Die Bundesregierung

Vorläufige Stellungnahme der Bundesrepublik Deutschland

zum Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz) COM (2020) 767 final

Die Bundesregierung begrüßt grundsätzlich die Vorlage des Verordnungsentwurfs der KOM. Mit dem Data-Governance-Gesetz setzt die KOM ein Vorhaben der EU Datenstrategie vom Februar 2020 um. Die verstärkte Nutzbarmachung bereits vorhandener Daten ist ein wichtiges Instrument zur Stärkung der Innovationskraft europäischer Volkswirtschaften, zur Schaffung eines europäischen Binnenmarkts für Daten und zur Förderung von zentralen Gemeinwohlbelangen sowie von Wissenschaft und Forschung. Die Harmonisierung der Bedingungen für die Weiterverwendung von Daten des öffentlichen Sektors ebenso wie Anforderungen für Dienste für die gemeinsame Datennutzung und für datenaltruistische Organisationen spielt eine besondere Rolle für die Erreichung dieser Ziele.

Diese vorläufige Stellungnahme ist das Ergebnis einer ersten Prüfung und Bewertung des VO-Entwurfs. Die Bundesregierung behält sich ausdrücklich die Ergänzung weiterer Fragen oder Anmerkungen vor.

Der Vorschlag steht im Einklang mit der Datenstrategie der Bundesregierung. Die Strategie zielt insbesondere darauf ab, die Datennutzung für sämtliche Akteure zu steigern. Der Bundesregierung ist besonders wichtig, Verfahren möglichst bürokratiearm auszugestalten und Kosten für Unternehmen zu vermeiden. Die Bundesregierung befürwortet die Nutzung der Vorteile und des Innovationspotentials von Daten, insbesondere zu Gunsten der Forschung. Dieses Potenzial wollen wir insbesondere für KMU und Forschungsinstitutionen sowie staatliche Einrichtungen in Bezug auf ihre Aufgabe der öffentlichen Daseinsvorsorge erschließen.

...

Für die Bundesregierung ist die Bewahrung des bestehenden hohen Schutzniveaus, insbesondere in den Bereichen Geschäftsgeheimnisse, dem Schutz personenbezogener Daten und dem geistigen Eigentum sowie die Sicherung einer gerechten Teilhabe, die Verhinderung von Datenmonopolen und die konsequente Begegnung von Datenmissbrauch von besonderer Bedeutung. Die Bundesregierung setzt sich dafür ein, dass der Vorschlag mit der Position der EU im internationalen Rahmen kohärent ist.

Ein wesentlicher Kritikpunkt am Verordnungsvorschlag betrifft das systematische Verhältnis zu anderen EU-Rechtsakten und zu Rechtsakten der Mitgliedsstaaten, welches nach Ansicht der Bundesregierung an vielen Stellen ungeklärt bleibt. Dies gilt insbesondere, jedoch nicht ausschließlich, in Hinblick auf die Datenschutzgrundverordnung (DSGVO, Verordnung (EU) 2016/679) und zum bereichsspezifischen Datenschutzrecht der Mitgliedsstaaten. Zwar wird im Verordnungsentwurf festgehalten, dass dieser die Regelungen der DSGVO unberührt lassen möchte. Gleichwohl kommt es trotz der Unberührtheitserklärung bei grundlegenden Fragen zu Überschneidungen, Widersprüchen, begrifflichen Inkohärenzen oder Regelungslücken. Es muss geprüft werden, ob und wie die Regelungen im Einklang mit der DSGVO umgesetzt werden können. Außerdem sollte klargestellt werden, wie die datenrelevanten europäischen Rechtsnormen kohärent ineinandergreifen, die Regelungen der DSGVO nicht unterlaufen sowie das Schutzniveau und die Handlungsspielräume der DSGVO gewahrt werden.

Vor diesem Hintergrund wird die Kommission gebeten, eine „Landkarte der datenrelevanten europäischen Rechtsnormen“ vorzulegen, aus welcher insbesondere Zielstellungen, Regelungsadressaten und Regelungsgegenstände transparent hervorgehen. Neben der DSGVO und dem bereichsspezifischem Datenschutzrecht sollten dabei u.a. auch die Open-Data/PSI-Richtlinie (Richtlinie 2019/1024), die Richtlinie zum Schutz von Geschäftsgeheimnissen, Verordnung 2018/1807 über den Rahmen für den freien Verkehr nicht-personenbezogener Daten und das Verhältnis dieser Verordnung zur ePrivacy-Richtlinie (Richtlinie 2002/58/EG) berücksichtigt werden. Auch geplante Rechtsakte sollten in diese „Landkarte der datenrelevanten europäischen Rechtsnormen“ aufgenommen werden.

