichen oder juristischen Personen, die von der den Dienst nutzenden Person hergestellt werden“.

²⁰ „(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch a) Unionsrecht oder b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt. Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige

D. Verschwommene Unterscheidung zwischen (der Verarbeitung von) personenbezogenen und nicht personenbezogenen Daten und unklares Verhältnis des Vorschlags zur Verordnung über den freien Verkehr nicht personenbezogener Daten

57. Der EDSA und der EDSB sind generell der Ansicht, dass ein besonders kritischer Punkt des Vorschlags, der den Schutz personenbezogener Daten betrifft und möglicherweise Ursache für die genannten Unvereinbarkeiten oder zumindest die Unklarheit des verfügenden Teils ist, in der verschwommenen Unterscheidung zwischen der Verarbeitung nicht personenbezogener Daten – wie sie für bestimmte Aspekte in der Verordnung (EU) 2018/1807 vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union²¹ („Verordnung über den freien Verkehr nicht personenbezogener Daten“) geregelt ist – und der Verarbeitung personenbezogener Daten besteht, wobei Letztere im Rahmen des datenschutzrechtlichen Besitzstands geregelt ist und sich an anderen Grundsätzen orientiert.
58. Diesbezüglich möchten der EDSA und der EDSB betonen, dass die Unterscheidung zwischen den Kategorien personenbezogene und nicht personenbezogene Daten in der Praxis schwer anzuwenden ist. In der Praxis ist nämlich bei einer Kombination aus nicht personenbezogenen Daten der Rückschluss auf personenbezogene Daten möglich bzw. können solche personenbezogenen Daten erzeugt werden, d. h. Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.²² Das ist insbesondere dann der Fall, wenn nicht personenbezogene Daten das Ergebnis der Anonymisierung personenbezogener Daten und somit von Informationen sind, die sich ursprünglich auf natürliche Personen bezogen. Darüber hinaus wird es in den Szenarien, die im Vorschlag hinsichtlich einer verstärkten Verfügbarkeit, Wiederverwendung und gemeinsamen Nutzung von Informationen vorgesehen sind, um „eine ‚Big Data‘-Mustererkennung oder maschinelles Lernen“²³ zu ermöglichen, umso schwieriger sein, die Anonymisierung sicherzustellen, je mehr nicht personenbezogene Daten mit anderen verfügbaren Informationen kombiniert werden, da damit das Risiko der erneuten Identifizierung von betroffenen Personen steigt. In Anbetracht dieses Szenarios sollten daher die Grundrechte der betroffenen Personen auf Privatsphäre und Datenschutz in den verschiedenen im Vorschlag vorgesehenen Kontexten in jedem Fall gewährleistet werden.
59. Gleichzeitig kann es Fälle von nicht personenbezogenen Daten geben, auf die die DSGVO nicht anwendbar ist und die sich aufgrund ihrer Quelle nicht auf natürliche Personen beziehen. Dies ist beispielsweise der Fall bei nicht personenbezogenen Daten von Vibrationssensoren in Industriemaschinen in Kombination mit anderen nicht personenbezogenen Daten, z. B. der Geolokalisierung der Maschine. Für solche nicht personenbezogenen Daten ist nicht das gleiche Maß an Schutzmaßnahmen erforderlich wie für nicht personenbezogene Daten, die das Ergebnis der

besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.“

²¹ Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (Text von Bedeutung für den EWR) (ABl. L 303 vom 28.11.2018, S. 59).

²² Siehe Stellungnahme 3/2020 des EDSB zur europäischen Datenstrategie, Rn. 30.

²³ Begründung, Seite 3.

Anonymisierung personenbezogener Daten sind, da nur Letztere (wie auch pseudonymisierte Daten) dem Risiko einer erneuten Identifizierung unterliegen können.

60. **Um Verwirrung darüber zu vermeiden, wie der Vorschlag „zusammen mit der DSGVO“ anzuwenden ist, empfehlen der EDSA und der EDSB eine Überarbeitung des Vorschlags, in der besser auf die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten sowie zwischen den verschiedenen Arten von nicht personenbezogenen Daten eingegangen wird.**
61. Ungeachtet der vom EDSB bereits geäußerten Bedenken in Bezug auf das Konzept gemischter Datensätze und auf personenbezogene und nicht personenbezogene Daten, die „untrennbar miteinander verbunden“ sind²⁴, erinnern der EDSA und der EDSB daher daran, dass nach Artikel 2 Absatz 2 der Verordnung über den freien Verkehr nicht personenbezogener Daten Folgendes gilt: *„Bei einem Datensatz, der aus personenbezogenen und nicht-personenbezogenen Daten besteht, gilt diese Verordnung für die nicht personenbezogenen Daten des Datensatzes. Sind personenbezogene und nicht-personenbezogene Daten in einem Datensatz untrennbar miteinander verbunden, berührt diese Verordnung nicht die Anwendung der Verordnung (EU) 2016/679.“* Folglich unterliegt ein gemischter Datensatz grundsätzlich den Pflichten der für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter sowie den Rechten der betroffenen Person, wie sie in der DSGVO festgelegt sind. Diese Überlegung ist im Kontext des Vorschlags besonders relevant, da Datensätze, die über einen Anbieter von Diensten für die gemeinsame Datennutzung oder eine datenaltruistische Organisation geteilt werden, in den meisten Fällen auch aus personenbezogenen Daten bestehen dürften. Es gibt neben personenbezogenen und nicht personenbezogenen Daten keine „dritte Kategorie“, d. h., ein solcher Datensatz gilt somit seinem Wesen nach und nach der „rechtlichen Regelung“ als personenbezogene Daten.²⁵
62. **Vor diesem Hintergrund weisen der EDSA und der EDSB auf das Risiko hin, dass mit dem Vorschlag ein paralleles Regelwerk entsteht, das weder mit der DSGVO noch mit der Verordnung über den freien Verkehr nicht personenbezogener Daten im Einklang steht und diese somit untergräbt und Schwierigkeiten bei der praktischen Anwendung verursacht.**

E. Governance/Aufgaben und Befugnisse der nach dem Vorschlag zu benennenden zuständigen Stellen und Behörden sowie Aufgaben und Befugnisse der Datenschutzbehörden

63. Der Vorschlag sieht vor, dass die Mitgliedstaaten zuständige Stellen benennen, die die öffentlichen Stellen bei der Gewährung des Zugangs zur Weiterverwendung von Daten unterstützen (Kapitel II des Vorschlags), und dass sie zuständige Behörden benennen, die die Einhaltung der Bestimmungen in

²⁴ Siehe die Kommentare des EDSB zu einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr nicht personenbezogener Daten in der Europäischen Union, veröffentlicht am 8. Juni 2018, abrufbar unter https://edps.europa.eu/sites/edp/files/publication/18-06-08-edps_formal_comments_freeflow_non_personal_data_de.pdf.

²⁵ Siehe auch 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, abrufbar unter:

<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52019DC0250>.

Bezug auf Dienste für die gemeinsame Nutzung von Daten und Datenaltruismus überwachen (Kapitel III und IV des Vorschlags).

64. Ergänzend sei angemerkt, dass der EDSA und der EDSB das Risiko befürchten, dass die nach dem Vorschlag benannten zuständigen Stellen und Behörden in die Zuständigkeiten und Aufgaben der unabhängigen Datenschutzbehörden eingreifen, da viele der Aufgaben der zuständigen Stellen und Behörden nach dem Vorschlag die Verarbeitung personenbezogener Daten betreffen. Daher könnte die Benennung von zuständigen Stellen/Behörden, die keine Datenschutzbehörden sind, die Sache für digitale Akteure und betroffene Personen sehr verwirrend machen und auch die Kohärenz in Bezug auf die Überwachung der Anwendung der Bestimmungen der DSGVO beeinträchtigen. Da die Benennung der zuständigen Stellen und Behörden im Ermessen der Mitgliedstaaten liegt, besteht möglicherweise auch das Risiko von Unstimmigkeiten und Unterschieden bei den Regulierungsansätzen in der Union.

3.3 Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen

3.3.1 Verhältnis des Vorschlags zur Richtlinie über offene Daten und zur DSGVO

65. Während es in der Begründung heißt, der „Vorschlag ergänzt die 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 (Richtlinie über offene Daten)“²⁶, heißt es in Erwägungsgrund 5 weiter: „Die Richtlinie (EU) 2019/1024 sowie sektorspezifische Vorschriften zielen darauf ab, dass der öffentliche Sektor die Zugänglichkeit der von ihm erzeugten Daten für die Verwendung und Weiterverwendung in größerem Umfang erleichtert. Dennoch werden in öffentlichen Datenbanken vorhandene Daten bestimmter Kategorien oft nicht einmal für Forschungszwecke oder innovative Tätigkeiten zur Verfügung gestellt (vertrauliche Geschäftsdaten, unter die Geheimhaltungspflicht fallende statistische Daten, durch die Rechte Dritter am geistigen Eigentum geschützte Daten, Geschäftsgeheimnisse und personenbezogene Daten, zu denen aufgrund bestimmter nationaler Vorschriften oder des Unionsrechts, wie der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680, kein Zugang gewährt werden darf). Zur Wahrung der Rechte Dritter an diesen sensiblen Daten müssen bestimmte verfahrenstechnische und rechtliche Hürden überwunden werden, bevor solche Daten zur Verfügung gestellt werden können. Die Überwindung dieser Hürden braucht in der Regel viel Zeit und Sachverstand, weshalb solche Daten bislang kaum genutzt werden. Zwar haben einige Mitgliedstaaten Strukturen und Verfahren geschaffen und mitunter Vorschriften erlassen, um die Weiterverwendung dieser Art von Daten zu erleichtern, doch gilt das nicht für die gesamte Union.“
66. Der EDSA und der EDSB stellen fest, dass trotz der oben genannten Präzisierungen die Verbindung zwischen dem Vorschlag und der „Richtlinie über offene Daten“ unklar zu sein scheint. Insbesondere könnte eine Rechtsunsicherheit in Bezug auf die erweiterte Weiterverwendung von Informationen des öffentlichen Sektors bestehen, die nach Artikel 3 (Datenkategorien) des Vorschlags für folgende Daten gelten würde:

²⁶ ABl. L 172 vom 26.6.2019, S. 56.

„Daten, die sich im Besitz öffentlicher Stellen befinden und aus folgenden Gründen geschützt sind:

a) geschäftliche Geheimhaltung,

b) statistische Geheimhaltung,

c) Schutz geistigen Eigentums Dritter,

d) Schutz personenbezogener Daten.“

67. In der Begründung des Vorschlags²⁷ werden der Anwendungsbereich einer solchen erweiterten Weiterverwendung und das Zusammenspiel des Vorschlags mit der Richtlinie über offene Daten nicht ausreichend geklärt. Darüber hinaus werden (zur „*Achtung der Rechte anderer*“, was im Hinblick auf den Schutz personenbezogener Daten unangemessen ist) Gründe *„des Schutzes personenbezogener Daten, aber auch des Schutzes der Rechte des geistigen Eigentums und des Geschäftsgeheimnisses“* miteinander vermengt.

68. Es ließe sich argumentieren, dass die Formulierung *„Daten, die sich im Besitz öffentlicher Stellen befinden und aus folgenden Gründen geschützt sind“*, nämlich unter anderem zum *„Schutz personenbezogener Daten“* (Artikel 3 Absatz 1 Buchstabe d), einerseits

– bedauerlich ist, da sie die Vorstellung nahelegt, die Datenschutzverordnung würde den freien Verkehr personenbezogener Daten *behindern*, anstatt die Regeln für den freien Verkehr personenbezogener Daten unter Wahrung der Rechte und Interessen der betroffenen Personen festzulegen, *und andererseits*

– teilweise unzutreffend ist, da die Richtlinie über offene Daten, anstatt personenbezogene Daten aus ihrem Anwendungsbereich auszuschließen²⁸, in Artikel 1 Absatz 2 Buchstabe h vorsieht, dass [die Richtlinie über offene Daten nicht gilt für] *„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*

²⁷ Siehe Seite 7: *„Kapitel II schafft einen Mechanismus für die **Weiterverwendung bestimmter Kategorien geschützter Daten des öffentlichen Sektors, die der Achtung der Rechte anderer unterliegen** (insbesondere aus Gründen des Schutzes personenbezogener Daten, aber auch des Schutzes der Rechte des geistigen Eigentums und des Geschäftsgeheimnisses). Dieser Mechanismus lässt sektorspezifische EU-Rechtsvorschriften über den Zugang zu diesen Daten und deren Weiterverwendung unberührt. **Die Weiterverwendung solcher Daten fällt nicht in den Anwendungsbereich der Richtlinie (EU) 2019/1024** (Richtlinie über offene Daten). Die Bestimmungen dieses Kapitels begründen kein Recht auf Weiterverwendung solcher Daten, sondern sehen eine Reihe harmonisierter grundlegender Bedingungen vor, unter denen die Weiterverwendung solcher Daten erlaubt werden kann (z. B. das Erfordernis der Nichtausschließlichkeit).“*

²⁸ Siehe Artikel 1 der Richtlinie über offene Daten.

Personen definiert ist, insbesondere im Einklang mit dem Unionsrecht oder dem nationalen Recht im Hinblick auf den Schutz personenbezogener Daten“²⁹.

69. Dieser letzte Aspekt wird jedoch in Erwägungsgrund 7 des Vorschlags näher erläutert.³⁰ In diesem Zusammenhang fragen sich der EDSA und der EDSB, warum dieser wichtige Punkt (wie auch viele andere, die den Schutz personenbezogener Daten betreffen) in einem Erwägungsgrund, nicht aber im verfügbaren Teil des Vorschlags enthalten ist.
70. Nach Artikel 3 Absatz 1 der Richtlinie über offene Daten gehören darüber hinaus personenbezogene Daten, die nicht unter diese Ausnahmeregelung fallen, da sie nach den Zugangsregelungen der Union oder der Mitgliedstaaten frei zugänglich sind und für rechtmäßige Zwecke weiterverwendet werden können, ohne den Schutz der Privatsphäre und der Integrität der betroffenen Personen zu beeinträchtigen, in den Anwendungsbereich der Richtlinie und können unter den in der Richtlinie festgelegten Voraussetzungen sowie unter Einhaltung der datenschutzrechtlichen Anforderungen zur Weiterverwendung bereitgestellt werden. Wie in Erwägungsgrund 154 der DSGVO dargelegt, lässt die EU-Gesetzgebung über die Weiterverwendung von Informationen des öffentlichen Sektors *„das Schutzniveau für natürliche Personen in Bezug auf die Verarbeitung personenbezogener Daten gemäß den Bestimmungen des Unionsrechts und des Rechts der Mitgliedstaaten unberührt und beeinträchtigt diesen in keiner Weise, und sie bewirkt insbesondere keine Änderung der in dieser Verordnung [der DSGVO] dargelegten Rechte und Pflichten“*. In diesem Sinne sollte der EU-Gesetzgeber bei der Festlegung neuer Grundsätze und Regeln für die Weiterverwendung von Informationen des öffentlichen Sektors die nötige Vereinbarkeit einer solchen Weiterverwendung mit dem Recht auf den Schutz personenbezogener Daten nach der DSGVO vorsehen.³¹
71. **Folglich betonen der EDSA und der EDSB, dass die Bestimmungen der Richtlinie über offene Daten und der DSGVO bereits Mechanismen vorsehen, die den Austausch personenbezogener Daten durch öffentliche Stellen in einer Weise ermöglichen, die mit den Anforderungen an den Schutz der Grundrechte der betroffenen Personen im Einklang steht. Der EDSA und der EDSB empfehlen daher, Kapitel II des Vorschlags an die bestehenden Vorschriften über den Schutz personenbezogener Daten in der DSGVO anzugleichen und mit der Richtlinie über offene Daten abzustimmen, um sicherzustellen, dass das Schutzniveau personenbezogener Daten in der EU nicht untergraben wird, und um gleichzeitig zu vermeiden, dass durch eine solche mangelnde Angleichung Rechtsunsicherheiten für betroffene Personen, öffentliche Stellen und Weiterverwender geschaffen werden. Alternativ könnten – unbeschadet der weiteren Hinweise in dieser gemeinsamen Stellungnahme zu den Auswirkungen der Bestimmungen des Vorschlags über die Weiterverwendung bestimmter Kategorien geschützter Daten, die sich im Besitz öffentlicher Stellen**

²⁹ Siehe hierzu auch die Erwägungsgründe 52 und 53 sowie Artikel 1 Absatz 4 und Artikel 10 der Richtlinie über offene Daten, wobei sich Letzterer spezifisch auf Forschungsdaten bezieht.

³⁰ Daten nach dieser Verordnung *„fallen nicht in den Anwendungsbereich der Richtlinie (EU) 2019/1024, die Daten ausschließt, die unzugänglich sind, weil es sich um vertrauliche Geschäftsdaten, unter die Geheimhaltungspflicht fallende statistische Daten oder durch Rechte Dritter am geistigen Eigentum geschützte Daten handelt. Die Richtlinie (EU) 2019/1024 erfasst nämlich keine personenbezogenen Daten, da nach ihren Zugangsregelungen der Zugang zu diesen Daten aus Gründen des Datenschutzes, des Schutzes der Privatsphäre und der Integrität des Einzelnen nach den Datenschutzvorschriften ausgeschlossen oder eingeschränkt ist.“* (Hervorhebung hinzugefügt).

³¹ Siehe Erwägungsgrund 154 sowie Artikel 86 DSGVO mit besonderem Verweis auf das Unionsrecht und das Recht der Mitgliedstaaten bezüglich des Zugangs der Öffentlichkeit zu amtlichen Dokumenten.

befinden, auf das Recht der betroffenen Personen auf Privatsphäre und Datenschutz – personenbezogene Daten aus dem Anwendungsbereich des Vorschlags ausgeschlossen werden.

3.3.2 Artikel 5: Bedingungen für die Weiterverwendung von Daten durch öffentliche Stellen

72. Die Bedingungen für die Weiterverwendung von Daten, die sich im Besitz öffentlicher Stellen befinden, sind in Artikel 5 des Vorschlags aufgeführt und in Erwägungsgrund 11 näher erläutert. Der EDSA und der EDSB sind in Bezug auf diesen Punkt der Ansicht, dass der Vorschlag einige Bedenken aufwirft.
73. **Der EDSA und der EDSB bekräftigen, dass jede Verarbeitung personenbezogener Daten, auf die im Vorschlag Bezug genommen wird, in voller Übereinstimmung mit der DSGVO erfolgen und daher mit angemessenen Datenschutzgarantien einhergehen muss. Dies bedeutet, dass bei der Weiterverwendung personenbezogener Daten stets die Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben und der Transparenz sowie die Grundsätze der Zweckbindung, der Datenminimierung, der Richtigkeit, der Speicherbegrenzung und der Integrität und Vertraulichkeit nach Artikel 5 DSGVO zu beachten sind.**
74. In diesem Szenario sind Verarbeitung nach Treu und Glauben, Transparenz und Zweckbindung wesentliche Garantien, um bei Personen, deren personenbezogene Daten im Besitz des öffentlichen Sektors sind, dahin gehend Vertrauen zu schaffen, dass die Weiterverwendung der von ihnen bereitgestellten Informationen in einer Weise erfolgt, die ihre Rechte und Interessen wahrt (siehe Erwägungsgrund 14 des Vorschlags), d. h. dass ihre personenbezogenen Daten nicht in unerwarteter Weise gegen sie verwendet werden. Wie wichtig der Grundsatz der Zweckbindung ist, haben gerade die Maßnahmen, die zur Bekämpfung der COVID-19-Pandemie in Erwägung gezogen werden, klar gezeigt, z. B. in Bezug auf Gesundheitsdaten, die unter Aufsicht der Gesundheitsbehörden als Verantwortliche verarbeitet und nicht für gewerbliche oder andere, damit unvereinbare Zwecke verwendet werden dürfen.³² Folglich müssen öffentliche Stellen, die nach nationalem oder EU-Recht für die Gewährung oder Verweigerung des Zugangs zur Weiterverwendung von Daten zuständig sind, berücksichtigen, dass die Weiterverwendung personenbezogener Daten nur zulässig ist, wenn der Grundsatz der Zweckbindung nach Artikel 5 Absatz 1 Buchstabe b und Artikel 6 DSGVO eingehalten wird.³³ Die Weiterverwendung von Daten, die für das öffentliche Wohl/zur Erfüllung eines öffentlichen Auftrags 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. Solche „schleichenden Ausweitungen“ der Zweckbestimmung dürften nicht nur einen Verstoß gegen die Datenschutzgrundsätze nach Artikel 5 DSGVO darstellen, sondern könnten auch ein wesentliches Ziel des Vorschlags, nämlich das Vertrauen der betroffenen Personen in den Weiterverwendungsmechanismus (siehe die Erwägungsgründe 14 und 19), untergraben.³⁴
75. In diesem Zusammenhang erinnern der EDSA und der EDSB daran, dass in Artikel 6 Absatz 4 DSGVO die zweckbezogene Vereinbarkeit der Weiterverarbeitung (personenbezogener Daten) erläutert wird. Nach der Begriffsbestimmung von „Weiterverwendung“ in Artikel 2 Nummer 2 des Vorschlags ist die

³² Siehe die Stellungnahme des EDSB zur europäischen Datenstrategie, Rn. 10.