Darüber hinaus sollte eine Handreichung erstellt werden, die denkbare Fallkonstellationen mehrerer Themengebiete anhand der datenrelevanten Rechtsnormen durchspielt, um den Regelungsadressaten die Anwendung der Verordnung zu erleichtern.

In ihrer Gesetzgebung muss die EU die internationale Dimension mitdenken. Die EU-Datengesetzgebung muss bestehende internationale Verpflichtungen der EU wahren. Sie muss kohärent sein mit den Positionen der EU in bilateralen, plurilateralen und multilateralen Verhandlungen und ihrem Eintreten für offene Märkte und gegen ungerechtfertigte Handelsbeschränkungen, um die Glaubwürdigkeit der EU nicht zu beschädigen.

Schließlich sind die vorgesehenen Maßnahmen vor einer konkreten Umsetzung darauf zu prüfen, dass durch ihre flächendeckende Einführung die digitale Souveränität Europas oder einzelner Mitgliedsstaaten nicht beeinträchtigt wird.

Auch im Einzelnen besteht teilweise erheblicher Klarstellungs-, Änderungs- und Ergänzungsbedarf. Dies betrifft u.a. Begriffsbestimmungen, rechtssystematische Fragen und Besonderheiten der Forschung. Kritisch zu hinterfragen ist zudem der durch die Regelungen entstehende Bürokratie- und Verwaltungsbedarf. Dieser sollte sich in einem verhältnismäßigen Rahmen bewegen. Die spezifischen Anforderungen an eine digitale Verwaltung sind zu berücksichtigen (z.B. für eine wirksame Bekämpfung von Steuerbetrug und Geldwäsche in einer globalen digitalen Welt). Auch vor diesem Hintergrund ist aus Sicht der Bundesregierung bei einzelnen Regelungen nach der Erforderlichkeit und Verhältnismäßigkeit zu fragen. Es sollte sichergestellt sein, dass die Maßnahmen praktikabel sind und die Nutzung von Daten tatsächlich erleichtern. Auch deswegen wird dafür plädiert, die Anzahl der involvierten nationalen Stellen und Behörden möglichst gering zu halten bzw. neue Aufgaben auf europäischer Ebene zu bündeln.

Im Einzelnen:

1. Kapitel I „Allgemeine Bestimmungen“

Die Anmerkungen und Änderungswünsche zu diesem Kapitel haben insbesondere den Anwendungsbereich, das Verhältnis des Regelungsvorschlags zu anderen EU-Rechtsakten und unklare Begriffsbestimmungen zum Gegenstand. Die Unberührtheitsklausel in Art. 1 Abs. 2 VO-Entwurf sieht vor, dass die besonderen Bestimmungen anderer EU-Rechtsakte über den Zugang oder die Weiterverwendung von bestimmten Kategorien von Daten oder die Anforderungen an die Verarbeitung personenbezogener oder nicht-personenbezogener Daten unberührt bleiben. Die Bundesregierung begrüßt dies ausdrücklich und hält dies für eine zentrale Grundvoraussetzung, dass die datenschutzrechtlichen Bestimmungen insbesondere der DSGVO von dem VO-Entwurf unberührt bleiben.

Es bleibt jedoch nicht nur unklar, wie sich das Verhältnis dieser allgemeinen Unberührtheitsklausel in Art. 1 Abs. 2 VO-E zu der spezifischer für Kapitel II geltenden Unberührtheitsklausel in Art. 3 Abs. 2 VO-E darstellt. Auch in der Sache wirft die Unberührtheitsklausel sowie der zugehörige Erwägungsgrund 3 zahlreiche Fragen zum Verhältnis des vorliegenden VO-Entwurfs zu anderen EU-Rechtsakten sowie zum mitgliedstaatlichen Recht auf, die der Klärung bedürfen:

Verhältnis zur DSGVO und anderen EU-Datenschutzrechtsakten: Die in Art. 1 Abs. 2 VO-Entwurf (im Folgenden: VO-E) enthaltene Klarstellung, dass die Anforderungen in Bezug auf die Verarbeitung personenbezogener Daten sowie sektor-spezifische Unionsvorschriften unberührt

bleiben, lässt viele Fragen offen. Die DSGVO muss insgesamt unberührt bleiben. Ziel muss sein, DSGVO und DGA zu verzahnen. Insbesondere die Zuständigkeiten, Aufgaben und Befugnisse der zuständigen Behörden, einschließlich der unabhängigen Datenschutzbehörden müssen klar abgegrenzt und die Betroffenenrechte gewahrt werden. Das Verhältnis zur JI-Datenschutzrichtlinie (EU) 2016/680 sollte durch Aufnahme einer Artikel 2 Abs. 2 Buchst. d DSGVO entsprechenden Klausel ausdrücklich klargestellt werden, die die dort genannten Daten aus dem Anwendungsbereich ausnimmt.