³³ Siehe hierzu Erwägungsgrund 52 der Richtlinie über offene Daten.

³⁴ Siehe die Stellungnahme des EDSB zur europäischen Datenstrategie, Rn. 25.

Weiterverwendung im Falle von personenbezogenen Daten aus datenschutzrechtlicher Sicht als Weiterverarbeitung personenbezogener Daten, die im Besitz öffentlicher Stellen sind, für spätere, nicht näher beschriebene (kommerzielle oder nichtkommerzielle) Zwecke zu betrachten. Artikel 5 des Vorschlags, in dem es um die Bedingungen für die Weiterverwendung geht, enthält jedoch keine Angaben zu den Zwecken, für die die Weiterverwendung rechtmäßig genehmigt werden kann, und legt auch nicht fest, dass die Zwecke einer späteren Weiterverwendung sorgfältig ermittelt und im Unionsrecht oder im Recht der Mitgliedstaaten nach Artikel 6 Absatz 1 Buchstabe c oder Artikel 6 Absatz 1 Buchstabe e und Artikel 6 Absatz 3 DSGVO³⁵ eindeutig definiert werden müssen, um schließlich nach Artikel 6 Absatz 4 DSGVO³⁶ die Anforderungen des Artikels 23 Absatz 1 DSGVO zu erfüllen.

76. Generell scheint der Vorschlag weder eine rechtliche Verpflichtung für öffentliche Stellen vorzusehen, die in ihrem Besitz befindlichen Daten zur Weiterverwendung zur Verfügung zu stellen, noch zielt er ausdrücklich auf die Wahrung der in Artikel 23 DSGVO aufgeführten Ziele ab.
77. **Daher empfehlen der EDSA und der EDSB nachdrücklich eine Änderung des Vorschlags, um klarzustellen, dass die Weiterverwendung personenbezogener Daten, die sich im Besitz öffentlicher Stellen befinden, nur dann zulässig ist, wenn sie im Unionsrecht oder im Recht der Mitgliedstaaten begründet ist. Darin ist eine Reihe eindeutiger, gesetzlich vereinbarter Zwecke festgelegt, für die die Weiterverarbeitung rechtmäßig zugelassen werden kann oder bei denen die Weiterverarbeitung eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft zum Schutz der in Artikel 23 DSGVO genannten Ziele darstellt.**
78. **Um einen rechtmäßigen Zugang zu personenbezogenen Daten durch „Datennutzer“ im Sinne der Begriffsbestimmung des Artikels 2 Nummer 6 des Vorschlags zu ermöglichen, müssen sich öffentliche Stellen, die nach nationalem oder EU-Recht befugt sind, einen solchen Zugang für die Weiterverwendung zu gewähren oder zu verweigern, des Weiteren und im Einklang mit oben genannter Empfehlung auf eine geeignete Rechtsgrundlage nach Artikel 6 DSGVO stützen, die für die besagte Weitergabe gilt. Dieser Aspekt wird jedoch in Artikel 5 des Vorschlags, in dem es um die Bedingungen für die Weiterverwendung personenbezogener Daten geht, die im Besitz öffentlicher Stellen sind, nicht genannt.**

³⁵ Nach Artikel 6 Absatz 3 DSGVO sollte das Unionsrecht oder das Recht der Mitgliedstaaten nach Artikel 6 Absatz 1 Buchstabe c oder Artikel 6 Absatz 1 Buchstabe e DSGVO unter anderem die „Zweckbindung“ der Verarbeitung personenbezogener Daten sowie den „Zweck, zu dem Daten offengelegt werden dürfen“, festlegen.

³⁶ In weiterer Hinsicht besteht das Risiko, dass die Einbeziehung von Daten, die im Besitz öffentlicher Stellen und aus Gründen der statistischen Geheimhaltung im Anwendungsbereich von Kapitel 2 des Vorschlags geschützt sind nach Artikel 3 Absatz 1 Buchstabe b und trotz des in Artikel 3 Absatz 3 genannten Grundsatzes den wesentlichen Grundsätzen des Datenschutzes im statistischen Bereich und insbesondere dem Grundsatz der Zweckbindung widerspricht, der die Verwendung vertraulicher Daten für Zwecke, die nicht ausschließlich statistischer Natur sind, strikt untersagt. Damit würde das Vertrauen natürlicher Personen in die Bereitstellung ihrer personenbezogenen Daten für statistische Zwecke untergraben (siehe Erwägungsgrund 27 der oben genannten Verordnung (EG) Nr. 223/2009 über europäische Statistiken sowie Artikel 4 Absätze 1 und 2 der Empfehlung des Europarats Nr. R (97)18 zum Schutz der für statistische Zwecke erhobenen und verarbeiteten personenbezogenen Daten).

79. In der Tat wird in Erwägungsgrund 11 des Vorschlags und dem entsprechenden Artikel 5 Absätze 3 bis 6 nicht auf das Unionsrecht oder das Recht der Mitgliedstaaten verwiesen, das die Rechtsgrundlage nach Artikel 6 Absatz 1 Buchstabe c oder e DSGVO bilden würde, vielmehr heißt es dort (Fettdruck hinzugefügt): *„Insbesondere sollten personenbezogene Daten nur dann zur Weiterverwendung an Dritte übermittelt werden, wenn es hierfür eine Rechtsgrundlage gibt.“* Diesbezüglich ist anzumerken, dass auf eine Rechtsgrundlage „nach der DSGVO“ verwiesen werden sollte. Darüber hinaus beschränkt sich dieser Erwägungsgrund auf die Aussage: *„Öffentliche Stellen sollten gegebenenfalls die Weiterverwendung von Daten auf der Grundlage der Einwilligung bzw. Erlaubnis der betroffenen natürlichen und juristischen Personen zur Weiterverwendung ihrer Daten mit geeigneten technischen Mitteln erleichtern. In diesem Zusammenhang sollten öffentliche Stellen die potenziellen Weiterverwender der Daten bei der Einholung dieser Einwilligung oder Erlaubnis unterstützen, indem sie technische Vorkehrungen treffen, mit denen Einwilligungsanfragen der Weiterverwender weitergeleitet werden können, soweit dies praktikabel ist. Dabei sollten keine Kontaktangaben weitergegeben werden, die es Weiterverwendern ermöglichen würden, die betreffenden natürlichen oder juristischen Personen direkt zu kontaktieren.“*
80. Der Wortlaut von Erwägungsgrund 14 des Vorschlags bleibt in Bezug auf das Zusammenspiel dieses Kapitels des Vorschlags mit der DSGVO ebenfalls unklar: *„... Daher sollten zusätzliche Schutzvorkehrungen für Situationen getroffen werden, in denen die Weiterverwendung solcher Daten des öffentlichen Sektors so erfolgt, dass Daten außerhalb des öffentlichen Sektors verarbeitet werden. Solche zusätzlichen Schutzvorkehrungen könnten darin bestehen, dass öffentliche Stellen die Rechte und Interessen natürlicher und juristischer Personen (insbesondere den Schutz personenbezogener Daten und sensibler Geschäftsdaten sowie den Schutz der Rechte des geistigen Eigentums) in vollem Umfang berücksichtigen, wenn solche Daten in Drittländer übertragen werden.“³⁷*
81. **Darüber hinaus stellen der EDSA und der EDSB fest, dass nach Artikel 5 Absatz 6 des Vorschlags Folgendes gilt: „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 ...“. Diesbezüglich sind der EDSA und der EDSB der Ansicht, dass die in den Absätzen 3 bis 5 aufgeführten Bedingungen (darunter der Zugang zu und die Weiterverwendung von Daten innerhalb einer sicheren Verarbeitungsumgebung) nicht als Alternative zu den in Artikel 6 DSGVO erschöpfend aufgeführten Rechtsgrundlagen angesehen werden können, es sei denn, in den genannten Absätzen wird auf das (Unionsrecht oder) Recht der Mitgliedstaaten verwiesen.³⁸**
82. Darüber hinaus ist im Vorschlag unklar, welche Rolle die öffentliche Stelle bei der Unterstützung der Weiterverwender bei der Einholung der Einwilligung der betroffenen Person für die Weiterverwendung spielt. Des Weiteren merken der EDSA und der EDSB zu Artikel 5 Absatz 6 des Vorschlags an, dass mit dieser Bestimmung eine Verpflichtung für öffentliche Stellen festgelegt wird

³⁷ Darüber hinaus halten der EDSA und der EDSB fest, dass öffentliche Stellen den rechtlichen Rahmen zum Schutz der Rechte und Interessen der betroffenen Personen nicht nur berücksichtigen, sondern auch **einhalten** sollten.

³⁸ Um der Eindeutigkeit willen sollte auch präzisiert werden, dass im Falle von Rechten des geistigen Eigentums, auf die in Artikel 5 Absatz 7 Bezug genommen wird, eine Verarbeitung personenbezogener Daten nicht zulässig ist (sie keine Rechtsgrundlage dafür darstellen).

(„unterstützt die öffentliche Stelle die Weiterverwender“), die inhaltlich nicht genau definiert ist. Hier sollte vielmehr die Rechtsgrundlage nach der DSGVO für die Kontaktierung der betroffenen Personen zur Einholung ihrer Einwilligung in die Weiterverwendung spezifiziert werden, wie auch die jeweilige Verantwortung im Zusammenhang mit der Einholung einer gültigen Einwilligung nach Artikel 7 DSGVO.³⁹ In diesem Zusammenhang sollte auch das deutliche Machtungleichgewicht berücksichtigt werden, das häufig in der Beziehung zwischen der betroffenen Person und den Behörden besteht.⁴⁰ Diesbezüglich erinnern der EDSA und der EDSB gemäß dem Grundsatz der Rechenschaftspflicht nach der DSGVO daran, dass die Wahl einer geeigneten Rechtsgrundlage für die Verarbeitung personenbezogener Daten sowie der Nachweis, dass die gewählte Rechtsgrundlage (in diesem Fall die Einwilligung) zulässigerweise angewandt werden kann, bei dem für die Verarbeitung Verantwortlichen liegt.

83. **Daher empfehlen der EDSA und der EDSB gemäß dem in der DSGVO verankerten Grundsatz der Rechtmäßigkeit nachdrücklich, unter den in Artikel 5 des Vorschlags vorgesehenen Bedingungen für die Weiterverwendung klarzustellen, dass eine geeignete Rechtsgrundlage nach der DSGVO im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehen und von den öffentlichen Stellen im Hinblick auf jede spätere Weiterverwendung personenbezogener Daten sorgfältig ermittelt werden muss.**
84. Weitere wesentliche Elemente, um das mit dem Vorschlag angestrebte Vertrauen aufzubauen, sind die Grundsätze der Verarbeitung nach Treu und Glauben und der Transparenz. Nach diesen Grundsätzen müssen die betroffenen Personen in vollem Umfang darüber informiert sein, ob die personenbezogenen Daten, die sie den öffentlichen Stellen zur Verfügung stellen oder die von diesen Stellen in Erfüllung ihrer öffentlichen Aufgaben weiterverarbeitet werden, für eine Weiterverwendung genutzt werden und für welche Zwecke. Auch müssen sie über die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben werden, informiert sein, wobei zu berücksichtigen ist, dass die betroffenen Personen in den meisten Fällen nach innerstaatlichem Recht gezwungen sind, ihre personenbezogenen Daten aufgrund gesetzlicher Verpflichtungen oder aufgrund der Beantragung einer öffentlichen Maßnahme oder Dienstleistung an die öffentliche Stelle weiterzugeben.⁴¹
85. Unter den in Artikel 5 des Vorschlags festgelegten Bedingungen für die Weiterverwendung gibt es jedoch weder einen Hinweis auf die Verpflichtung der öffentlichen Stellen, die betroffenen Personen nach der DSGVO zu informieren, noch darauf, dass es erforderlich ist, sie in den Prozess der Ermöglichung der Weiterverwendung ihrer personenbezogenen Daten einzubeziehen. Dies untergräbt nicht nur die Grundsätze der Verarbeitung nach Treu und Glauben und der Transparenz, die in der DSGVO festgelegt sind, um sicherzustellen, dass die betroffenen Personen einen klaren Überblick und die Kontrolle über die mögliche Verwendung ihrer eigenen personenbezogenen Daten

³⁹ Würde die Verantwortung bei der öffentlichen Stelle oder dem Weiterverwender liegen?

⁴⁰ In weiterer Hinsicht sollte daran erinnert werden, dass die Einwilligung in den meisten Fällen keine geeignete Rechtsgrundlage für Verarbeitungstätigkeiten darstellt, die von Behörden durchgeführt werden. Siehe EDSA-Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/579 unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de.

⁴¹ Siehe das Urteil des Gerichtshofs der Europäischen Union vom 1. Oktober 2015, Smaranda Bara u. a., C-201/14, ECLI:EU:C:2015:638.

haben, sondern widerspricht auch den Zielen des Vorschlags, das Vertrauen der betroffenen Personen darin zu stärken, dass die Weiterverwendung „in einer Art und Weise erfolgt, die ihre Rechte und Interessen wahrt“⁴². **Der EDSA und der EDSB empfehlen daher, in den Vorschlag einen ausdrücklichen Verweis aufzunehmen, dass die öffentlichen Stellen verpflichtet sind, die betroffenen Personen nach der DSGVO zu informieren und dadurch die Wahrnehmung der ihnen durch die Datenschutzvorschriften verliehenen Rechte, insbesondere des Widerspruchsrechts nach Artikel 21 DSGVO, zu unterstützen. In diesem Zusammenhang empfehlen der EDSA und der EDSB auch, in dem Vorschlag geeignete Mittel festzulegen, mit denen Einzelpersonen auf offene und kooperative Weise an dem Prozess der Einwilligung in die Weiterverwendung ihrer personenbezogenen Daten teilnehmen können.**

86. Um ein angemessenes Maß an Vertrauen in den Weiterverwendungsmechanismus zu erreichen, müssen öffentliche Stellen, die nach nationalem oder EU-Recht für die Gewährung des Zugangs zur Weiterverwendung zuständig sind, bei der Festlegung des Anwendungsbereichs und der Bedingungen für die Gewährung des Zugangs zur Weiterverwendung außerdem die Grundsätze der Datenminimierung beachten und den besonderen Schutz berücksichtigen, der für bestimmte Sektoren erforderlich ist, die routinemäßig mit besonderen Kategorien personenbezogener Daten umgehen, wie z. B. der Gesundheitssektor. Bei diesen Entscheidungen sollten auch die Richtigkeit, die Speicherbegrenzung, die Integrität und die Vertraulichkeit der personenbezogenen Daten sowie die möglichen Auswirkungen auf die betroffenen Personen sorgfältig berücksichtigt werden.
87. **In diesem Zusammenhang weisen der EDSA und der EDSB den Gesetzgeber darauf hin, dass bei der Festlegung der Vorschriften für die Weiterverwendung personenbezogener Daten sowie der damit verbundenen Bedingungen und spezifischen Datenschutzgarantien die nötigen Anforderungen an den Schutz personenbezogener Daten, insbesondere in „sensiblen Sektoren“ wie dem Gesundheitssektor, berücksichtigt werden müssen.**
88. Nach der DSGVO ist insbesondere die Datenschutz-Folgenabschätzung ein wichtiges Instrument, um sicherzustellen, dass die Datenschutzerfordernungen ordnungsgemäß berücksichtigt und die Rechte und Interessen natürlicher Personen angemessen geschützt werden, sodass ihr Vertrauen in den Weiterverwendungsmechanismus gestärkt werden kann. Daher empfehlen der EDSA und der EDSB, in den verfügbaren Teil des Vorschlags aufzunehmen, dass öffentliche Stellen im Falle einer Datenverarbeitung, die unter Artikel 35 DSGVO fällt, eine Datenschutz-Folgenabschätzung durchführen müssen.⁴³ Die Datenschutz-Folgenabschätzung wird dazu beitragen, die Risiken und die geeigneten Datenschutzgarantien für die Weiterverwendung zu ermitteln, um diesen Risiken entgegenzuwirken, insbesondere für bestimmte Sektoren, die routinemäßig mit besonderen Kategorien personenbezogener Daten zu tun haben. Neben dem Unionsrecht oder dem Recht der Mitgliedstaaten sollte sich die Entscheidung über die Weiterverwendung – insbesondere hinsichtlich einiger „sensibler Sektoren“ (Gesundheitswesen, aber auch Verkehr oder Energienetze) – auch auf diese Folgenabschätzung stützen sowie auf die spezifischen Bedingungen für die Weiterverwender und die konkreten Garantien für die betroffenen Personen (z. B. Klärung der Risiken einer erneuten Identifizierung anonymisierter Daten und der Garantien gegen diese Risiken). Die Ergebnisse einer

⁴² Siehe Erwägungsgrund 14 des Vorschlags.

⁴³ Siehe hierzu Erwägungsgrund 53 der Richtlinie über offene Daten.

solchen Folgenabschätzung sollten schließlich, wann immer möglich, als weitere Maßnahme zur Stärkung des Vertrauens und der Transparenz öffentlich gemacht werden.⁴⁴

89. Bezüglich der Bedingungen für die Weiterverwendung wird in Artikel 5 Absatz 3 des Vorschlags präzisiert, dass öffentliche Stellen die Verpflichtung auferlegen „können“, dass nur zuvor anonymisierte oder pseudonymisierte personenbezogene Daten weiterverwendet werden dürfen. Das bedeutet, dass öffentliche Stellen nicht verpflichtet sind, personenbezogene Daten so aufzubereiten, dass den Weiterverwendern nur zuvor anonymisierte oder pseudonymisierte personenbezogene Daten zur Verfügung gestellt werden. Folglich dürfen öffentliche Stellen sogar Daten für Weiterverwender offenlegen, die eine direkte Identifizierung der natürlichen Personen – auf die sich die Daten beziehen – ermöglichen, wenn die Bereitstellung anonymisierter Daten „nicht dem Bedarf des Weiterverwenders“ entspricht.⁴⁵ In diesem Fall könnte die Weiterverwendung personenbezogener Daten in den Räumlichkeiten der öffentlichen Stelle oder der Fernzugang zur Verarbeitung in einer sicheren Verarbeitungsumgebung durch öffentliche Stellen nach Artikel 5 Absatz 4 des Vorschlags weiterhin erlaubt sein. In Anbetracht der raschen Entwicklung von Techniken zur erneuten Identifizierung und der Verfügbarkeit fortschrittlicher Rechnerressourcen sollte der Gesetzgeber jedoch berücksichtigen, dass Anonymisierung, Pseudonymisierung und selbst die Verwendung einer sicheren Umgebung – gerade auf lange Sicht – nicht generell als frei von Schwachstellen angesehen werden können.
90. In diesem Zusammenhang begrüßen der EDSA und der EDSB, dass in Erwägungsgrund 11 des Vorschlags vorgesehen ist, dass der „Rückgriff auf solche sicheren Verarbeitungsumgebungen“ von den öffentlichen Stellen davon abhängig gemacht werden könnte, *„dass der Weiterverwender eine Vertraulichkeitsvereinbarung unterschreibt, die es ihm untersagt, Informationen offenzulegen, die er möglicherweise trotz der getroffenen Schutzvorkehrungen erlangt hat, wenn dadurch die Rechte und Interessen Dritter verletzt würden.“* **Der EDSA und der EDSB empfehlen jedoch auch, einen Verweis auf eine solche Vertraulichkeitsvereinbarung in den verfügbaren Teil des Vorschlags unter die in Artikel 5 festgelegten Bedingungen für die Weiterverwendung aufzunehmen. Durch diese Vereinbarung sollte den Weiterverwendern auch untersagt sein, eine Person, auf die sich die Daten beziehen, erneut zu identifizieren, und die Weiterverwender sollten verpflichtet sein, die Risiken einer erneuten Identifizierung laufend zu bewerten und jede Datenverletzung, die zu einer erneuten Identifizierung der betroffenen Personen führt, nach den Artikeln 33 und 34 DSGVO nicht nur der Datenschutzbehörde und den betroffenen Personen, sondern auch der betreffenden öffentlichen Stelle zu melden.**
91. **In jedem Fall betonen der EDSA und der EDSB, dass Anonymisierung und Pseudonymisierung nicht in gleicher Weise zu bewerten sind und von den öffentlichen Stellen bei der Beurteilung der Weiterverwendung aus der Perspektive des Datenschutzes unterschiedlich gewichtet werden sollten. Die Anonymisierung stellt ein Mittel dar, um die Weiterverwendung von Informationen des öffentlichen Sektors aus einer wettbewerbsorientierten Perspektive heraus zu fördern und gleichzeitig die verschiedenen Anforderungen der Datenschutzgesetzgebung zu erfüllen, da**

⁴⁴ Siehe die Stellungnahme des EDSB zu dem Vorschlag für eine Neufassung der Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors, verfügbar unter: https://edps.europa.eu/sites/edp/files/publication/2018-0246_psi_directive_opinion_en_de.pdf?lspt_context=gdpr.

⁴⁵ Siehe Erwägungsgrund 11 des Vorschlags.

„anonyme Informationen“, wie in Erwägungsgrund 26 der DSGVO festgehalten, nicht in den Anwendungsbereich der genannten Gesetzgebung fallen. Im Gegensatz dazu sollten Informationen, die einer Pseudonymisierung unterzogen wurden (die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten), immer noch als „personenbezogene Daten“ betrachtet werden, was die Anwendung weiterer Maßnahmen nach sich zieht, die in der Datenschutzgesetzgebung vorgeschrieben sind. Gleichzeitig verringert dies die Risiken für die betroffenen Personen und hilft den öffentlichen Stellen und Weiterverwendern, die Datenschutzverpflichtungen zu erfüllen (insbesondere die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen und der Datenminimierung). Die letztgenannten Überlegungen gelten auch für die in Artikel 5 Absatz 4 des Vorschlags vorgesehenen Maßnahmen, die öffentliche Stellen als Bedingungen für die Weiterverwendung vorschreiben können.

3.3.3 Artikel 5 Absatz 11: Weiterverwendung „hochsensibler“ nicht personenbezogener Daten

92. In Artikel 5 Absatz 11 wird auf das Konzept nicht personenbezogener Daten, die nach Unionrecht als „hochsensibel“ gelten, im Hinblick auf ihre Übermittlung in Drittländer eingegangen. In Erwägungsgrund 19 des Vorschlags werden einige Beispiele genannt: Als hochsensible Gesundheitsdaten „könnten im Gesundheitsbereich bestimmte Datensätze, die sich im Besitz von öffentlichen Gesundheitseinrichtungen, wie beispielsweise Krankenhäusern, befinden,“ gelten, „beispielsweise im Zusammenhang mit dem europäischen Gesundheitsdatenraum oder anderen sektorspezifischen Vorschriften“. In Bezug auf solche nicht personenbezogenen Daten sollte die Kommission delegierte Rechtsakte zur Festlegung besonderer Bedingungen für die Übermittlung solcher Daten in Drittländer erlassen.
93. Der EDSA und der EDSB merken diesbezüglich an, dass selbst wenn die Informationen in einem anonymisierten Datensatz nicht das Risiko einer direkten Identifizierung oder einer Aussonderung einer natürlichen Person bergen, diese Informationen in Kombination mit anderen verfügbaren Informationen das Risiko einer indirekten Identifizierung mit sich bringen könnten, sodass sie wahrscheinlich unter die Definition von personenbezogenen Daten fallen. Tatsächlich wird es umso schwieriger sein, die Anonymisierung dauerhaft zu gewährleisten, je mehr Informationen verfügbar sind und je mehr Daten weiterverwendet und geteilt werden.⁴⁶ Folglich möchten der EDSA und der EDSB darauf aufmerksam machen, dass ein Großteil der Daten, die heute schon – und in Zukunft noch verstärkt – durch Techniken der künstlichen Intelligenz, des maschinellen Lernens, des Internets der Dinge, des Cloud-Computings und der Big-Data-Analyse generiert und verarbeitet werden, häufig unter die Definition personenbezogener Daten fallen könnten. Hinsichtlich dieses Szenarios **fordern der EDSA und der EDSB den Gesetzgeber auf zu bedenken, dass auch die im Vorschlag vorgesehene Weiterverwendung nicht personenbezogener „hochsensibler“ Daten Auswirkungen auf den Schutz**

⁴⁶ Siehe hierzu Stellungnahme 05/2014 zu Anonymisierungstechniken der Artikel-29-Datenschutzgruppe (WP216) sowie das Urteil des EuGH vom 19. Oktober 2016, Patrick Breyer/Bundesrepublik Deutschland, C-582/14, das sich auf Erwägungsgrund 26 der Richtlinie 95/46/EG bezieht und sich mit den rechtlichen und praktischen Mitteln befasst, wie eine erneute Identifizierung durch die Verwendung zusätzlicher Daten, über die Dritte verfügen, beeinflusst werden kann. Die demnächst erscheinenden EDSA-Leitlinien zur Anonymisierung/Pseudonymisierung werden sich eingehender mit diesem Thema befassen.

personenbezogener Daten haben kann, insbesondere dann, wenn diese nicht personenbezogenen Daten das Ergebnis der Anonymisierung personenbezogener Daten und damit von Informationen, die sich ursprünglich auf natürliche Personen bezogen, sind. Auch in diesen Fällen müssen die Grundrechte der betroffenen Personen auf Schutz der Privatsphäre und Datenschutz in vollem Umfang gewährleistet sein. Darüber hinaus empfehlen der EDSA und der EDSB nachdrücklich, das Konzept der „hochsensiblen nicht personenbezogenen Daten“ zu präzisieren, indem zumindest konkrete Beispiele genannt werden.

3.3.4 Artikel 6: Gebühren für die Weiterverwendung von Daten

94. Hinsichtlich der in Artikel 6 des Vorschlags vorgesehenen Gebühren merken der EDSA und der EDSB an, dass die Richtlinie über offene Daten in den Erwägungsgründen 36 und 38 sowie in Artikel 6 Absätze 1, 4 und 5 ausdrücklich auf „Kosten der Anonymisierung“ Bezug nimmt. Insbesondere sieht die Richtlinie über offene Daten eine Ausnahme von der kostenfreien Weiterverwendung von Dokumenten vor, damit öffentliche Stellen in Situationen, in denen die Aufbereitung, das Aggregieren und/oder die Anonymisierung der zur Weiterverwendung angebotenen personenbezogenen Daten angesichts der erhöhten Risiken, die mit dem Angebot der Daten zur Weiterverwendung verbunden sind, gerechtfertigt ist, den Weiterverwendern angemessene Kosten dafür in Rechnung stellen können.
95. In Anbetracht der Tatsache, dass die Pseudonymisierung oder Anonymisierung von Informationen, die sich im Besitz öffentlicher Stellen befinden, in bestimmten Fällen eine komplexe, zeitaufwendige und kostspielige Aufgabe sein kann, die Fachwissen erfordert, das möglicherweise nicht immer zur Verfügung steht, empfehlen der EDSA und der EDSB, in Artikel 6 Absatz 5 des Vorschlags aufzunehmen, dass in den **Gebühren, die von öffentlichen Stellen für die Erlaubnis zur Weiterverwendung von Daten erhoben werden, die Kosten, die den öffentlichen Stellen für die Pseudonymisierung oder Anonymisierung** der zur Weiterverwendung zur Verfügung gestellten personenbezogenen Daten entstehen, **angemessen berücksichtigt werden können.**
96. Es sei auch angemerkt, dass **der Vorschlag den in der Richtlinie über offene Daten festgelegten allgemeinen Grundsatz der „kostenfreien“ Weiterverwendung aufhebt.** Denn es heißt in Artikel 6 Absatz 1 des Vorschlags: *„Öffentliche Stellen, die eine Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien erlauben, können Gebühren für die Erlaubnis der Weiterverwendung dieser Daten erheben.“* In dieser Hinsicht ist das Zusammenspiel mit der Richtlinie über offene Daten unklar.
97. Außerdem ist festzustellen, dass in Artikel 6 Absatz 5 zwar vorgesehen ist, dass die Gebühren „aus den Kosten abgeleitet [werden], die im Zusammenhang mit der Bearbeitung von Anträgen auf Weiterverwendung ... entstehen“, doch der Vorschlag scheint finanzielle Anreize für öffentliche Stellen einzuführen, damit diese die Weiterverwendung personenbezogener Daten gestatten.
98. Es sei auch angemerkt, dass öffentliche Stellen nach Artikel 6 Absatz 4 verpflichtet sind, Maßnahmen zu ergreifen, *„um – im Einklang mit den Vorschriften über staatliche Beihilfen – Anreize für die Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien [die auch personenbezogene Daten beinhalten] zu nichtkommerziellen Zwecken und durch kleine und mittlere Unternehmen zu schaffen.“*

99. Dieser Aspekt ist, auch in Anbetracht der in den allgemeinen Bemerkungen dieser gemeinsamen Stellungnahme beschriebenen kritischen Punkte des Vorschlags, aus datenschutzrechtlicher Sicht problematisch, und zwar sowohl in rechtlicher Hinsicht als auch im Hinblick auf die praktische Umsetzung. Besonders die Unklarheit über die Art der Anreize und deren Empfänger kann zu der Frage führen, ob die Einwilligung als eine der Rechtsgrundlagen, auf die sich Artikel 5 Absatz 6 des Vorschlags für die Weiterverwendung personenbezogener Daten stützt, die geeignete Rechtsgrundlage wäre, zumal es den betroffenen Personen frei steht, ihre Einwilligung in die Weiterverwendung ihrer personenbezogenen Daten zu erteilen oder zu verweigern.⁴⁷

3.3.5 Governance und institutionelle Aspekte: Artikel 7 (Zuständige Stellen). Artikel 8 (Zentrale Informationsstelle)

100. Der Vorschlag sieht vor, dass die Mitgliedstaaten eine zentrale Anlaufstelle für die Weiterverwendung von Daten des öffentlichen Sektors (Artikel 8) und Stellen für die Unterstützung öffentlicher Stellen mit technischen Mitteln und rechtlicher Beratung bei der Weiterverwendung von Daten des öffentlichen Sektors einrichten (Artikel 7). Nach Artikel 7 Absatz 3 können solche „zuständigen Stellen“ damit betraut werden, den Zugang zur Weiterverwendung von Daten, einschließlich personenbezogener Daten, zu gewähren.
101. Demnach werden die zuständigen Stellen die öffentlichen Stellen unter anderem dabei unterstützen, die Einwilligung oder Erlaubnis zur Weiterverwendung einzuholen, und können auch damit betraut werden, Zugang zur Weiterverwendung von Daten im Besitz der öffentlichen Stelle, einschließlich von personenbezogenen Daten, zu gewähren.
102. Erstens sollte die Bestimmung in Artikel 7 Absatz 2 Buchstabe c präziser formuliert werden, insbesondere aufgrund der Ungenauigkeit der verwendeten Begriffe („Erlaubnis zur Weiterverwendung ... durch die Weiterverwender“, „altruistische und andere Zwecke“, „entsprechend den besonderen Festlegungen der Dateninhaber“). Die Grundaussage der Bestimmung (die zuständigen Stellen unterstützen die öffentlichen Stellen gegebenenfalls bei der Einholung der Einwilligung oder Erlaubnis zur Weiterverwendung für altruistische und andere Zwecke durch die Weiterverwender entsprechend den besonderen Festlegungen der Dateninhaber) ist daher ebenfalls unklar.
103. Zweitens sind diese Stellen zwar im Wesentlichen mit Unterstützungs- und Beratungsaufgaben gegenüber öffentlichen Stellen im Hinblick auf die Weiterverwendung von Daten betraut, doch betreffen einige ihrer Aufgaben die Umsetzung der in den Datenschutzvorschriften festgelegten Garantien und die Stärkung des Schutzes der Rechte und Interessen natürlicher Personen in Bezug auf ihre personenbezogenen Daten. In Kapitel II des Vorschlags wird jedoch nicht geklärt, ob

⁴⁷ Wie in den EDSA-Leitlinien 05/2020 über die Einwilligung nach der DSGVO dargelegt, wird grundsätzlich eine Einwilligung durch jede Form von unangemessenem Druck oder Einflussnahme (die sich auf viele verschiedene Weisen manifestieren kann) auf die betroffene Person, die diese von der Ausübung ihres freien Willens abhalten, unwirksam.

Datenschutzaufsichtsbehörden – denen die DSGVO u. a. auch beratende Befugnisse überträgt – als zuständige Stelle nach Artikel 7 des Vorschlags benannt werden können.⁴⁸

104. In diesem Zusammenhang betonen der EDSA und der EDSB zunächst, dass es für öffentliche Stellen, Weiterverwender und betroffene Personen wahrlich komplex sein kann, wie die zuständigen Stellen, die sich in gewissem Maße mit der Verarbeitung personenbezogener Daten nach Kapitel II des Vorschlags befassen können, benannt und vielfach eingesetzt werden. Auch könnte die Kohärenz bei der Überwachung der Anwendung der Bestimmungen der DSGVO dadurch beeinträchtigt werden. **Folglich sind der EDSA und der EDSB der Ansicht, dass – sofern personenbezogene Daten auf der Grundlage des Vorschlags weiterverwendet werden – die Datenschutzaufsichtsbehörden die einzigen sein sollten, die für die Aufsicht über eine solche Verarbeitung personenbezogener Daten zuständig sind. Diesen Behörden sollten angemessene Ressourcen zur Verfügung gestellt werden, damit sie diese Aufgabe wirksam und effizient wahrnehmen können.**
105. **Sollten darüber hinaus spezielle Stellen benannt werden, die öffentliche Stellen und Weiterverwender von Daten unterstützen sollen und mit der Gewährung des Zugangs für die Weiterverwendung von Daten, einschließlich personenbezogener Daten, betraut werden, können diese Stellen nicht als „zuständig“ bezeichnet werden, da sie nicht als Aufsichtsbehörde fungieren würden, die die Bestimmungen über die Verarbeitung personenbezogener Daten zu überwachen und durchzusetzen vermag. Um die Rechtssicherheit und die einheitliche Anwendung des EU-Besitzstands im Bereich des Schutzes personenbezogener Daten zu gewährleisten, müssen die Tätigkeiten und Pflichten dieser benannten Stellen auch der unmittelbaren Zuständigkeit und Aufsicht der Datenschutzbehörden unterliegen, wenn personenbezogene Daten betroffen sind.**
106. **Durch ihre Zuständigkeiten und Aufgaben im Rahmen der DSGVO verfügen die Datenschutzbehörden bereits über spezifisches Know-how bei der Überwachung der Einhaltung der Vorschriften für die Datenverarbeitung sowie darin, das Bewusstsein der Verantwortlichen und der Auftragsverarbeiter für ihre Verpflichtungen in Bezug auf die Verarbeitung personenbezogener Daten zu stärken. Damit eine Kohärenz zwischen dem in Kapitel II des Vorschlags vorgesehenen institutionellen Rahmen und der DSGVO gewährleistet werden kann, empfehlen der EDSA und der EDSB daher zu präzisieren, dass die Datenschutzaufsichtsbehörden die primär zuständigen Behörden für die Überwachung und Durchsetzung der Bestimmungen des Kapitels II in Bezug auf die Verarbeitung personenbezogener Daten sind. Die Datenschutzaufsichtsbehörden sollten im Sinne einer kohärenten Anwendung dieser Bestimmungen eng mit den spezifischen Stellen zusammenarbeiten, die nach dem Vorschlag zur Unterstützung der öffentlichen Stellen und Weiterverwender benannt werden und mit der Gewährung des Zugangs für die Weiterverwendung von Daten betraut sind – erforderlichenfalls in Absprache mit anderen einschlägigen Fachbehörden.**
107. Der EDSA und der EDSB stellen außerdem fest, dass der Vorschlag in Artikel 8 Absatz 4 einen Rechtsbehelf für Weiterverwender vorsieht, mit dem sie die Entscheidung über die Verweigerung des

⁴⁸ So wie es zum Beispiel im Zusammenhang mit bestehenden Datenräumen, wie der französischen Gesundheitsdatenstelle (Health Data Hub), der Fall ist, wo die französische Datenschutzbehörde für die Genehmigung des Zugangs zu bestimmten personenbezogenen Daten zuständig ist. Siehe in diesem Zusammenhang auch die Beratungsbefugnisse, die den Datenschutzbehörden in Verbindung mit Datenschutz-Folgenabschätzungen übertragen wurden, um die Einhaltung der Vorschriften zum Schutz personenbezogener Daten nach Artikel 57 Absatz 1 Buchstabe l und Artikel 58 Absatz 3 Buchstabe a DSGVO sicherzustellen.

Zugangs zur Weiterverwendung anfechten können, der sich von dem in der Richtlinie über offene Daten vorgesehenen Rechtsbehelf unterscheidet. Nach der Richtlinie über offene Daten (siehe Artikel 4 Absatz 4) umfassen die Rechtsbehelfe insbesondere die Möglichkeit der Überprüfung durch eine unabhängige Überprüfungsinstanz mit den entsprechenden Fachkenntnissen, wie u. a. *„die gemäß der Verordnung (EU) 2016/679 errichtete Aufsichtsbehörde oder ein nationales Gericht, deren Entscheidungen für die betreffende öffentliche Stelle bindend sind.“* Unbeschadet der bereits in dieser gemeinsamen Stellungnahme gemachten Anmerkungen, wonach es erforderlich ist, das Zusammenspiel des Vorschlags mit der Richtlinie über offene Daten zu präzisieren, machen der EDSA und der EDSB den Gesetzgeber auf die Unstimmigkeiten zwischen diesen beiden Regelungen aufmerksam.

3.4 Anforderungen an Anbieter von Diensten für die gemeinsame Datennutzung

In der Begründung wird Folgendes erläutert: *„Kapitel III zielt darauf ab, das Vertrauen in die gemeinsame Nutzung personenbezogener und nicht personenbezogener Daten zu stärken und die Transaktionskosten im Zusammenhang mit der gemeinsamen B2B- und C2B-Datennutzung zu senken, indem eine Anmeldeverordnung für Anbieter für die gemeinsame Datennutzung geschaffen wird. Die Anbieter werden eine Reihe von Anforderungen zu erfüllen haben; dabei müssen sie insbesondere neutral in Bezug auf die ausgetauschten Daten bleiben. Sie dürfen diese Daten nicht für andere Zwecke verwenden. Bei Anbietern, die Dienste für die gemeinsame Datennutzung für natürliche Personen erbringen, muss auch das zusätzliche Kriterium der Übernahme treuhänderischer Pflichten gegenüber den Personen, die diese Dienste nutzen, erfüllt sein. Mit diesem Ansatz soll sichergestellt werden, dass die Dienste für die gemeinsame Datennutzung offen und kooperativ funktionieren, wobei gleichzeitig die Position natürlicher und juristischer Personen gestärkt wird, indem ihnen ein besserer Überblick und eine bessere Kontrolle über ihre Daten ermöglicht wird. Eine von den Mitgliedstaaten benannte zuständige Behörde wird für die Überwachung der Einhaltung der mit der Bereitstellung dieser Dienste verbundenen Anforderungen zuständig sein.“*⁴⁹

108. In Artikel 9 Absatz 1 des Vorschlags, auf den in Erwägungsgrund 22 näher eingegangen wird, werden drei verschiedene Arten von Diensten für die gemeinsame Datennutzung genannt:
- unter Buchstabe a: Vermittlungsdienste zwischen Dateninhabern, die juristische Personen sind, und potenziellen Datennutzern,
 - unter Buchstabe b: Vermittlungsdienste zwischen betroffenen Personen und potenziellen Datennutzern,
 - unter Buchstabe c: „Datengenossenschaften“.
109. In Bezug auf die erste Art von Dienst für die gemeinsame Datennutzung bezieht sich Artikel 9 Absatz 1 Buchstabe a auf *„Vermittlungsdienste zwischen Dateninhabern, die juristische Personen sind, und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung solcher Dienste; zu solchen Diensten können auch der zwei- oder mehrseitige Austausch von Daten oder die Einrichtung von Plattformen oder Datenbanken, die den Austausch oder die*

⁴⁹ Begründung, Seite 7.

gemeinsame Verwertung von Daten ermöglichen, sowie die Einrichtung einer speziellen Infrastruktur für die Vernetzung von Dateninhabern und Datennutzern gehören“.

110. In Erwägungsgrund 22 wird präzisiert: *„Anbieter von Diensten für die gemeinsame Datennutzung (Datenmittler) dürften eine Schlüsselrolle in der Datenwirtschaft spielen, da sie das Aggregieren und den Austausch erheblicher Mengen einschlägiger Daten erleichtern. Datenmittler, die Dienste anbieten, die die verschiedenen Akteure miteinander verbinden, können zur effizienten Bündelung von Daten sowie zur Erleichterung des bilateralen Datenaustauschs beitragen. 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. Diese Verordnung sollte ausschließlich für Anbieter von Diensten für die gemeinsame Datennutzung gelten, deren Hauptziel in der Herstellung einer geschäftlichen, rechtlichen und möglicherweise auch technischen Beziehung zwischen den Dateninhabern, einschließlich betroffener Personen, einerseits und möglichen Nutzern andererseits sowie darin besteht, die Parteien bei einer Transaktion von Datenbeständen zwischen beiden zu unterstützen. Sie sollte sich lediglich auf Dienste erstrecken, die auf die Vermittlung zwischen einer unbestimmten Zahl von Dateninhabern und Datennutzern abzielen, nicht aber auf Dienste für die gemeinsame Datennutzung, die für eine geschlossene Gruppe von Dateninhabern und -nutzern gedacht sind.“*
111. **Angesichts der obigen Ausführungen sind der EDSA und der EDSB der Ansicht, dass das in den allgemeinen Bemerkungen dieser gemeinsamen Stellungnahme als übergreifendes Problem genannte Risiko der Schaffung eines parallelen Regelwerks durch den Vorschlag, das nicht mit der DSGVO in Einklang steht, in Bezug auf Kapitel III des Vorschlags besonders deutlich wird. Es ist unklar, wie die Bestimmungen in Artikel 9 des Vorschlags, die sich auf „Dateninhaber“, „potenzielle Datennutzer“, „den Austausch oder die gemeinsame Verwertung von Daten“ und „die Vernetzung von Dateninhabern und Datennutzern“ beziehen, mit den Vorschriften und Grundsätzen der DSGVO zusammenwirken.**
112. Wir erinnern daran, dass – soweit sich die Vermittlung auf personenbezogene Daten bezieht – ein plattformartiger Dienst für die gemeinsame Datennutzung, der „auf die Vermittlung zwischen einer unbestimmten Zahl von Dateninhabern und Datennutzern“ abzielt und die Nutzung durch eine geschlossene Gruppe von Datennutzern ausschließt, insbesondere mit dem Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen nach Artikel 25 DSGVO vereinbar sein muss.⁵⁰

⁵⁰ Siehe Artikel 25 Absatz 2: „Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen **nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.**“

Siehe auch EDSA-Leitlinien 4/2019 zum Grundsatz des Datenschutzes durch Technik und Voreinstellungen, Seite 20:

„Wesentliche Elemente der technischen und voreingestellten Zweckbindung können sein:

113. Der EDSA und der EDSB verweisen auch auf die datenschutzrechtlichen Grundsätze der Transparenz (und der Zweckbindung) der Verarbeitung personenbezogener Daten. Wie in den Leitlinien für Transparenz der Artikel-29-Datenschutzgruppe dargelegt, ist es wichtig, dass „*die betroffene Person den Umfang und die Folgen der Verarbeitung im Vorfeld ermitteln kann*“; „*anders gesagt, welche Art von Auswirkungen ergeben sich durch die in den Datenschutzerklärungen/-hinweisen beschriebene spezifische Verarbeitung konkret für die betroffene Person*“.⁵¹
114. **Das Konzept von plattformartigen Diensten für die gemeinsame Datennutzung, „die auf die Vermittlung zwischen einer unbestimmten Zahl von Dateninhabern und Datennutzern abzielen“, als eine Art offener Datenmarktplatz würde den oben genannten Datenschutzgrundsätzen des eingebauten Datenschutzes (durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), der Transparenz und der Zweckbindung zuwiderlaufen, wenn die Plattform der betroffenen Person keine Vorauswahl und vorherige Information über die Zwecke und Nutzer ihrer personenbezogenen Daten ermöglicht. Im Sinne der Klarheit sollte dieser Aspekt zumindest in einem Erwägungsgrund des Vorschlags präzisiert werden.**
115. **Bei der Formulierung „Datenmittler zwischen Dateninhabern und juristischen Personen“ ist der Anwendungsbereich ebenfalls unklar und sollte daher genauer erläutert werden.**⁵²

– Vorbestimmung: Die rechtmäßigen Zwecke müssen vor der Technikgestaltung der Verarbeitung festgelegt werden.

– Spezifität: Die Zwecke müssen in Bezug auf die Frage, warum personenbezogene Daten verarbeitet werden, spezifiziert und eindeutig sein.

– Zweckorientierung: Die Technikgestaltung der Verarbeitung soll sich am Zweck der Verarbeitung orientieren, und die Grenzen der Verarbeitung sind anhand des Zwecks der Verarbeitung festzulegen.

– Erforderlichkeit: Der Zweck bestimmt, welche personenbezogenen Daten für die Verarbeitung erforderlich sind.

– Vereinbarkeit: Jeder neue Zweck muss mit dem ursprünglichen Zweck, für den die Daten erhoben wurden, vereinbar sein, und die entsprechenden Änderungen an der Technikgestaltung müssen sich daran orientieren.

– Beschränkung der Weiterverarbeitung: Der für die Verarbeitung Verantwortliche darf keine Datensätze miteinander verbinden oder eine Weiterverarbeitung für neue, unvereinbare Zwecke durchführen.

– Beschränkung der Weiterverwendung: Der für die Verarbeitung Verantwortliche sollte technische Maßnahmen, einschließlich Hashing und Verschlüsselung, einsetzen, um die Möglichkeit der Umnutzung personenbezogener Daten zu beschränken. Der Verantwortliche sollte auch organisatorische Maßnahmen treffen, wie z. B. Richtlinien und vertragliche Verpflichtungen, die die Wiederverwendung personenbezogener Daten einschränken.

– Überprüfung: Der für die Verarbeitung Verantwortliche sollte regelmäßig überprüfen, ob die Verarbeitung für die Zwecke, für die die Daten erhoben wurden, erforderlich ist, und die Technikgestaltung auf die Zweckbindung hin prüfen.“

⁵¹ Artikel-29-Datenschutzgruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, Seite 7.

⁵² In Erwägungsgrund 22 wird präzisiert: „... Anbieter von **Cloud-Diensten** sowie **Diensteanbieter, die Daten von Dateninhabern einholen, sie aggregieren, anreichern oder umwandeln und Lizenzen für die Nutzung** der sich daraus ergebenden Daten an die Datennutzer vergeben, ohne eine direkte Beziehung zwischen Dateninhabern und Datennutzern herzustellen, z. B. **Werbe- oder Datenmakler, Datenberatungsunternehmen und Anbieter von Datenprodukten, deren Mehrwert der Diensteanbieter aus den Daten erzeugt hat**, sollten ausgenommen sein. Gleichzeitig sollte es Anbietern von Diensten für die gemeinsame Datennutzung gestattet sein, die

116. Generell sei auch angemerkt, dass im Vorschlag nicht näher erläutert wird, **wie (auf welcher Rechtsgrundlage der DSGVO) Anbieter von Diensten für die gemeinsame Datennutzung personenbezogene Daten für die Zwecke des Austauschs erheben werden.**
117. Auch ist unklar, **ob Anbieter von Diensten für die gemeinsame Datennutzung Daten vermitteln können, die durch öffentliche Stellen im Sinne von Kapitel II des Vorschlags weiterverwendet werden dürfen.**
118. Aus Gründen der Transparenz und um das Vertrauen der Bürgerinnen und Bürger zu stärken (statt zu schwächen) ist es außerdem wichtig, im Vorschlag klarzustellen, dass der Dienst für die gemeinsame Datennutzung erbracht wird, wenn Dateninhaber und Datennutzer einen „Preis“ dafür zahlen. Dieser Punkt lässt sich aus dem Wortlaut von Artikel 11 Nummer 3 des Vorschlags⁵³ ableiten, ist jedoch unklar und lückenhaft (er vermittelt kein klares Bild von den monetären Transaktionen, die mit der Verarbeitung personenbezogener Daten einhergehen). Mit dem klaren Anreiz, personenbezogene Daten zu „monetarisieren“, gewinnt auch die Kontrolle der Einhaltung des Datenschutzes an Bedeutung.⁵⁴ Bedauerlicherweise werden in der Folgenabschätzung⁵⁵ in dieser Hinsicht, wie auch in Bezug auf die anderen Kapitel des Vorschlags, die Risiken für den Datenschutz nicht berücksichtigt.
119. Darüber hinaus stellen der EDSA und der EDSB fest, dass der Vorschlag kein klares Bild vermittelt – etwa durch Beispiele in den Erwägungsgründen –, was die „Nutzungsfälle“ von Diensten für die gemeinsame Datennutzung (deren „monetärer Transaktionsaspekt“, wie betont, in diesem Fall der Öffentlichkeit und den betroffenen Personen deutlich gemacht werden soll) betrifft. So wird beispielsweise in Erwägungsgrund 22 präzisiert, welche Plattformen für den Datenaustausch nicht als „Datenmittler“ gelten: *„Plattformen für den Datenaustausch, die ausschließlich von einem einzigen*

ausgetauschten Daten auf Wunsch des Datennutzers **so anzupassen, dass dies die Nutzbarkeit der Daten durch den Datennutzer verbessert** (z. B. durch Umwandlung in bestimmte Formate). Darüber hinaus sollten **Dienste, die sich auf die Vermittlung von Inhalten, insbesondere von urheberrechtlich geschützten Inhalten, konzentrieren, nicht unter diese Verordnung fallen.**

Plattformen für den Datenaustausch, die ausschließlich von einem einzigen Dateninhaber genutzt werden, um die Nutzung der in seinem Besitz befindlichen Daten zu ermöglichen, sowie Plattformen, die im Zusammenhang mit Objekten und Geräten, die mit dem Internet der Dinge verbunden sind, entwickelt wurden und deren Hauptziel darin besteht, die Funktionen des verbundenen Objekts oder Geräts sicherzustellen und Mehrwertdienste zu ermöglichen, sollten nicht unter diese Verordnung fallen. ‚Bereitsteller konsolidierter Datenträger‘ im Sinne von Artikel 4 Absatz 1 Nummer 53 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates sowie ‚Kontoinformationsdienstleister‘ im Sinne von Artikel 4 Nummer 19 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates sollten für die Zwecke dieser Verordnung nicht als Anbieter von Diensten für die gemeinsame Datennutzung gelten. Einrichtungen, die lediglich die Nutzung von Daten erleichtern, die auf der Grundlage von Datenaltruismus bereitgestellt werden, und ohne Erwerbszweck tätig sind, sollten nicht unter Kapitel III dieser Verordnung fallen, da deren Tätigkeit Zielen von allgemeinem Interesse dient, indem sie die für diese Zwecke verfügbaren Datenmengen steigert.“

⁵³ In Artikel 11 Nummer 3 des Vorschlags heißt es: „der Anbieter stellt sicher, dass das Verfahren für den Zugang zu seinem Dienst sowohl für Dateninhaber als auch für Datennutzer – auch in Bezug auf die **Preise** – fair, transparent und nichtdiskriminierend ist“.

⁵⁴ Diesbezüglich entwickelt der EDSA Leitlinien zur Erhebung und Nutzung personenbezogener Daten gegen finanzielle Vergütung.

⁵⁵ Folgenabschätzung zum Daten-Governance-Gesetz, SWD(2020) 295 final, abrufbar unter:

<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0295:FIN:EN:PDF>

Dateninhaber genutzt werden, um die Nutzung der in seinem Besitz befindlichen Daten zu ermöglichen, sowie Plattformen, die im Zusammenhang mit Objekten und Geräten, die mit dem Internet der Dinge verbunden sind, entwickelt wurden und deren Hauptziel darin besteht, die Funktionen des verbundenen Objekts oder Geräts sicherzustellen und Mehrwertdienste zu ermöglichen, sollten nicht unter diese Verordnung fallen.“ Es wird diesbezüglich aber kein Beispiel für einen vorgesehenen Nutzungsfall genannt.

3.4.1 Datenmittler im Sinne des Artikels 9 Absatz 1 Buchstabe b: Vermittlungsdienste zwischen betroffenen Personen und potenziellen Datennutzern⁵⁶

120. Der EDSA und der EDSB merken an, dass die Bestimmungen nach Artikel 9 Absatz 1 Buchstabe b in Bezug auf Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, und potenziellen Datennutzern in Ausübung der in der Verordnung (EU) 2016/679 verankerten Rechte unbeschadet der wirksamen Anwendung der Rechte der betroffenen Personen und der Pflichten des für die Verarbeitung Verantwortlichen gemäß der DSGVO anzuwenden sind.
121. Im Vorschlag sind jedoch weder die Modalitäten genauer angegeben, nach denen solche Diensteanbieter die Personen bei der Ausübung ihrer Rechte nach der DSGVO wirksam unterstützen würden, noch gibt es Hinweise darauf, für welche Verarbeitung personenbezogener Daten und in Bezug auf welche Datennutzer genau diese Unterstützung gelten würde.⁵⁷
122. Der EDSA und der EDSB sind in erster Linie der Ansicht, dass in der DSGVO die wirksame Ausübung der Rechte der betroffenen Personen und die möglichen Modalitäten für eine solche Ausübung unter der Überwachung der nationalen Aufsichtsbehörden nach Artikel 51 der Verordnung vorgesehen sind. Der Mangel an Klarheit über die genauen Modalitäten der Unterstützung bei der Ausübung der Rechte der betroffenen Personen sowie über die Empfänger eines solchen Verfahrens und ihre Pflichten gegenüber den betroffenen Personen kann zu weiteren Rechtsunsicherheiten bei der wirksamen Ausübung der Rechte der betroffenen Personen nach der DSGVO führen.
123. **Der EDSA und der EDSB würden daher empfehlen, dass der Vorschlag die Bestimmungen des EU-Rechtsrahmens (DSGVO) aufgreift, nach denen diese Modalitäten und die damit verbundenen Verpflichtungen für Anbieter und Empfänger von Diensten für die gemeinsame Datennutzung vom Europäischen Datenschutzausschuss nach Artikel 70 DSGVO näher bestimmt werden können.**⁵⁸

⁵⁶ Artikel 9 Absatz 1 Buchstabe b des Vorschlags bezieht sich auf: „Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung solcher Dienste, in Ausübung der in der Verordnung (EU) 2016/679 verankerten Rechte“.

⁵⁷ Artikel 11 Nummer 10 des Vorschlags enthält eine nach wie vor recht vage Formulierung: „der Anbieter, der Dienste für betroffene Personen anbietet, **handelt im besten Interesse der betroffenen Personen und erleichtert ihnen die Ausübung ihrer Rechte**; insbesondere berät er betroffene Personen in Bezug auf mögliche Arten der Nutzung der Daten und übliche Geschäftsbedingungen für solche Nutzungen“.

⁵⁸ Diesbezüglich arbeitet der EDSA derzeit an Leitlinien zu den Rechten der betroffenen Personen.

124. Auch ist unklar, ob sich die Vermittlungsdienste nach Artikel 9 Absatz 1 Buchstabe b des Vorschlags, die in Artikel 2 des Vorschlags nicht definiert sind, auf Systeme für das Personal Information Management (PIMS) beziehen und ob sie sich ausschließlich auf diese (und in welchem Ausmaß) beziehen. Der EDSA und der EDSB weisen darauf hin, dass es einen Unterschied zwischen PIMS, durch die die Verwaltung personenbezogener Daten ermöglicht und die Ausübung der Rechte der betroffenen Personen erleichtert werden („Schnittstelle zur betroffenen Person“)⁵⁹, und Anbietern von Diensten für die gemeinsame Datennutzung im B2B-Bereich (deren Zusammenhang mit „Datenmaklern“ unklar ist) gibt. In Bezug auf Letztere, bei denen zu den betroffenen Personen eine noch größere Distanz und das Risiko besteht, dass diese weder einen klaren Überblick noch die Kontrolle über die gemeinsame Nutzung ihrer personenbezogenen Daten haben, könnte es noch mehr kritische Aspekte aus datenschutzrechtlicher Sicht geben.⁶⁰
125. Es gelten jedoch in jedem Fall die Grundsätze der Transparenz, Verarbeitung nach Treu und Glauben und Zweckbindung.
126. In seiner Stellungnahme zu PIMS wies der EDSB darauf hin, dass es auf jeden Fall unabdingbar ist, *„die Transparenz des Geschäftsmodells gegenüber den Personen zu gewährleisten, deren Daten verarbeitet werden, damit sie wissen, um welche Interessen (von PIMS und anderen Diensteanbietern) es geht und PIMS in vollem Bewusstsein der Lage nutzen können.“*⁶¹

⁵⁹ Siehe die Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM) vom 20. Oktober 2016, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf.

⁶⁰ Siehe die Stellungnahme des EDSB zur europäischen Datenstrategie, Rn. 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 datenbezogene 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 werden.“

⁶¹ Siehe Seite 13, Rn. 52, der Stellungnahme des EDSB zu Systemen für das Personal Information Management (PIM) vom 20. Oktober 2016, abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf.

Siehe auch Rn. 53, Seite 13: *„Das PIMS-Modell fordert eine Debatte der Frage heraus, wer eigentlich unsere personenbezogenen Daten ‚besitzt‘. Gestützt auf Artikel 8 der EU-Charta der Grundrechte haben natürliche Personen in der EU das Grundrecht auf den Schutz ihrer personenbezogenen Daten. Die Rechte und Pflichten im Zusammenhang mit der Ausübung dieses Rechts sind in allen Einzelheiten in der vor Kurzem angenommenen DSGVO geregelt. Die Problematik ist nicht PIMS-spezifisch: Personenbezogene Daten werden häufig als ‚Währung‘ für die Bezahlung sogenannter ‚kostenloser‘ Dienste im Internet wahrgenommen. Dieser Trend bedeutet jedoch nicht, dass personenbezogene Daten natürlicher Personen rechtlich als Gut betrachtet werden können, das wie jedes andere Gut auf dem Markt gehandelt werden darf. Ganz im Gegenteil: PIMS werden grundsätzlich nicht in der Lage sein, personenbezogene Daten zu verkaufen; vielmehr wird ihre Rolle darin bestehen, Dritten für konkrete Zwecke und bestimmte Zeiträume vorbehaltlich der von den natürlichen Personen selbst festgelegten Bedingungen und aller vom anzuwendenden Datenschutzrecht vorgesehenen Garantien die Verwendung personenbezogener Daten zu erlauben.“*

127. Der Vorschlag enthält in Bezug auf Anbieter von Diensten für die gemeinsame Datennutzung, die keine Niederlassung in der Union haben, einige Erläuterungen, um festzustellen, ob ein solcher Anbieter in der Union Dienste anbietet. Diese Präzisierung in Erwägungsgrund 27 des Vorschlags scheint im Einklang mit Erwägungsgrund 23 der DSGVO zu stehen. Im Interesse der Rechtssicherheit könnte es sinnvoll sein zu präzisieren, dass besagte Anbieter von Diensten für die gemeinsame Datennutzung, die keine Niederlassung in der Union haben, im Falle der Verarbeitung personenbezogener Daten den Vorschriften und Grundsätzen der DSGVO unterliegen.

3.4.2 Datenmittler nach Artikel 9 Absatz 1 Buchstabe c: „Datengenossenschaften“

128. Der EDSA und der EDSB betonen, dass der Begriff „Dienste von Datengenossenschaften“ in Artikel 9 Absatz 1 Buchstabe c des Vorschlags⁶² nicht klar vermittelt, um welche Art von Diensten und um welche Verpflichtungen es dabei geht. Diesbezüglich bedarf es einer klaren Definition solcher Anbieter von Diensten für die gemeinsame Datennutzung sowie ihrer geltenden Pflichten, um Rechtsunsicherheiten bei der Erbringung solcher Dienste zu vermeiden.
129. Im Vorschlag heißt es zwar, dass Datengenossenschaften bestrebt sind, *„die Position von Einzelpersonen bei der sachkundigen Entscheidung vor der Einwilligung zur Datennutzung zu stärken, die Geschäftsbedingungen von Datennutzerorganisationen im Zusammenhang mit der Datennutzung zu beeinflussen oder mögliche Streitigkeiten zwischen Mitgliedern einer Gruppe darüber beizulegen, wie Daten verwendet werden können, wenn sich diese Daten auf mehrere betroffene Personen innerhalb dieser Gruppe beziehen“*⁶³, doch es sei daran erinnert, dass die Verpflichtung zur Transparenz sowie die Bedingungen für eine gültige Einwilligung der betroffenen Person nach Artikel 6 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 und die Bedingung für die Verarbeitung personenbezogener Daten auf dieser Rechtsgrundlage in derselben Verordnung definiert und vorgesehen sind.
130. **Der EDSA und der EDSB sind daher der Ansicht, dass die Position von Einzelpersonen bei der sachkundigen Entscheidung oder die Lösung möglicher Streitigkeiten darüber, wie Daten verwendet werden können, keine verhandelbaren Bedingungen sind, sondern vielmehr Verpflichtungen der für die Verarbeitung Verantwortlichen gemäß der Verordnung (EU) 2016/679. In diesem Zusammenhang ist auch darauf hinzuweisen, dass die Bezugnahme in Erwägungsgrund 24 des Vorschlags auf Daten, die sich auf mehrere betroffene Personen „beziehen“, im Falle von personenbezogenen Daten möglicherweise nicht mit der Definition personenbezogener Daten nach der Verordnung (EU) 2016/679⁶⁴ vereinbar ist, die auf „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ... beziehen“, verweist.**

⁶² Artikel 9 Absatz 1 Buchstabe c des Vorschlags bezieht sich auf: „Dienste von Datengenossenschaften, d. h. Dienstleistungen zur Unterstützung betroffener Personen oder von Ein-Personen-Betrieben, Kleinstunternehmen und kleinen und mittleren Unternehmen, die Mitglieder der Genossenschaft sind oder **der Genossenschaft die Befugnis übertragen, vor ihrer Einwilligung die Bedingungen der Datenverarbeitung auszuhandeln, damit sie eine sachkundige Entscheidung treffen können, bevor sie in die Datenverarbeitung einwilligen, und zur Bereitstellung von Mechanismen für den Meinungs austausch über die Zwecke und Bedingungen der Datenverarbeitung, die den Interessen der betroffenen Personen oder juristischen Personen am besten gerecht werden.**“

⁶³ Erwägungsgrund 24 des Vorschlags.

⁶⁴ Begriffsbestimmung nach Artikel 4 Nummer 1 DSGVO.

131. Darüber hinaus können, wie es in Erwägungsgrund 24 des Vorschlags heißt, *„die Rechte gemäß der Verordnung (EU) 2016/679 nur von der jeweiligen Einzelperson selbst ausgeübt und nicht an eine Datengenossenschaft übertragen oder delegiert werden“*. Der EDSA und der EDSB sind der Ansicht, dass die Formulierung solcher Grundsätze, die die Möglichkeit eröffnen, dass Datengenossenschaften die Befugnis übertragen werden kann, *„vor ihrer Einwilligung die Bedingungen der Datenverarbeitung auszuhandeln“*, unklar, wenn nicht sogar widersprüchlich ist. Die *„Bedingungen“* für die Verarbeitung personenbezogener Daten sind im Übrigen die, die in der DSGVO verankert sind, und können daher nicht durch einen Vertrag oder eine andere Form von privater Vereinbarung geändert oder ersetzt werden.

3.4.3 Artikel 10: Anmelde­regelung – allgemeine Voraussetzungen für die Zulassung zur Registrierung – Inhalt der Anmeldung; Ergebnis (und Fristen) der Anmeldung. Artikel 11: Bedingungen für die Erbringung von Diensten für die gemeinsame Datennutzung

132. In Kapitel III des Vorschlags wird die Verpflichtung für Anbieter von Diensten zur gemeinsamen Datennutzung nach Artikel 9 Absatz 1 festgelegt, sich bei der zuständigen Behörde anzumelden (Anmeldepflicht). Artikel 10 Absätze 1 und 2 enthält Vorschriften zur Bestimmung der rechtlichen Zuständigkeit des Mitgliedstaats für die Zwecke des Vorschlags. Dabei handelt es sich um die rechtliche Zuständigkeit des Mitgliedstaats der Hauptniederlassung des Anbieters von Diensten zur gemeinsamen Datennutzung. Im Falle von nicht in der Union niedergelassenen Anbietern von Diensten zur gemeinsamen Datennutzung ist es der Mitgliedstaat, in dem der gesetzliche Vertreter des Anbieters niedergelassen ist.
133. Die Informationen, die in der Anmeldung enthalten sein müssen, sind in Artikel 10 Absatz 6 Buchstaben a bis h des Vorschlags aufgeführt.⁶⁵ Ferner heißt es in Artikel 10 Absatz 7: *„Auf Antrag des Anbieters gibt die zuständige Behörde innerhalb einer Woche eine standardisierte Erklärung ab, in der sie bestätigt, dass der Anbieter die in Absatz 4 genannte Anmeldung vorgenommen hat.“*
134. Die Anmelde­regelung besteht, wie in der Begründung hervorgehoben wird, *„in einer Anmeldepflicht mit einer nachträglichen Kontrolle der Einhaltung der Anforderungen für die Ausübung der Tätigkeiten“*

⁶⁵ „Die Anmeldung muss folgende Angaben enthalten:

- a) den Namen des Anbieters von Diensten für die gemeinsame Datennutzung,
- b) den Rechtsstatus, die Rechtsform und die Registernummer des Anbieters, sofern dieser im Handelsregister oder einem anderen vergleichbaren öffentlichen Register eingetragen ist,
- c) die Anschrift der Hauptniederlassung des Anbieters in der Union, falls zutreffend, und die Anschrift einer etwaigen Zweigniederlassung in einem anderen Mitgliedstaat oder des gemäß Absatz 3 benannten gesetzlichen Vertreters,
- d) eine Website mit Informationen über den Anbieter und seine Tätigkeiten, falls zutreffend,
- e) die Kontaktpersonen und Kontaktangaben des Anbieters,
- f) eine Beschreibung des Dienstes, den der Anbieter zu erbringen beabsichtigt,
- g) das voraussichtliche Datum der Aufnahme der Tätigkeit,
- h) die Mitgliedstaaten, in denen der Anbieter seine Dienste zu erbringen beabsichtigt.“

durch die zuständigen Behörden der Mitgliedstaaten.“⁶⁶ Dieser letzte Punkt wird in den Erwägungsgründen 30 und 31 des Vorschlags näher erläutert.⁶⁷

135. Somit beschränkt sich die „Überprüfung“ des Anbieters von Diensten für die gemeinsame Datennutzung auf die Überprüfung der (hauptsächlich formalen) Anforderungen nach Artikel 10 durch die zuständige Behörde und hat innerhalb einer sehr kurzen Frist zu erfolgen (eine Woche ab dem Datum der Anmeldung).
136. **In diesem Zusammenhang merken der EDSA und der EDSB an, dass die „Überprüfungs“regelung beinahe „deklarative“ Züge aufweist und dass sich die Kommission für die „lockerste“ Regelung entschieden hat (im Gegensatz z. B. zu einer Genehmigungsregelung). Der EDSA und der EDSB weisen darauf hin, dass die Regelung zumindest im Hinblick auf die Verarbeitung personenbezogener Daten einen höheren Schutz bieten sollte (d. h. mehr Kontrollen und Garantien für die betroffenen Personen, auch in Bezug auf äußerst wichtige Datenschutzaspekte). Dadurch könnte auch für das von der Kommission angestrebte höhere Maß an Vertrauen gesorgt werden.**
137. **Hierfür sollte insbesondere Erwägungsgrund 31 des Vorschlags geändert werden.**
138. Nach dem Datenschutzgrundsatz der Rechenschaftspflicht müssen Anbieter von Diensten für die gemeinsame Datennutzung unter anderem nachweisen können, dass sie Maßnahmen und Verfahren eingeführt haben, die es den betroffenen Personen ermöglichen, ihre individuellen Datenschutzrechte problemlos auszuüben (Verfahren zur Beachtung der Rechte der betroffenen Personen). Ferner sollten sie – als Nachweis der Einhaltung der Datenschutzvorschriften – die Entscheidungen über die gemeinsame Datennutzung (insbesondere die Zwecke, für die die personenbezogenen Daten weitergegeben werden, und die Empfänger oder Kategorien von Empfängern, gegenüber denen sie offengelegt werden) dokumentieren.⁶⁸ Diese Aspekte (die den „Kern“ der in dem Vorschlag

⁶⁶ Begründung, Seite 5.

⁶⁷ „(30) Es sollte ein Anmeldeverfahren für Dienste für die gemeinsame Datennutzung eingeführt werden, um eine Daten-Governance auf der Grundlage einer vertrauenswürdigen Datenweitergabe in der Union zu gewährleisten. Die Vorteile eines vertrauenswürdigen Umfelds ließen sich am besten dadurch erreichen, dass eine Reihe von Anforderungen an die Erbringung von Diensten für die gemeinsame Datennutzung geknüpft würde, **ohne dass jedoch eine ausdrückliche Entscheidung oder ein Verwaltungsakt der zuständigen Behörde für die Erbringung solcher Dienste erforderlich wäre.**

(31) Um eine wirksame grenzüberschreitende Erbringung von Dienstleistungen zu unterstützen, sollte der Anbieter von Diensten für die gemeinsame Datennutzung aufgefordert werden, **eine Anmeldung nur an die benannte zuständige Behörde des Mitgliedstaats zu richten, in dem sich seine Hauptniederlassung oder sein gesetzlicher Vertreter befindet.** Eine solche **Anmeldung sollte nicht mehr als eine einfache Erklärung der Absicht beinhalten, solche Dienste zu erbringen, und nur durch die in dieser Verordnung genannten Informationen ergänzt werden.**“ (Hervorhebung hinzugefügt).

⁶⁸ In Artikel 30 DSGVO heißt es: „Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben: a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten; b) die Zwecke der Verarbeitung; c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten; d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen; e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe

vorgesehenen Kennzeichnung bilden sollten⁶⁹) werden dazu führen, dass die Öffentlichkeit den Anbietern von Diensten für die gemeinsame Datennutzung mehr Vertrauen entgegenbringt.

139. Der EDSA und der EDSB merken ferner an, dass die Erbringung von Diensten für die gemeinsame Datennutzung, wie in Artikel 11 festgelegt, den Bedingungen nach den Nummern 1 bis 11 unterliegt. Diesbezüglich stellen der EDSA und der EDSB fest, dass bei den (erschöpfend aufgeführten) Bedingungen zwar auf die Einhaltung der Wettbewerbsvorschriften verwiesen wird (Nummer 9), nicht jedoch auf die Einhaltung der Datenschutzvorschriften.
140. **Angesichts der obigen Ausführungen und in Anbetracht des möglichen Risikos für die betroffenen Personen bei der Verarbeitung personenbezogener Daten durch Anbieter von Diensten für die gemeinsame Datennutzung halten der EDSA und der EDSB die im Vorschlag vorgesehene deklaratorische Anmelde­regelung nicht für ein ausreichend strenges Überprüfungsverfahren für solche Dienste. Der EDSA und der EDSB empfehlen, alternative Verfahren zu prüfen, die vor allem eine systematischere Einbeziehung von Instrumenten zur Rechenschaftspflicht und zur Einhaltung der Vorschriften für die Verarbeitung personenbezogener Daten nach der DSGVO berücksichtigen, insbesondere die Einhaltung eines Verhaltenskodex oder eines Zertifizierungsmechanismus.**
141. Auch ist festzustellen, dass die in Kapitel IV des Vorschlags vorgesehenen Garantien für datenaltruistische Organisationen (Artikel 18, Transparenzanforderungen; Artikel 19, besondere Anforderungen) nach dem Vorschlag nicht für Anbieter von Diensten für die gemeinsame Datennutzung vorgesehen sind, obwohl auch diese Dienste für die gemeinsame Datennutzung Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen haben können.
142. Dieser Unterschied zwischen den beiden Anmelde­regelungen könnte Anlass zu dem Umkehrschluss geben, dass die Anforderungen, die für datenaltruistische Organisationen festgelegt wurden und sich im Falle der Verarbeitung personenbezogener Daten auf den Schutz personenbezogener Daten beziehen (z. B. Dateninhaber über eine etwaige Verarbeitung außerhalb der Union zu informieren⁷⁰), nicht für Anbieter von Diensten für die gemeinsame Datennutzung gelten.
143. **In diesem Zusammenhang merken der EDSA und der EDSB besonders an, dass Organisationen, die an Vorkehrungen beteiligt sind, durch die Daten gemeinsam genutzt und gebündelt werden können, bestimmte gemeinsame Standards einhalten müssen, deren Überwachung durch unabhängige Datenschutzbehörden in dem Vorschlag ausdrücklich erwähnt werden sollte. Dies gilt nicht nur in Bezug auf Bedingungen für eine Interoperabilität, sondern auch in Bezug auf die Bedingungen für die Gewährleistung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten und eine**

des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien; f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien; g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1. “

⁶⁹ In der Folgenabschätzung zum Vorschlag wird unter anderem auf Seite 19 auf die Kennzeichnung oder Zertifizierung verwiesen: „Die gegenseitige Anerkennung von Zertifizierungs-/Kennzeichnungsmechanismen und eines Vertrauenssystems für Datenaltruismus wird es ermöglichen, die Daten in dem erforderlichen Umfang zu sammeln und zu nutzen“; Seite 25: „Zertifizierungs- oder Kennzeichnungsrahmen für Datenmittler“; Seite 26: „Ein Zertifizierungs- oder Kennzeichnungsrahmen würde es neuen Datenmittlern ermöglichen, stärker als vertrauenswürdige Organisatoren/Koordinatoren der gemeinsamen Nutzung oder Bündelung von Daten zutage zu treten.“

⁷⁰ Artikel 19 Absatz 1 Buchstabe b des Vorschlags.

Erleichterung der Ausübung der Rechte der betroffenen Personen (z. B. durch eine Vereinbarung der gemeinsam für die Verarbeitung Verantwortlichen nach Artikel 26 der DSGVO).

144. Darüber hinaus stellen der EDSA und der EDSB fest, dass im Vorschlag auf Szenarien verwiesen wird (Verwendung von Metadaten für die Entwicklung des Dienstes für die gemeinsame Datennutzung nach Artikel 11 Nummer 2; kontinuierlicher Zugang der Dateninhaber und Datennutzer nach einer Insolvenz des Anbieters von Diensten für die gemeinsame Datennutzung zu den von diesem gespeicherten Daten nach Artikel 11 Nummer 6), die genauerer Angaben bedürfen, damit sie im Einklang mit den Vorschriften und Grundsätzen zum Schutz personenbezogener Daten stehen.
145. Der EDSA und der EDSB merken außerdem an, dass die unter den allgemeinen Bemerkungen dieser Stellungnahme gemachten Anmerkungen zu den im Vorschlag verwendeten Begriffsbestimmungen und zur Frage der Rechtsgrundlage nach der DSGVO für die Verarbeitung personenbezogener Daten auch im Hinblick auf die Bestimmungen von Kapitel III des Vorschlags relevant sind.
146. Vor allem in Bezug auf das Ziel, den betroffenen Personen eine bessere Kontrolle über den Zugang zu und die Verwendung von personenbezogenen Daten zu gewährleisten, erinnern wir außerdem daran, dass der Grundsatz der Zweckbindung gerade im Hinblick auf Datenmittler zwischen Unternehmen wichtig ist. Erwägungsgrund 26 des Vorschlags⁷¹, in dem offenbar der Zweck der Verarbeitung personenbezogener Daten mit der Vermittlung der gemeinsamen Nutzung von Daten angegeben wird, ohne dies weiter zu spezifizieren, könnte aus datenschutzrechtlicher Sicht Bedenken aufwerfen.⁷²
147. Der EDSA und der EDSB sind der Ansicht, dass die in Abschnitt 3.3 dieser gemeinsamen Stellungnahme gemachten Anmerkungen zur Weiterverwendung personenbezogener Daten, die sich im Besitz öffentlicher Stellen befinden, auch im Hinblick auf Dienste für die gemeinsame Datennutzung relevant sind:
- Jede gemeinsame Nutzung von oder jeder Zugang zu personenbezogenen Daten muss in Bezug auf Umfang und Zweck genau bestimmt sein und unter Einhaltung der DSGVO erfolgen, wobei die Anforderungen der Rechtmäßigkeit und Zweckbindung sowie die legitimen Erwartungen der betroffenen Personen zu berücksichtigen sind.
 - Es sollte deutlich sein, dass jeder „Mitwirkende“ an der Datenverarbeitungskette, einschließlich des Anbieters von Diensten für die gemeinsame Datennutzung und des/der Nutzer(s), den betroffenen

⁷¹ Erwägungsgrund 26 des Vorschlags: „Ein Schlüsselement zur Schaffung von Vertrauen in die Dienste für die gemeinsame Datennutzung und zur Stärkung der Kontrolle über diese Dienste durch die Dateninhaber und Datennutzer ist die Neutralität der Anbieter dieser Dienste in Bezug auf die zwischen Dateninhabern und Datennutzern weitergegebenen Daten. Es ist daher notwendig, dass Anbieter von Diensten für die gemeinsame Datennutzung bei den Transaktionen **lediglich als Mittler tätig werden** und die weitergegebenen Daten nicht für **andere Zwecke** verwenden. ...“

⁷² Siehe auch Artikel 2 Nummer 4 des Vorschlags; demnach bezeichnet der Ausdruck „Metadaten‘ Daten, die in Bezug auf Tätigkeiten einer natürlichen oder juristischen Person **zwecks Erbringung eines Dienstes für die gemeinsame Datennutzung** erfasst werden“; nach Artikel 2 Nummer 7 bezeichnet der Ausdruck „gemeinsame Datennutzung‘ die Weitergabe von Daten durch einen Dateninhaber an einen Datennutzer **für eine gemeinschaftliche oder individuelle Nutzung der geteilten Daten**“; in Artikel 11 Nummer 1 heißt es: „der Anbieter darf die Daten, für die er Dienste erbringt, für **keine anderen Zwecke verwenden, als sie den Datennutzern zur Verfügung zu stellen**“.

Personen die Informationen nach den Artikeln 13 und 14 DSGVO zur Verfügung stellen muss (oft ist der auf Fälle, in denen die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, anzuwendende Artikel 14 die relevante Bestimmung der DSGVO in diesem Zusammenhang). Wir empfehlen, hier hinzuzufügen, dass der Anbieter von Diensten für die gemeinsame Datennutzung der betroffenen Person benutzerfreundliche Werkzeuge zur Verfügung stellen muss, die ihr einen umfassenden Überblick über den Austausch ihrer personenbezogenen Daten geben, sowie ein benutzerfreundliches Werkzeug, das den Widerruf der Einwilligung ermöglicht, falls der bereitgestellte Dienst ein Werkzeug zur Einholung der Einwilligung der betroffenen Person in Bezug auf die Verarbeitung ihrer personenbezogenen Daten nach Artikel 11 Nummer 11 des Vorschlags beinhaltet.

– Die Datenschutz-Folgenabschätzung ist ein wichtiges Instrument, um sicherzustellen, dass die Datenschutzanforderungen ordnungsgemäß berücksichtigt und die Rechte und Interessen natürlicher Personen angemessen geschützt werden, um ihr Vertrauen in den Weiterverwendungsmechanismus zu stärken. Daher empfehlen der EDSA und der EDSB, in den verfügenden Teil des Vorschlags aufzunehmen, dass **der Anbieter von Diensten für die gemeinsame Datennutzung (und der Datennutzer) im Falle einer Datenverarbeitung, die unter Artikel 35 DSGVO fällt, eine Datenschutz-Folgenabschätzung durchführen muss**. Der im Rahmen des Vorschlags vorgesehene Datenaustausch kann nämlich eine umfangreiche Verarbeitung beinhalten, bei der Daten aus einer Vielzahl von Quellen kombiniert werden, darunter möglicherweise auch besondere Datenkategorien und/oder personenbezogene Daten schutzbedürftiger betroffener Personen. In diesem Fall sind die für die Verarbeitung Verantwortlichen verpflichtet, eine Datenschutz-Folgenabschätzung nach Artikel 35 DSGVO durchzuführen. Darüber hinaus sollten die Ergebnisse solcher Abschätzungen, wann immer möglich, sowohl vom Anbieter von Diensten für die gemeinsame Datennutzung als auch von dem/den Nutzer(n) veröffentlicht werden, um für mehr Vertrauen und Transparenz zu sorgen.

3.4.4 Artikel 12 und 13: Zuständige Behörden und Überwachung der Einhaltung (der Artikel 10 und 11)

148. Artikel 12 Absatz 3 des Vorschlags sieht Folgendes vor: *„Die benannten zuständigen Behörden, die Datenschutzbehörden, die nationalen Wettbewerbsbehörden, die für Cybersicherheit zuständigen Behörden und andere einschlägige Fachbehörden tauschen die Informationen aus, die für die Wahrnehmung ihrer Aufgaben in Bezug auf Anbieter von Diensten für die gemeinsame Datennutzung erforderlich sind.“*
149. Diese Formulierung sieht für die Datenschutzbehörden eine noch geringere Rolle vor als der Wortlaut des Vorschlags in Bezug auf datenaltruistische Organisationen⁷³, wo von *„Zusammenarbeit mit der Datenschutzbehörde“* die Rede ist.

⁷³ In Artikel 20 Absatz 3 heißt es: „Die zuständige Behörde nimmt ihre Aufgaben [als Behörde, die für das Register der anerkannten **datenaltruistischen Organisationen** und für die Überwachung der Einhaltung der Anforderungen von Kapitel IV des Vorschlags zuständig ist] in Bezug auf die Verarbeitung personenbezogener Daten **in Zusammenarbeit mit der Datenschutzbehörde** sowie mit den einschlägigen sektoralen Gremien

150. Wie in Abschnitt 3.7 dieser gemeinsamen Stellungnahme betont, erinnern der EDSA und der EDSB in diesem Zusammenhang daran, dass sich viele Bestimmungen dieses Kapitels sowie der anderen Kapitel des Vorschlags auf die Verarbeitung personenbezogener Daten beziehen und dass die Datenschutzbehörden die Behörden sind, die nach Artikel 8 der Charta und Artikel 16 AEUV „verfassungsrechtlich“ für die Aufsicht über den Schutz personenbezogener Daten zuständig sind.
151. In Bezug auf Artikel 13 des Vorschlags – Überwachung der Einhaltung – sind der EDSA und der EDSB ungeachtet des Erwägungsgrunds 28, demgemäß die Bestimmungen dieser Verordnung die Zuständigkeit der Aufsichtsbehörden nach der DSGVO unberührt lassen, der Ansicht, dass die Governance und Überwachung der Einhaltung besser definiert werden sollten. Dadurch könnte eine angemessenere Überprüfung der Anbieter von Diensten für die gemeinsame Datennutzung (und der datenaltruistischen Organisationen), auch im Hinblick auf die Einhaltung der DSGVO, gewährleistet werden; gleichzeitig könnten Überschneidungen oder Zuteilungskonflikte zwischen den im Rahmen des Vorschlags eingerichteten Behörden (die nach dem Wortlaut des Artikels 12 Absatz 3 und des Artikels 20 Absatz 3 keine Datenschutzbehörden sind) und den Datenschutzbehörden vermieden werden.
152. **Der EDSA und der EDSB sind daher der Ansicht, dass eine bessere Definition der Governance dadurch erreicht würde, dass die Datenschutzbehörden als die wichtigsten zuständigen Behörden für die Überwachung und Beaufsichtigung der Einhaltung der Bestimmungen von Kapitel III des Vorschlags benannt würden.**
153. Die Benennung von Datenschutzbehörden als die wichtigsten zuständigen Behörden für die Überwachung und Durchsetzung der Bestimmungen in Kapitel III des Vorschlags würde auch einen einheitlicheren Regulierungsansatz in allen Mitgliedstaaten gewährleisten und somit zur einheitlichen Umsetzung des Vorschlags beitragen. Gemäß ihren Zuständigkeiten und Aufgaben nach der DSGVO verfügen die Datenschutzbehörden bereits über besondere Fachkenntnisse in Bezug auf die Überwachung der Einhaltung der Vorschriften für die Datenverarbeitung, die Prüfung bestimmter Tätigkeiten der Datenverarbeitung und der gemeinsamen Nutzung von Daten, die Bewertung angemessener Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus bei der Speicherung und Übermittlung personenbezogener Daten sowie darin, das Bewusstsein der Verantwortlichen und Auftragsverarbeiter für ihre Pflichten im Zusammenhang mit der Verarbeitung personenbezogener Daten zu schärfen.
154. Die Benennung der Datenschutzbehörden als wichtigste zuständige Behörde für die Überwachung und Durchsetzung der Bestimmungen in Kapitel III wird durch die vorgesehene Bestimmung in Artikel 12

desselben Mitgliedstaats wahr. In Bezug auf etwaige **Fragen, die eine Prüfung der Einhaltung der Verordnung (EU) 2016/679 erfordern**, ersucht die zuständige Behörde zunächst um eine Stellungnahme oder einen Beschluss der gemäß dieser Verordnung zuständigen Aufsichtsbehörde und richtet sich nach dieser Stellungnahme oder diesem Beschluss.“

Es sei auch darauf hingewiesen, dass in Erwägungsgrund 28 in Bezug auf **Anbieter von Diensten für die gemeinsame Datennutzung** festgelegt ist: „Diese Verordnung sollte die Verpflichtung der Anbieter von Diensten für die gemeinsame Datennutzung zur Einhaltung der Verordnung (EU) 2016/679 und **die Verantwortung der Aufsichtsbehörden, die Einhaltung dieser Verordnung sicherzustellen, unberührt lassen.**“ Diese Präzisierung wird **nicht** in Bezug auf datenaltruistische Organisationen vorgenommen.

Absatz 3 unterstützt, die den Informationsaustausch zwischen den Datenschutzbehörden, den nationalen Wettbewerbsbehörden, den für Cybersicherheit zuständigen Behörden und anderen einschlägigen Fachbehörden ermöglicht, um eine kohärente Anwendung dieser Bestimmungen zu gewährleisten.

155. Darüber hinaus sind der EDSA und der EDSB der Ansicht, dass sich die Befugnis der zuständigen Behörden bei der Überwachung der Einhaltung der Vorschriften nicht auf die Befugnis, „Informationen anzufordern“, beschränken kann, wie es nach Artikel 13 Absatz 2 des Vorschlags den Anschein hat. Diese Einschränkung ergibt sich eindeutig aus dem deklaratorischen Charakter der im Vorschlag vorgesehenen „Kennzeichnungsregelung“, wengleich sie aufgrund der hohen Erwartung an die Einhaltung des Datenschutzes, die sich aus einer solchen Kennzeichnung insbesondere gegenüber den betroffenen Personen ergibt, nicht dem Grad der Überprüfung entspricht, den eine solche Kennzeichnung erforderlich macht.
156. Der EDSA und der EDSB betonen schließlich, dass den Datenschutzbehörden angemessene Ressourcen zur Verfügung gestellt werden sollten, damit sie die erforderliche Aufsicht wirksam und effizient durchführen können.

3.5 Datenaltruismus

3.5.1 Zusammenspiel zwischen Datenaltruismus und Einwilligung nach der DSGVO

157. Das Konzept des „Datenaltruismus“, auf das in dem Vorschlag Bezug genommen wird, umfasst Situationen, in denen natürliche oder juristische Personen Daten freiwillig und ohne Entgelt für „Zwecke von allgemeinem Interesse wie die wissenschaftliche Forschung oder die Verbesserung öffentlicher Dienstleistungen“⁷⁴ zur Weiterverwendung zur Verfügung stellen.
158. Es ließe sich argumentieren, dass der Vorschlag die bereits in der DSGVO vorgesehene Möglichkeit für Dateninhaber (zu denen nach dem Vorschlag auch betroffene Personen gehören), Daten freiwillig zur Verfügung zu stellen, nicht „erschafft“, sondern vielmehr „formalisiert/kodifiziert“. In der Tat kann eine betroffene Person bereits in die Verarbeitung sie betreffender personenbezogener Daten u. a. für wissenschaftliche Forschungszwecke einwilligen.
159. Trotz der in Artikel 2 Nummer 10 des Vorschlags enthaltenen Begriffsbestimmung (der Ausdruck „Datenaltruismus“ [bezeichnet] die Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder die Erlaubnis anderer Dateninhaber zur unentgeltlichen Nutzung ihrer nicht personenbezogenen Daten für Zwecke von allgemeinem Interesse wie die wissenschaftliche Forschung oder die Verbesserung öffentlicher Dienstleistungen“) ist das Konzept des „Datenaltruismus“ noch nicht klar und ausreichend definiert. Insbesondere ist unklar, ob die Einwilligung, wie sie im Vorschlag vorgesehen ist, dem Begriff der „Einwilligung“ nach der DSGVO – unter anderem den Bedingungen für die Rechtmäßigkeit einer solchen Einwilligung – entspricht. Darüber hinaus ist der Mehrwert des „Datenaltruismus“ unklar, wenn man den bereits bestehenden

⁷⁴ Artikel 2 Nummer 10 des Vorschlags.

Rechtsrahmen für die Einwilligung nach der DSGVO berücksichtigt, der spezifische Bedingungen für die Gültigkeit der Einwilligung vorsieht.

160. Die DSGVO und der Vorschlag bestehen in Bezug auf die Verarbeitung personenbezogener Daten durch datenaltruistische Organisationen parallel nebeneinander. Der EDSA und der EDSB unterstützen das Ziel, die Verarbeitung personenbezogener Daten für genau definierte Zwecke von allgemeinem Interesse zu erleichtern, doch muss dieses Ziel in voller Übereinstimmung mit den geltenden Datenschutzvorschriften und -grundsätzen erreicht werden. Der EDSA und der EDSB betonen insbesondere, dass eines der Hauptziele der DSGVO darin besteht, sicherzustellen, dass die betroffene Person die Kontrolle über ihre personenbezogenen Daten behält. In diesem Zusammenhang weisen der EDSA und der EDSB deutlich darauf hin, dass **alle Anforderungen hinsichtlich der Einwilligung, wie sie in der DSGVO festgelegt sind, erfüllt werden müssen.**
161. Der EDSA und der EDSB weisen erneut darauf hin, dass **das Grundrecht auf den Schutz personenbezogener Daten keinesfalls von der betroffenen Person „aufgegeben“ werden kann**, auch nicht durch einen „Akt des Altruismus“ in Bezug auf personenbezogene Daten. Der für die Verarbeitung Verantwortliche (die datenaltruistische Organisation) bleibt in vollem Umfang an die Vorschriften und Grundsätze zum Schutz personenbezogener Daten gebunden, auch wenn die betroffene Person der datenaltruistischen Organisation ihre Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.
162. **Angesichts der obigen Ausführungen sollte der Vorschlag im verfügbaren Teil präzisieren, dass er sich auf die Einwilligung im Sinne des Artikels 4 Nummer 11 DSGVO bezieht und dass für die datenaltruistische Organisation nach Artikel 7 Absatz 3 gilt, dass der Widerruf der Einwilligung so einfach sein muss wie die Erteilung der Einwilligung.**⁷⁵
163. Der EDSA und der EDSB heben auch die Tatsache hervor, dass die von den datenaltruistischen Organisationen verarbeiteten Daten besondere Kategorien personenbezogener Daten, wie z. B. Gesundheitsdaten, enthalten können.
164. Der EDSA und der EDSB betonen zudem, dass im Einklang mit dem Grundsatz der Datenminimierung Daten in anonymisierter Form verarbeitet werden sollten, wenn dies möglich und dem Zweck angemessen ist.
165. Der EDSA und der EDSB begrüßen die Bestimmung in Artikel 22 Absatz 3 des Vorschlags, wonach im Falle der Übermittlung personenbezogener Daten an die datenaltruistische Organisation den

⁷⁵ Siehe EDSA-Leitlinien 5/2020 zur Einwilligung, Rn. 121 und 122:

„121. In Artikel 6 werden die Bedingungen für die rechtmäßige Verarbeitung personenbezogener Daten festgelegt und sechs Rechtsgrundlagen beschrieben, auf die sich der Verantwortliche stützen kann. Die Anwendung einer dieser sechs Rechtsgrundlagen muss vor der Verarbeitungstätigkeit und in Bezug auf einen spezifischen Zweck festgelegt werden.

122. Hier muss festgestellt werden, dass **ein Verantwortlicher, der sich für einen Teil der Verarbeitung auf eine Einwilligung stützt, bereit sein muss, die Entscheidung zu respektieren und den Teil der Verarbeitung zu beenden, wenn eine betroffene Person ihre Einwilligung widerruft.** Es wäre gegenüber der betroffenen Person ein in höchstem Maß missbräuchliches Verhalten, ihr zu sagen, dass die Daten auf der Grundlage der Einwilligung verarbeitet werden, wenn tatsächlich eine andere Rechtsgrundlage zugrunde gelegt wird.“

betroffenen Personen im Einklang mit der DSGVO durch das Einwilligungsformular ermöglicht wird, ihre Einwilligung zu einem bestimmten Datenverarbeitungsvorgang zu erteilen und zu widerrufen.

166. Diesbezüglich sind der EDSA und der EDSB der Ansicht, dass die Regeln für den Widerruf der Einwilligung, einschließlich der daraus entstehenden Folgen, klar sein sollten. Es sollte insbesondere klar sein, wie sowohl die datenaltuistische Organisation als auch die Datennutzer den Anträgen auf Widerruf nachkommen, unter anderem durch Löschung der personenbezogenen Daten nach Artikel 17 Absatz 1 Buchstabe b DSGVO. Der EDSA und der EDSB erinnern daran, dass von den datenaltuistischen Organisationen bei Entscheidungen über „Datenaltuismus“ möglicherweise Datenschutz-Folgenabschätzungen nach Artikel 35 DSGVO durchgeführt werden müssen.
167. Wissenschaftliche Forschung beinhaltet oft die Verarbeitung und gemeinsame Nutzung besonderer Kategorien personenbezogener Daten in großem Umfang, weshalb Letztere daher in bestimmten Fällen als Datenverarbeitung betrachtet werden könnte, die nach der DSGVO ein hohes Risiko birgt. Darüber hinaus sollten Datenschutz-Folgenabschätzungen in diesem Zusammenhang unter Beteiligung des behördlichen Datenschutzbeauftragten (DSB) und eines ethischen Prüfungsausschusses durchgeführt werden. Auch sollte nach Möglichkeit und im Sinne einer guten Praxis zumindest eine Zusammenfassung davon veröffentlicht werden.
168. Nach der DSGVO sollte die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung.
169. In Erwägungsgrund 33 der DSGVO wird betont, dass der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten oftmals nicht vollständig angegeben werden kann. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht.⁷⁶ Dies wird auch in Erwägungsgrund 38 des Vorschlags berücksichtigt.
170. Der EDSA und der EDSB betonen jedoch, dass die Erteilung dieser Art von Einwilligung für Zwecke von allgemeinem Interesse⁷⁷ als solche (die nicht streng definiert sind und sich auf einen möglicherweise

⁷⁶ Siehe die kürzlich verabschiedeten EDSA-Leitlinien zur Einwilligung, Leitlinien 05/2020, insbesondere zur Einwilligung im Zusammenhang mit wissenschaftlicher Forschung auf den Seiten 30–32.

⁷⁷ Siehe EDSA-Leitlinien 03/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch, Rn. 42 bis 45:

„42. Grundsätzlich müssen personenbezogene Daten nach Artikel 5 Absatz 1 Buchstabe b ‚für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden‘.

43. Im Sinne der ‚Vereinbarkeitsvermutung‘ nach Artikel 5 Absatz 1 Buchstabe b DSGVO ‚[gilt] eine Weiterverarbeitung ... für **wissenschaftliche ... Forschungszwecke** ... gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken‘. Dieses Thema wird aufgrund seines horizontalen und komplexen Charakters in den geplanten **Leitlinien des EDSA für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke** eingehender behandelt.

anderen und viel breiteren Bereich als wissenschaftliche Forschung beziehen) nach der DSGVO nicht zulässig ist.

171. In Erwägungsgrund 35 des Vorschlags wird auf „Zwecke von allgemeinem Interesse“ verwiesen, indem (keine Definition, sondern) eine nicht erschöpfende Liste von Beispielen geliefert wird, die angewandte und privat finanzierte Forschung und technologische Entwicklung sowie Datenanalyse umfasst.⁷⁸
172. **In Anbetracht des Vorstehenden sind der EDSA und der EDSB der Ansicht, dass die Kommission genauer definieren sollte, welchen Zwecken von allgemeinem Interesse ein solcher „Datenaltruismus“ dienen sollte. Der EDSA und der EDSB vertreten die Ansicht, dass eine fehlende Definition hier zu Rechtsunsicherheit sowie zu einem niedrigeren Schutzniveau für personenbezogene Daten in der EU führen kann. So muss beispielsweise die Anforderung an die datenaltruistische Organisation, den Dateninhaber (einschließlich der betroffenen Person) über „die Zwecke von allgemeinem Interesse“ zu informieren, „für die sie die Verarbeitung ihrer Daten durch einen Datennutzer erlaubt“, im Einklang mit dem Grundsatz stehen, nach dem Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen (Grundsatz der Zweckbindung nach Artikel 5 Buchstabe b DSGVO). Daher sollte in dem Vorschlag eine vollständige Liste klar definierter Zwecke enthalten sein.** Gleichzeitig nehmen der EDSA und der EDSB die in Erwägungsgrund 38 des Vorschlags vorgenommene Präzisierung zur Kenntnis.⁷⁹ Diese Präzisierung

44. In Artikel 89 Absatz 1 DSGVO heißt es: ‚Die Verarbeitung zu ... wissenschaftlichen ... Forschungszwecken ... unterliegt **geeigneten Garantien** Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen.‘

45. Die Anforderungen von Artikel 89 Absatz 1 DSGVO unterstreichen die Bedeutung des Grundsatzes der Datenminimierung, des Grundsatzes der Integrität und Vertraulichkeit sowie des Grundsatzes des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen (siehe unten). Angesichts der Sensibilität von Gesundheitsdaten und der Risiken bei der Weiterverwendung von Gesundheitsdaten für wissenschaftliche Forschungszwecke müssen daher strenge Maßnahmen ergriffen werden, um ein angemessenes Sicherheitsniveau gemäß Artikel 32 Absatz 1 DSGVO zu gewährleisten.“

Siehe auch das am 2. Februar 2021 angenommene EDSA-Dokument als Antwort auf das Ansuchen der Europäischen Kommission um Klarstellung zur einheitlichen Anwendung der DSGVO mit Schwerpunkt auf der Gesundheitsforschung.

⁷⁸ Erwägungsgrund 35: „Zu diesen Zwecken gehören die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Erstellung amtlicher Statistiken oder die bessere Erbringung öffentlicher Dienstleistungen. Die Unterstützung der wissenschaftlichen Forschung, einschließlich z. B. der technologischen Entwicklung und Demonstration, der Grundlagenforschung, der angewandten Forschung und der privat finanzierten Forschung, sollte ebenfalls als Zweck von allgemeinem Interesse betrachtet werden. Ziel dieser Verordnung ist es, zur Entstehung von Datenbeständen beizutragen, die auf der Grundlage von Datenaltruismus bereitgestellt werden und so groß sind, dass sie Datenanalysen und maschinelles Lernen auch grenzüberschreitend in der Union ermöglichen.“

⁷⁹ Erwägungsgrund 38: „In der Union anerkannte datenaltruistische Organisationen **sollten einschlägige Daten direkt bei natürlichen und juristischen Personen sammeln oder von Dritten gesammelte Daten verarbeiten können.**“

sollte nicht nur im Erwägungsgrund enthalten sein, sondern in den verfügbaren Teil des Vorschlags aufgenommen werden und darüber hinaus klar zwischen Folgendem unterscheiden:

- der Einwilligung in Forschungsbereiche,
- der Weiterverarbeitung für wissenschaftliche oder historische oder statistische Zwecke,
- und der Verarbeitung für Zwecke von allgemeinem Interesse (die im Vorschlag zu definieren sind).

173. Darüber hinaus merken der EDSA und der EDSB an, dass der Begriff „Datenarchive“ in Erwägungsgrund 36⁸⁰, auf den nur in diesem Erwägungsgrund und nicht im verfügbaren Teil des Vorschlags Bezug genommen wird und der sich auf die Verarbeitung sowohl personenbezogener als auch nicht personenbezogener Daten bezieht, einer Klarstellung bedarf.

3.5.2 Artikel 16 und 17: Eintragsregelung – allgemeine Eintragsanforderungen – Inhalt der Eintragung; Ergebnis (und Fristen) der Eintragung

174. In Kapitel IV des Vorschlags ist die Möglichkeit vorgesehen, dass Organisationen, die „Datenaltruismus“ betreiben, sich als „in der Union anerkannte datenaltruistische Organisation“⁸¹ eintragen lassen können, mit dem erklärten Ziel, das Vertrauen der Bürger in ihre Tätigkeit zu stärken. In diesem Zusammenhang betonen der EDSA und der EDSB, dass aus dem Vorschlag nicht hervorgeht, ob die Eintragung obligatorisch ist oder nicht und ob die Bestimmungen in Kapitel IV auch für den Fall gelten, dass Organisationen, die Datenaltruismus betreiben, nicht eingetragen sind.

175. Die allgemeinen Eintragsanforderungen sind in Artikel 16 aufgeführt; die Anforderungen für die Eintragung sind in Artikel 17, insbesondere in Artikel 17 Absatz 4 Buchstaben a bis i aufgeführt. Die „Überprüfung“ der datenaltruistischen Organisation beschränkt sich auf die Überprüfung der Anforderungen nach Artikel 16 sowie Artikel 17 Absatz 4 durch die zuständige Behörde und muss innerhalb von zwölf Wochen nach Antragstellung erfolgen. Es ist im Vorschlag jedoch nicht definiert, mit welcher Art der Überprüfung die zuständige Behörde beauftragt ist.

176. Der EDSA und der EDSB merken diesbezüglich an, dass eine Regelung, die im Falle der Verarbeitung personenbezogener Daten stärkere Garantien bietet, besser geeignet wäre, angemessene Kontrollen

In der Regel stützt sich Datenaltruismus auf die Einwilligung der betroffenen Personen im Sinne von Artikel 6 Absatz 1 Buchstabe a und Artikel 9 Absatz 2 Buchstabe a sowie auf die Einhaltung der Anforderungen an eine rechtmäßige Einwilligung gemäß Artikel 7 der Verordnung (EU) 2016/679.

Gemäß der Verordnung (EU) 2016/679 können **wissenschaftliche Forschungszwecke, bestimmte Forschungsbereiche** oder Teile von Forschungsprojekten durch die Einwilligung in die Weiterverarbeitung der Daten für diese Zwecke unterstützt werden, sofern anerkannte Standards der Ethik für die wissenschaftliche Forschung eingehalten werden.

Gemäß Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 sollte eine **Weiterverarbeitung der Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke** gemäß Artikel 89 Absatz 1 der Verordnung (EU) 2016/679 nicht als unvereinbar mit den ursprünglichen Zwecken gelten.“

⁸⁰ Erwägungsgrund 36: „Juristische Personen, die bestrebt sind, **Zwecke von allgemeinem Interesse** zu unterstützen, indem sie einschlägige Daten auf der Grundlage von Datenaltruismus in größerem Maßstab zur Verfügung stellen und bestimmte Anforderungen erfüllen, sollten sich als ‚in der Union anerkannte datenaltruistische Organisationen‘ eintragen lassen können. Dies könnte zur Einrichtung von **Datenarchiven** führen.“

⁸¹ Erwägungsgrund 36 des Vorschlags.

zu gewährleisten und letztlich das Vertrauen zu stärken, als die im Vorschlag vorgesehene „leichtere“ Eintragsregelung (fast eine einfache „deklaratorische“ Regelung), die der für Anbieter von Diensten für die gemeinsame Datennutzung vorgesehenen Regelung ähnelt.

177. Der EDSA und der EDSB heben die Problematik der Tatsache hervor, dass es aus rechtlicher, technischer und organisatorischer Sicht fast keine Anforderung gibt, um eine „in der Union anerkannte datenaltruistische Organisation“ (oder ein „Anbieter von Diensten für die gemeinsame Datennutzung“) zu werden. So wird eine Organisation, die nach Artikel 15 Absatz 3 des Vorschlags berechtigt ist, „sich in ihrer schriftlichen und mündlichen Kommunikation als ‚in der Union anerkannte datenaltruistische Organisation‘“ zu bezeichnen („Kennzeichnungseffekt“), höchstwahrscheinlich personenbezogene Daten sammeln, indem sie die Erwartungen der Bürgerinnen und Bürger insbesondere an die vollständige Einhaltung des Datenschutzes durch dieselbe Organisation zu ihrem Vorteil nutzt.
178. Der EDSA und der EDSB betonen, dass datenaltruistische Organisationen vertrauenswürdige Einrichtungen sein müssen. In Bezug auf die allgemeinen Anforderungen für die Eintragung (nach Artikel 16 des Vorschlags) sind der EDSA und der EDSB außerdem der Ansicht, dass die in Artikel 16 Buchstabe b des Vorschlags vorgesehene (z. B. rechtliche, organisatorische, wirtschaftliche) Unabhängigkeit der datenaltruistischen Organisation von Einrichtungen, die Erwerbszwecke verfolgen, präzisiert werden sollte.⁸²
179. **Insbesondere empfehlen der EDSA und der EDSB, in Artikel 16 einen direkten Verweis auf die Datenschutzanforderungen aufzunehmen, besonders auf die technischen und organisatorischen Anforderungen, die die Anwendung der Datenschutzstandards und die Ausübung der Rechte der betroffenen Personen ermöglichen.**
180. **In Anbetracht der obigen Ausführungen und der möglichen Auswirkungen auf die betroffenen Personen im Hinblick auf die Verarbeitung personenbezogener Daten, die von einer datenaltruistischen Organisation vorgenommen werden kann, sind der EDSA und der EDSB der Ansicht, dass die im Vorschlag vorgesehene Eintragsregelung kein ausreichend strenges Überprüfungsverfahren für eine solche Organisation vorsieht. Der EDSA und der EDSB empfehlen, alternative Verfahren zu prüfen, die vor allem eine systematischere Einbeziehung von Instrumenten zur Rechenschaftspflicht und zur Einhaltung der Vorschriften für die Verarbeitung personenbezogener Daten nach der DSGVO berücksichtigen, insbesondere die Einhaltung eines Verhaltenskodex oder eines Zertifizierungsmechanismus.**

⁸² „Um für eine Eintragung infrage zu kommen, muss die datenaltruistische Organisation ... b) selbst ohne Erwerbszweck tätig sein und **unabhängig von jeder Organisation, die Erwerbszwecke verfolgt, handeln;**“ (Hervorhebung hinzugefügt).

3.5.3 Artikel 18 und 19: Transparenzanforderungen und „besondere Anforderungen zum Schutz der Rechte und Interessen betroffener Personen und juristischer Personen im Hinblick auf ihre Daten“

181. Der EDSA und der EDSB merken an, dass die Anforderungen, die mit der Eintragsregelung einhergehen, die **Pflichten der datenaltruistischen Organisationen in ihrer Rolle als Verantwortliche oder Auftragsverarbeiter nach der DSGVO stärken, aber nicht ersetzen** sollten.
182. Der EDSA und der EDSB merken an, dass Erwägungsgrund 36 des Vorschlags in dieser Hinsicht unklar ist, denn er lässt darauf schließen, dass die Mittel für den Widerruf der Einwilligung von der als Auftragsverarbeiter handelnden datenaltruistischen Organisation bereitgestellt werden müssen.⁸³ Dafür, dass sich die datenaltruistische Organisation als Auftragsverarbeiter anstelle des Verantwortlichen qualifiziert, bedarf es jedoch einer weiteren Bewertung, da dies nicht das einzige mögliche Szenario im Kontext des Vorschlags wäre.
183. Auch sollte klar definiert werden, wozu die Eintragung (als datenaltruistische Organisation) ermächtigt, insbesondere im Hinblick auf den Aspekt der Rechtsgrundlage für die Verarbeitung personenbezogener Daten nach der DSGVO.⁸⁴ Diesbezüglich weisen der EDSA und der EDSB erneut darauf hin, dass die **Eintragsregelung kein Ersatz dafür sein kann, dass eine geeignete Rechtsgrundlage für die Verarbeitung personenbezogener Daten nach Artikel 6 Absatz 1 DSGVO erforderlich ist**, damit die Datenverarbeitung rechtmäßig ist. Mit anderen Worten: Nach der DSGVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn und sofern mindestens eine der Rechtsgrundlagen nach Artikel 6 Absatz 1 DSGVO gegeben ist.
184. Hinsichtlich Artikel 18 des Vorschlags haben der EDSA und der EDSB Zweifel daran, wie die Unabhängigkeit der datenaltruistischen Organisation in den Fällen gewahrt wird, in denen ihre

⁸³ In Erwägungsgrund 36 heißt es (Fettdruck hinzugefügt): „**Weitere Garantien** sollten umfassen, dass **einschlägige Daten** in einer von einer eingetragenen Einrichtung betriebenen **sicheren Verarbeitungsumgebung verarbeitet werden** können, dass mithilfe von **Aufsichtsmechanismen** wie Ethikräten oder -gremien sichergestellt wird, dass der für die Verarbeitung Verantwortliche hohe wissenschaftliche Ethikstandards einhält, dass **wirksame technische Mittel vorhanden sind, um die Einwilligung auf der Grundlage der Informationspflichten der für die Verarbeitung Verantwortlichen gemäß der Verordnung (EU) 2016/679 jederzeit widerrufen oder ändern zu können**, sowie **Mittel, mit deren Hilfe sich die betroffenen Personen über die Verwendung der von ihnen bereitgestellten Daten laufend informieren können.**“ (Hervorhebung hinzugefügt).

⁸⁴ Dazu heißt es in Erwägungsgrund 38 des Vorschlags (Fettdruck hinzugefügt): „In der Union anerkannte datenaltruistische Organisationen **sollten einschlägige Daten direkt bei natürlichen und juristischen Personen sammeln** oder von Dritten gesammelte Daten verarbeiten können. **In der Regel** stützt sich Datenaltruismus auf die Einwilligung der betroffenen Personen im Sinne von Artikel 6 Absatz 1 Buchstabe a und Artikel 9 Absatz 2 Buchstabe a sowie auf die Einhaltung der Anforderungen an eine rechtmäßige Einwilligung gemäß Artikel 7 der Verordnung (EU) 2016/679. Gemäß der Verordnung (EU) 2016/679 können wissenschaftliche Forschungszwecke, bestimmte Forschungsbereiche oder Teile von Forschungsprojekten durch die Einwilligung in die Weiterverarbeitung der Daten für diese Zwecke unterstützt werden, sofern anerkannte Standards der Ethik für die wissenschaftliche Forschung eingehalten werden. Gemäß Artikel 5 Absatz 1 Buchstabe b der Verordnung (EU) 2016/679 sollte eine Weiterverarbeitung der Daten für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 der Verordnung (EU) 2016/679 nicht als unvereinbar mit den ursprünglichen Zwecken gelten.“

Finanzierung auf „Gebühren, die von den die Daten verarbeitenden natürlichen oder juristischen Personen gezahlt wurden,“⁸⁵ (d. h. für Daten, die diesen natürlichen oder juristischen Personen von der datenaltuistischen Organisation zur Verfügung gestellt werden) beruht. Darüber hinaus sind der EDSA und der EDSB der Ansicht, dass in dem Vorschlag besser erläutert werden sollte, in welchen Situationen die datenaltuistische Organisation von natürlichen oder juristischen Personen Gebühren für die Verarbeitung der von den betroffenen Personen für den Datenaltuismus „überlassenen“ Daten verlangen kann.

185. Auch in diesem Fall stellt sich, wie bereits in Bezug auf die Weiterverwendung von Daten im Besitz öffentlicher Stellen angemerkt, die Frage nach den Anreizen für den Verantwortlichen, mehr personenbezogene Daten zu verarbeiten, in diesem Fall für mehr „Datenaltuismus“. Dass sich datenaltuistische Organisationen als eingetragene Einrichtungen, die keinen Erwerbszweck verfolgen, qualifizieren (Erwägungsgrund 36) – was vom EDSA und dem EDSB begrüßt würde – schwächt die Bedeutung der vorgenannten Frage nur unwesentlich.
186. Darüber hinaus wirft der Wortlaut von Erwägungsgrund 36, in dem es um die Anforderungen an datenaltuistische Organisationen geht, Bedenken auf, da er sich auf die „freiwillige Erfüllung“ auch in Bezug auf Aspekte, die mit der (obligatorischen) Einhaltung der DSGVO in Zusammenhang stehen, bezieht.⁸⁶
187. Der Erwägungsgrund weist auch Unstimmigkeiten mit Artikel 17 Absatz 3 im verfügenden Teil des Vorschlags auf, der sich auf nicht in der Union niedergelassene datenaltuistische Organisationen bezieht (es sei denn, der fakultative Charakter der in Erwägungsgrund 36 erwähnten Anforderungen wird hervorgehoben).
188. **In Bezug auf Artikel 19 des Vorschlags sind der EDSA und der EDSB der Ansicht, dass ausdrücklich auf die Artikel 13 und 14 DSGVO hingewiesen werden sollte, um die Kohärenz zwischen diesem Artikel des Vorschlags und den Verpflichtungen in Bezug auf den Grundsatz der Transparenz nach der DSGVO sicherzustellen. Auch sollte darauf hingewiesen werden, dass die datenaltuistische Organisation und die Datennutzer der betroffenen Person in Bezug auf die Verarbeitung der sie betreffenden personenbezogenen Daten die erforderlichen Informationen bereitstellen.**

⁸⁵ Siehe Artikel 18 Absatz 1 Buchstabe d des Vorschlags.

⁸⁶ Erwägungsgrund 36 (Fettdruck hinzugefügt): „... Die **freiwillige Erfüllung der Anforderungen** durch diese eingetragenen Einrichtungen sollte für Vertrauen sorgen, dass die für altruistische Zwecke bereitgestellten Daten dem allgemeinen Interesse dienen. Dieses **Vertrauen** sollte sich insbesondere aus einem **Niederlassungsort in der Union** sowie aus der Anforderung, dass eingetragene Einrichtungen **keinen Erwerbszweck verfolgen** dürfen, aus Transparenzanforderungen und aus **spezifischen Garantien** zum Schutz der Rechte und Interessen **der betroffenen Personen und Unternehmen** ergeben. **Weitere Garantien** sollten umfassen, dass einschlägige Daten in einer von einer eingetragenen Einrichtung betriebenen **sicheren Verarbeitungsumgebung** verarbeitet werden können, dass mithilfe von **Aufsichtsmechanismen** wie Ethikräten oder -gremien sichergestellt wird, dass der für die Verarbeitung Verantwortliche hohe wissenschaftliche Ethikstandards einhält, dass wirksame **technische Mittel** vorhanden sind, **um die Einwilligung** auf der Grundlage der Informationspflichten der für die Verarbeitung Verantwortlichen gemäß der Verordnung (EU) 2016/679 jederzeit **widerrufen oder ändern zu können**, sowie Mittel, mit deren Hilfe sich die betroffenen Personen über die Verwendung der von ihnen bereitgestellten Daten **laufend informieren** können.“

189. Darüber hinaus halten der EDSA und der EDSB den derzeitigen Wortlaut von Artikel 19 Absatz 1 Buchstabe a⁸⁷ für unklar und nur schwer mit den Bestimmungen der DSGVO vereinbar.
190. **In Bezug auf dieses Kapitel des Vorschlags wäre es auch sehr wichtig, die Bereitstellung anonymisierter Daten im Einklang mit dem Grundsatz der Datenminimierung – sofern möglich und für den Zweck der Datenverarbeitung angemessen – ausdrücklich zu betonen, um die betroffenen Personen, gerade im Falle der Verarbeitung besonderer Datenkategorien, vor unangemessenen Risiken für ihre Grundrechte und -freiheiten zu schützen.**

3.5.4 Artikel 20 und 21: für die Eintragung zuständige Behörden und Überwachung der Einhaltung

191. **In Bezug auf Artikel 20 Absatz 3 des Vorschlags sind der EDSA und der EDSB der Ansicht, dass die Governance und die Überwachung der Einhaltung der Vorschriften verstärkt werden sollten, um eine angemessenere Überprüfung der datenaltuistischen Organisationen, einschließlich ihrer Einhaltung der DSGVO, zu gewährleisten. Auch sollte dadurch sichergestellt werden, dass die Überwachung der Einhaltung der Bestimmungen des Vorschlags klar definiert ist, sodass im Falle von personenbezogenen Daten die Datenschutzerfordernungen in vollem Umfang eingehalten werden, und dass in dem Fall die Aufsicht in der Zuständigkeit der gemäß der DSGVO eingerichteten Datenschutzbehörden verbleibt.**
192. **Die Benennung von Datenschutzbehörden als die wichtigsten zuständigen Behörden für die Überwachung der Einhaltung und Durchsetzung der Bestimmungen aus Kapitel IV des Vorschlags würde auch einen einheitlicheren Regulierungsansatz in allen Mitgliedstaaten gewährleisten und somit zur einheitlichen Anwendung des Vorschlags beitragen. Durch ihre Zuständigkeiten und Aufgaben nach der DSGVO verfügen die Datenschutzbehörden bereits über besondere Fachkenntnisse in Bezug auf die Überwachung der Einhaltung der Vorschriften für die Datenverarbeitung, die Prüfung bestimmter Tätigkeiten der Datenverarbeitung und der gemeinsamen Nutzung von Daten, die Bewertung angemessener Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus bei der Speicherung und Übermittlung personenbezogener Daten sowie darin, das Bewusstsein der Verantwortlichen und der Auftragsverarbeiter für ihre Pflichten im Zusammenhang mit der Verarbeitung personenbezogener Daten zu schärfen.**
193. Darüber hinaus sind der EDSA und der EDSB der Ansicht, dass sich die Befugnis der zuständigen Behörden bei der Überwachung der Einhaltung der Vorschriften nicht auf die Befugnis, „Informationen anzufordern“, beschränken kann, wie es nach Artikel 21 Absatz 2 des Vorschlags den Anschein hat. Diese Einschränkung ergibt sich eindeutig aus dem deklaratorischen Charakter der im Vorschlag vorgesehenen „Kennzeichnungsregelung“, wengleich sie aufgrund der hohen Erwartung an die Einhaltung des Datenschutzes, die sich aus einer solchen Kennzeichnung insbesondere gegenüber den betroffenen Personen ergibt, nicht dem Grad der Überprüfung entspricht, den eine solche Kennzeichnung erforderlich macht.

⁸⁷ In Artikel 19 Absatz 1 Buchstabe a heißt es (Fettdruck hinzugefügt): „Die im Register der anerkannten datenaltuistischen Organisationen eingetragenen Einrichtungen informieren Dateninhaber über Folgendes: a) **die Zwecke von allgemeinem Interesse, für die sie die Verarbeitung ihrer Daten durch einen Datennutzer erlaubt**, in leicht verständlicher Form“.

194. Der EDSA und der EDSB betonen, dass den Datenschutzbehörden angemessene Ressourcen zur Verfügung gestellt werden sollten, damit sie die erforderliche Aufsicht wirksam und effizient durchführen können. Darüber hinaus merken der EDSA und der EDSB diesbezüglich an, dass es in Erwägungsgrund 28, der sich auf Anbieter von Diensten für die gemeinsame Datennutzung bezieht, heißt: *„Diese Verordnung sollte die Verpflichtung der Anbieter von Diensten für die gemeinsame Datennutzung zur Einhaltung der Verordnung (EU) 2016/679 und die Verantwortung der Aufsichtsbehörden, die Einhaltung dieser Verordnung sicherzustellen, unberührt lassen.“* Diese Präzisierung sollte auch im Hinblick auf datenaltruistische Organisationen vorgenommen werden.

3.5.5 Artikel 22: Europäisches Einwilligungsformular für Datenaltruismus

195. Artikel 22 des Vorschlags ermächtigt die Kommission, im Wege von Durchführungsrechtsakten ein „europäisches Einwilligungsformular für Datenaltruismus“ festzulegen.⁸⁸ Diesbezüglich sieht Artikel 22, wie in Erwägungsgrund 41 ausgeführt, vor, dass das Einwilligungsformular mithilfe von Durchführungsrechtsakten von der Kommission mit Unterstützung des Europäischen Dateninnovationsrats und in Absprache mit dem EDSA festgelegt wird.
196. **Der EDSA und der EDSB sind dabei der Ansicht, dass anstelle einer bloßen Konsultation des EDSA mit dem Vorschlag ein verbindlicherer, besser strukturierter und institutionalisierter Mechanismus geschaffen werden sollte.**

3.6 Internationale Datenübermittlungen: Artikel 5 Absätze 9 bis 13; Erwägungsgründe 17 und 19; Artikel 30

197. Die Bestimmungen des Vorschlags scheinen zwar in Bezug auf Datenübermittlungen in Drittländer a priori nur auf nicht personenbezogene Daten beschränkt zu sein, doch könnten bei ihrer Anwendung womöglich Fragen bezüglich der rechtlichen und politischen Übereinstimmung mit dem EU-Datenschutzrechtsrahmen auftauchen, insbesondere, wenn personenbezogene Daten und nicht personenbezogene Daten eines Datensatzes untrennbar miteinander verbunden sind.
198. Es scheint zwar in der Absicht der Kommission zu liegen, personenbezogene Daten auszuschließen, doch kommt im Vorschlag nicht immer klar zum Ausdruck, dass der Anwendungsbereich der Bestimmungen für die Übermittlung auf nicht personenbezogene Daten beschränkt ist. Insbesondere Artikel 5 Absatz 9 und Artikel 5 Absatz 10, die sich auf die Übermittlung von Daten im Besitz öffentlicher Stellen beziehen, könnten für personenbezogene Daten gelten, wenn es sich bei diesen personenbezogenen Daten gleichzeitig um vertrauliche Daten handelt oder um Daten, die durch Rechte des geistigen Eigentums geschützt sind.⁸⁹

⁸⁸ Artikel 22 Absatz 1: „Um das Sammeln von Daten auf der Grundlage des Datenaltruismus zu erleichtern, kann die Kommission Durchführungsrechtsakte zur Festlegung eines europäischen Einwilligungsformulars für Datenaltruismus erlassen. Das Formular ermöglicht das Einholen von Einwilligungen in allen Mitgliedstaaten in einem einheitlichen Format. Diese Durchführungsrechtsakte werden nach dem in Artikel 29 Absatz 2 genannten Beratungsverfahren erlassen.“

⁸⁹ Siehe Artikel 5 Absatz 10 des Vorschlags: „Öffentliche Stellen übermitteln vertrauliche Daten oder durch Rechte des geistigen Eigentums geschützte Daten nur dann an einen Weiterverwender, der beabsichtigt, die Daten in ein nicht gemäß Absatz 9 benanntes Drittland zu übertragen, wenn der Weiterverwender sich

199. **Gleichzeitig enthält der Vorschlag eine Bestimmung (Artikel 5 Absatz 11), die so verstanden werden kann, als würde sie nicht personenbezogene Daten besser schützen als personenbezogene Daten, da die Kommission dem Vorschlag zufolge letztlich mittels delegierter Rechtsakte⁹⁰ besondere Bedingungen für die Übermittlung nicht personenbezogener Daten an bestimmte Drittländer festlegen könnte, die sogar ein Verbot beinhalten können.⁹¹**
200. **Der Kommission die Möglichkeit zu bieten, über Durchführungsrechtsakte⁹² „Angemessenheitsbeschlüsse“ für die Übermittlung nicht personenbezogener Daten an ein bestimmtes Drittland zu erlassen, dürfte auch Fragen des Zusammenwirkens und der Kohärenz mit den in der DSGVO vorgesehenen Mitteln für die Übermittlung personenbezogener Daten an dasselbe Drittland aufwerfen.**
201. **Um die Kohärenz mit dem Datenschutzrechtsrahmen zu gewährleisten, ist es in jedem Fall wichtig, in diesem Zusammenhang daran zu erinnern, dass im Falle von „gemischten Datensätzen“ die DSGVO und insbesondere deren Kapitel V gelten.**
202. Der EDSA und der EDSB merken an, dass sich Artikel 30 des Vorschlags⁹³ nur auf nicht personenbezogene Daten bezieht und in dessen Absatz 2 offenbar die Bestimmungen von Artikel 48 DSGVO aufgegriffen werden (mit dem Unterschied, dass mit Artikel 30 Absatz 2 eine zeitliche Einschränkung in Bezug auf die betreffenden internationalen Übereinkünfte eingeführt wird).
203. Gemäß Artikel 30 Absatz 3 des Vorschlags muss die Stelle (die öffentliche Stelle, die Stelle, der die Weiterverwendung gewährt wurde, der Anbieter von Diensten für die gemeinsame Datennutzung, die datenaltruistische Organisation), die von einem Gericht oder einer Verwaltungsbehörde eines Drittlands eine Entscheidung über die Übermittlung von oder den Zugang zu nicht personenbezogenen Daten aus der Union erhält, die Stellungnahme der gemäß dem Vorschlag zuständigen Behörden oder Stellen einholen, um festzustellen, ob die anzuwendenden Übermittlungsbedingungen erfüllt sind (Artikel 30 Absatz 3 letzter Satz).
204. Die Konsultation der zuständigen Behörde ist erforderlich, wenn die Entscheidung des Gerichts oder der Verwaltungsbehörde des Drittlands „den Adressaten in Widerspruch zum Unionsrecht oder zum Recht des betreffenden Mitgliedstaats bringen“ würde (Artikel 30 Absatz 3).⁹⁴

verpflichtet, a) die gemäß den Absätzen 7 bis 8 auferlegten Verpflichtungen auch nach der Übermittlung der Daten in das Drittland weiterhin zu erfüllen und b) die Zuständigkeit der Gerichte des Mitgliedstaats der öffentlichen Stelle für alle Streitigkeiten im Zusammenhang mit der Erfüllung der Verpflichtung nach Buchstabe a) anzuerkennen.“

⁹⁰ Siehe Erwägungsgrund 19 des Vorschlags.

⁹¹ Siehe Erwägungsgrund 19 des Vorschlags.

⁹² Siehe Artikel 5 Absätze 9 bis 11 des Vorschlags.

⁹³ Artikel 30: Internationaler Zugang, in Kapitel VIII, Schlussbestimmungen, enthalten.

⁹⁴ Die vorgenannten Bedingungen in Artikel 30 Absatz 3 scheinen ausreichend zu sein, um **an die Stelle der Bedingungen in Absatz 2 zu treten und somit die in diesem Absatz genannte internationale Regelung zu ersetzen**. In Artikel 30 Absatz 4 heißt es: „Sind die Bedingungen des Absatzes 2 **oder 3** nicht erfüllt, so **überträgt die öffentliche Stelle, die natürliche oder juristische Person, der das Recht auf Weiterverwendung von Daten nach Kapitel 2 gewährt wurde, der Anbieter von Diensten für die gemeinsame Datennutzung oder die im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung** aufgrund einer

205. Diese Bestimmung scheint im Vergleich zu Artikel 48 DSGVO einen Schritt weiter zu gehen, indem sie in bestimmten Fällen die Konsultation der zuständigen Behörde vorschreibt. Daher könnte sie so aufgefasst werden, als würde sie in gewisser Weise nicht personenbezogene Daten besser schützen als personenbezogene Daten, da eine solche Stellungnahme in der DSGVO nicht vorgesehen ist.

3.7 Horizontale Bestimmungen zu institutionellen Rahmenbedingungen; Beschwerden; Expertengruppe des Europäischen Dateninnovationsrats; delegierte Rechtsakte; Sanktionen, Bewertung und Überprüfung, Änderungen der Verordnung über ein einheitliches digitales Zugangstor, Übergangsmaßnahmen und Inkrafttreten

3.7.1 Artikel 23: Anforderungen an zuständige Behörden

206. Kapitel V des Vorschlags enthält die Anforderungen an die Arbeitsweise der zuständigen Behörden, die für die Überwachung und Umsetzung des Anmelderahmens für Anbieter von Diensten für die gemeinsame Datennutzung und für Datenaltruismus betreibende Einrichtungen benannt wurden. Aus den Kapiteln III und IV des Vorschlags geht hervor, dass sich diese zuständigen Behörden von den Datenschutzbehörden unterscheiden. Die in Artikel 23 des Vorschlags festgelegten Anforderungen legen eine „technische“ Charakteristik dieser Behörden nahe, indem sie „von allen Anbietern von Diensten für die gemeinsame Datennutzung und allen im Register der anerkannten datenaltruistischen Organisationen eingetragenen Einrichtungen rechtlich getrennt und funktional unabhängig sein“ müssen.
207. In dieser Hinsicht scheint die Rolle der Datenschutzaufsichtsbehörden – nach Kapitel III – auf einen bloßen Informationsaustausch mit der zuständigen Behörde und – nach Kapitel IV – auf die Zusammenarbeit mit Letzterer und, auf deren Ersuchen, auf die Abgabe einer Stellungnahme oder Entscheidung zu Fragen, die eine Bewertung der Einhaltung der DSGVO erfordern, beschränkt zu sein. Darüber hinaus ist in dem Vorschlag nicht festgelegt, wie und in welchem Umfang die Datenschutzbehörden mit diesen zuständigen Behörden zusammenarbeiten werden und welche finanziellen und personellen Ressourcen vorgesehen sind, damit die Datenschutzbehörden die für eine solche Zusammenarbeit erforderlichen Aufgaben erfüllen können.
208. Der EDSA und der EDSB merken an, dass viele Bestimmungen des Vorschlags, deren Überwachung den nach den Artikeln 12 und 20 benannten zuständigen Behörden übertragen wird, den Schutz

vertretbaren Auslegung des Ersuchens **nur die auf das Ersuchen hin zulässige Mindestmenge an Daten.**“ (Fettdruck hinzugefügt).

Diese Bestimmungen des Vorschlags könnten **mit anderen Rechtsvorschriften der Union oder der Mitgliedstaaten, insbesondere im Bereich der justiziellen Zusammenarbeit in Straf- oder Zivilsachen, unvereinbar sein.** Diese Anmerkung gewinnt dadurch an datenschutzrechtlicher Bedeutung, dass **im Falle einer Missdeutung des Begriffs „nicht personenbezogene Daten“ ein hohes Risiko besteht, dass öffentliche Stellen, Anbieter von Diensten für die gemeinsame Datennutzung, datenaltruistische Organisationen, Weiterverwender von Daten und Datennutzer personenbezogene Daten in ein Drittland mit einem (deutlich) niedrigeren Schutzstandard für die betroffenen Personen übermitteln.**

personenbezogener Daten betreffen. Aus diesem Grund **betonen der EDSA und der EDSB, dass die Zuständigkeiten und Befugnisse der unabhängigen Aufsichtsbehörden in vollem Umfang zu respektieren sind, da sie mit der Verantwortung betraut sind, die Grundrechte und Grundfreiheiten natürlicher Personen im Zusammenhang mit der Verarbeitung zu schützen und den freien Verkehr personenbezogener Daten zu erleichtern, wie dies in der DSGVO und der EU-DSVO im Einklang mit Artikel 16 AEUV und Artikel 8 der Charta sowie in Übereinstimmung mit der einschlägigen Rechtsprechung des Gerichtshofs der Europäischen Union⁹⁵ festgelegt ist. In Anbetracht der obigen Ausführungen empfehlen der EDSA und der EDSB, im Vorschlag ausdrücklich anzuerkennen, dass, soweit es um personenbezogene Daten geht, die Datenschutzbehörden – erforderlichenfalls in Absprache mit anderen einschlägigen Fachbehörden – die wichtigsten zuständigen Behörden für die Überwachung der Einhaltung der Bestimmungen in Kapitel III und IV des Vorschlags sind. Wie bereits betont, sollten diesen Behörden angemessene Ressourcen zur Verfügung gestellt werden, damit sie die erforderliche Überwachung wirksam und effizient durchführen können.**

3.7.2 Artikel 24: Beschwerden; Artikel 25: Recht auf wirksamen gerichtlichen Rechtsbehelf

209. Der EDSA und der EDSB merken an, dass Artikel 24 Folgendes vorsieht: *„Natürliche und juristische Personen haben das Recht, bei der jeweiligen nationalen zuständigen Behörde Beschwerde gegen einen Anbieter von Diensten für die gemeinsame Datennutzung oder gegen eine im Register der anerkannten datenaltruistischen Organisationen eingetragene Einrichtung einzulegen.“* Dabei wird jedoch der mögliche Inhalt der Beschwerde (nämlich gegen welche Bestimmung des Vorschlags verstoßen wurde) nicht angegeben. Auch scheint es, dass Beschwerden gegen öffentliche Stellen oder Weiterverwender, auf die in Kapitel II des Vorschlags Bezug genommen wird, nicht möglich sind, da dies in Artikel 24 des Vorschlags nicht vorgesehen ist.
210. Darüber hinaus enthält Artikel 25 das Recht auf einen wirksamen gerichtlichen Rechtsbehelf für jede betroffene natürliche oder juristische Person in Bezug auf Untätigkeit im Anschluss an eine bei der zuständigen Behörde eingereichte Beschwerde sowie in Bezug auf Entscheidungen der in den Artikeln 13, 17 und 21 genannten zuständigen Behörden (Entscheidungen über die Überwachung von Diensten für die gemeinsame Datennutzung, die Eintragung von datenaltruistischen Organisationen, die Überwachung der Einhaltung der Vorschriften durch im Register eingetragene datenaltruistische Organisationen).
211. Der EDSA und der EDSB stellen fest, dass sich durch die genannten Bestimmungen des Vorschlags über das Recht, bei der jeweils zuständigen nationalen Behörde eine Beschwerde einzulegen (Artikel 24), und über das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen Untätigkeit oder Entscheidungen der genannten zuständigen Behörde (Artikel 25) das in dieser Stellungnahme bereits hervorgehobene Risiko erhöhen könnte, dass zwischen der DSGVO und dem Vorschlag parallele und unvereinbare Regelungen bestehen. So würden beispielsweise Beschwerden im Zusammenhang mit Vermittlungsdiensten, die betroffenen Personen Mittel zur Ausübung der in der DSGVO vorgesehenen

⁹⁵ Siehe unter anderem das Urteil des EuGH vom 9. März 2010, Europäische Kommission/Bundesrepublik Deutschland, C-518/07, abrufbar unter: <http://curia.europa.eu/juris/liste.jsf?language=de&num=C-518/07>. In seinem Urteil vom 9. März 2010 befand der Gerichtshof, dass die Datenschutzbehörden frei von jeglicher, direkter oder indirekter externer Einflussnahme sein sollten. Das bloße Risiko einer externen Einflussnahme reicht aus, um zu dem Schluss zu kommen, dass die Datenschutzbehörde nicht völlig unabhängig handeln kann.

Rechte zur Verfügung stellen (siehe Artikel 9 Absatz 1 Buchstabe b), dem Vorschlag zufolge in den Zuständigkeitsbereich der zuständigen Behörden fallen. Anders ausgedrückt: Die Unstimmigkeiten und Überschneidungen im „materiellen Recht“ würden auch in Überschneidungen der Zuständigkeiten bei administrativen und gerichtlichen Verfahren „ausufern“.

212. Aus diesem Grund **fordern der EDSA und der EDSB eine klare, unmissverständliche und strenge Definition der materiellrechtlichen Bestimmungen des Vorschlags, deren Aufsicht den zuständigen Behörden übertragen wird, sowie des Überwachungsmechanismus, der eine volle Einhaltung der DSGVO sicherstellt.**

3.7.3 Artikel 26 und 27: Zusammensetzung und Aufgaben der Expertengruppe des Europäischen Dateninnovationsrats

213. Mit Kapitel VI des Vorschlags *„wird eine formale Expertengruppe (der ‚Europäische Dateninnovationsrat‘) eingesetzt, die die Entwicklung bewährter Verfahren durch die Behörden der Mitgliedstaaten erleichtern wird, insbesondere mit Blick auf die Bearbeitung von Anträgen auf Weiterverwendung von Daten, die den Rechten anderer unterliegen (gemäß Kapitel II), die Sicherstellung einer einheitlichen Vorgehensweise in Bezug auf den Anmelderahmen für die Anbieter von Diensten für die gemeinsame Datennutzung (Kapitel III) und den Datenaltruismus (Kapitel IV). Darüber hinaus wird die formal eingesetzte Expertengruppe die Kommission bei der Steuerung der sektorübergreifenden Normung und der Ausarbeitung strategischer sektorübergreifender Normungsaufträge unterstützen und beraten.“*⁹⁶
214. Der EDSA und der EDSB merken an, dass der neu eingerichtete Europäische Dateninnovationsrat, der *„sich aus Vertretern der zuständigen Behörden aller Mitgliedstaaten, des Europäischen Datenschutzausschusses, der Kommission, einschlägiger Datenräume und anderen Vertretern zuständiger Fachbehörden zusammensetzt“* (Artikel 26 Absatz 1), mit den in Artikel 27 Buchstaben a bis e ⁹⁷ aufgeführten Aufgaben betraut würde, die auch im Hinblick auf die Verarbeitung personenbezogener Daten von Belang sind.

⁹⁶ Begründung, Seite 8.

⁹⁷ „Der Innovationsrat hat folgende Aufgaben:

- a) Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis der öffentlichen Stellen und der in Artikel 7 Absatz 1 genannten zuständigen Stellen, die **Anträge auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien bearbeiten**;
- b) Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis der zuständigen Behörden bei der Anwendung der **Anforderungen, die für Anbieter von Diensten für die gemeinsame Datennutzung gelten**;
- c) Beratung der Kommission bei der **Festlegung von Prioritäten für die Verwendung bzw. Entwicklung sektorübergreifender Normen für die Datennutzung und sektorübergreifende gemeinsame Datennutzung** sowie für den sektorübergreifenden Vergleich und Austausch bewährter Verfahren in Bezug auf Sicherheitsanforderungen und Zugangsverfahren in bestimmten Sektoren, wobei sektorspezifische Normungstätigkeiten zu berücksichtigen sind;
- d) Unterstützung der Kommission bei der **Verbesserung der Interoperabilität von Daten sowie von Diensten für die gemeinsame Datennutzung** zwischen verschiedenen Sektoren und Bereichen auf der Grundlage bestehender europäischer, internationaler oder nationaler Normen;

215. Der EDSA und der EDSB begrüßen die Aufnahme des EDSA als Mitglied des Europäischen Dateninnovationsrats. Der EDSA und der EDSB sind jedoch der Ansicht, dass die auf den Europäischen Dateninnovationsrat bezogenen Bestimmungen, insbesondere dann, wenn sie sich auf die Verarbeitung personenbezogener Daten beziehen, wahrscheinlich einen Eingriff in die Aufgaben und Zuständigkeiten der nationalen Datenschutzbehörden und des EDSA darstellen, die dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und der Erleichterung des freien Verkehrs personenbezogener Daten in der Union⁹⁸ dienen (vor allem unter Berücksichtigung des breiten Aufgabenspektrums, mit dem der EDSA nach Artikel 70 DSGVO betraut ist, nämlich die Kommission zu beraten und Leitlinien, Empfehlungen und bewährte Verfahren herauszugeben, sowie in Anbetracht der Aufgaben, mit denen der EDSB nach Artikel 57 EU-DSVO betraut ist).
216. Daher empfehlen der EDSA und der EDSB, im verfügbaren Teil klarzustellen, dass dann, wenn es um die Verarbeitung personenbezogener Daten geht, die nach nationalem und Unionsrecht eingerichteten Datenschutzaufsichtsbehörden die „zuständige Behörde“ sind. Darüber hinaus sollte klargestellt werden, dass die Beratung der Europäischen Kommission in Datenschutzfragen und die Entwicklung kohärenter Verfahrensweisen im Zusammenhang mit der Verarbeitung personenbezogener Daten nicht in den Zuständigkeitsbereich des Europäischen Dateninnovationsrats fallen, da Artikel 70 DSGVO diese Aufgaben ausdrücklich dem EDSA überträgt.
217. Aus Gründen der Präzision und Rechtsklarheit sowie zur Vermeidung möglicher Missverständnisse empfehlen der EDSA und der EDSB außerdem, den Europäischen Dateninnovationsrat in „Expertengruppe der Kommission für Daten-Governance“ oder ähnlich umzubenennen, um den *Rechtsstatus* und den *Charakter* des nach Artikel 26 des Vorschlags eingesetzten Gremiums besser zu vermitteln.

3.7.4 Artikel 31: anzuwendende Sanktionen bei Verstößen gegen die vorgeschlagene Verordnung

218. Im Vorschlag sind die Sanktionen für Verstöße gegen die vorgeschlagene Verordnung nicht harmonisiert (und auch nicht festgelegt, welche Verstöße zu ahnden sind, welche Geldbußen bei Verstößen gegen die Bestimmungen zu verhängen sind und welche Behörden oder Stellen für die Verhängung solcher Sanktionen zuständig sind), sondern es ist Folgendes vorgesehen: *„Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diese Verordnung zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum [Beginn der Anwendung dieser Verordnung] mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.“*

e) Erleichterung der Zusammenarbeit zwischen den zuständigen nationalen Behörden im Rahmen dieser Verordnung mittels Kapazitätsaufbau und Informationsaustausch, insbesondere durch die Festlegung von Methoden für einen effizienten Informationsaustausch über das Anmeldeverfahren für Anbieter von Diensten für die gemeinsame Datennutzung und die Eintragung und Überwachung anerkannter datenaltruistischer Organisationen.“

⁹⁸ Siehe beispielsweise Artikel 27 Buchstabe a, demzufolge der Innovationsrat die Aufgabe hat „Beratung und Unterstützung der Kommission bei der Entwicklung einer einheitlichen Praxis der öffentlichen Stellen und der in Artikel 7 Absatz 1 genannten zuständigen Stellen, die Anträge auf Weiterverwendung von Daten der in Artikel 3 Absatz 1 genannten Datenkategorien bearbeiten“, zu leisten (Hervorhebung hinzugefügt).

219. Der EDSA und der EDSB merken an, dass diese Bestimmung, die die Durchsetzbarkeit des Vorschlags (die Möglichkeit, harmonisierte Sanktionen zu verhängen) einschränkt und möglicherweise auch die „Wahl des günstigsten Gerichtsstands“ im nachsichtigsten Mitgliedstaat begünstigt, dem erklärten Ziel des Vorschlags abträglich ist, demzufolge das Vertrauen in die Weiterverwendung, die Dienste für die gemeinsame Datennutzung und den Datenaltruismus gestärkt werden soll.

3.7.5 Artikel 33: Änderung der Verordnung (EU) 2018/1724

220. Mit diesem Artikel des Vorschlags wird die Verordnung über ein einheitliches digitales Zugangstor (Verordnung (EU) 2018/1724)⁹⁹ geändert, indem die folgenden Verwaltungsverfahren eingeführt werden: Anmeldung als Anbieter von Diensten für die gemeinsame Datennutzung, Eintragung als europäische datenaltruistische Organisation. Das erwartete Ergebnis besteht in der Bestätigung des Eingangs der Anmeldung bzw. in der Bestätigung der Eintragung.
221. **Diesbezüglich stellen der EDSA und der EDSB fest, dass die bereits in dieser Stellungnahme geprüften Anmelde- und Eintragungsregelungen kein Ersatz dafür sein können, dass eine geeignete Rechtsgrundlage für die Verarbeitung personenbezogener Daten nach Artikel 6 Absatz 1 DSGVO erforderlich ist, damit die Datenverarbeitung rechtmäßig ist. Mit anderen Worten: Nach der DSGVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn und soweit eine geeignete Rechtsgrundlage nach Artikel 6 Absatz 1 DSGVO gegeben ist. Im Vorschlag sollte dieser Punkt deutlich formuliert werden, um jegliche Unklarheit zu vermeiden.**

Brüssel, 10. März 2021

Für den Europäischen Datenschutzausschuss

Die Vorsitzende

(Andrea Jelinek)

Für den Europäischen Datenschutzbeauftragten

Der Europäische Datenschutzbeauftragte

(Wojciech Wiewiórowski)

⁹⁹ Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (Text von Bedeutung für den EWR.) (ABl. L 295 vom 21.11.2018, S. 1).