- **Verhältnis zur Umweltinformationsrichtlinie:** Das Verhältnis zur Umweltinformationsrichtlinie und zur Inspire-Richtlinie muss verdeutlicht werden. Die Unberührtheitsklausel in Art. 1 Abs. 2 VO-Entwurf muss die Umweltinformationsrichtlinie (UI-RL) direkter in Bezug nehmen. Erwägungsgrund 3 muss in der Aufzählung der europäischen Rechtsakte, die von der VO unberührt bleiben, auch die UI-RL und die INSPIRE-RL aufnehmen. Anderenfalls ist für den Rechtsanwender nur schwer zu erkennen, welche Datenkategorien von der Verordnung unberührt bleiben. Die Liste in Erwägungsgrund 3 darf nicht abschließend formuliert sein.
- **Verhältnis zu anderen sektorspezifischen EU-Rechtsakten betreffend Registerdaten:** Es sollte klargestellt werden, dass andere sektorspezifische Rechtsakte, die für Registerdaten spezielle Regelungen enthalten, insbesondere bspw. für die Daten der Handels- und Unternehmensregister die Gesellschaftsrechtsrichtlinie (RL EU 2017/1132) in der durch die Digitalisierungsrichtlinie (RL EU 2019/1151) geänderten Fassung, der Geldwäscherichtlinie (Richtlinie 2018/843) zu den Transparenzregisterdaten und für die Daten zu Insolvenzverfahren die Verordnung (EU) 2015/848 über Insolvenzverfahren, unberührt bleiben. Andernfalls besteht das Problem sich möglicherweise widersprechender Rechtsakte bereits auf EU-Ebene, da die sonstigen Rechtsakte regelmäßig auch detaillierte Regelungen etwa über den Zugang, das Format, die Speicherung, die Zulässigkeit von Abrufgebühren oder die Nutzung der Registerdaten enthalten. Die vorgenannten Rechtsakte sollte daher ebenfalls ausdrücklich in die Aufzählung anderweitiger sektorspezifischer Rechtsakte in Erwägungsgrund 3 aufgenommen werden.
- **Verhältnis zum bereichsspezifischen Recht der Mitgliedstaaten:** Die in Art. 1 Abs. 2 VO-E enthaltene Unberührtheitsklausel in Bezug auf besondere Bestimmungen anderer Rechtsakte der Union muss gerade mit Blick auf Regelungsbereiche, die der Kompetenz der Mitgliedsstaaten unterliegen (s. z.B. Art. 168 AEUV), um das bereichsspezifische Recht der Mitgliedstaaten ergänzt werden, die im Rahmen der Öffnungsklauseln der DSGVO eingeführt oder beibehalten wurden. Dies gilt z.B. für hochsensible Daten, die im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit zur Erfüllung von gesetzlichen Aufgaben verarbeitet werden (beispielsweise für den in den

Sozialgesetzbüchern geregelten Sozialdatenschutz und weitere bereichsspezifische Regelungen zum Umgang mit besonderen Kategorien von Daten). Auch in der Unberührtheitsklausel von Art. 3 Abs. 3 VO-Entwurf wird auf nationale Rechtsvorschriften Bezug genommen, so dass die Nichterwähnung in Art. 1 Abs. 2 VO-E nicht nachvollziehbar ist. Daher sollte Art. 1 Abs. 2 VO-E sowie der dazu gehörige Erwägungsgrund 3 – insbesondere aus Gründen der Kohärenz – um die sektorspezifischen Regelungen der Mitgliedsstaaten ergänzt werden.

Die **Begriffsbestimmungen** in **Artikel 2 VO-E** sind teilweise unklar gefasst, müssen auf Kohärenz mit den materiellen Regelungen des Entwurfs geprüft oder ergänzt werden. Insbesondere wird die Kommission gebeten, die Abweichungen der Begriffsbestimmungen zur Open-Data/PSI-RL näher zu erläutern.

- **Art. 2 Nr. 2 VO-E:** Die Definition von „Weiterverwendung“ sollte dahingehend ergänzt werden, dass auch der Austausch von Daten zwischen öffentlichen Stellen und internationalen Organisation (z.B. EPO, WIPO, EUIPO) als nicht unter die VO fallende „Weiterverwendung“ qualifiziert wird. Dies gebietet die Zielrichtung der Verordnung. Denn beispielsweise der Austausch zwischen dem Deutschen Patent- und Markenamt und EPA bzw. WIPO dient im Patentbereich dazu, die Recherchetätigkeiten der Prüfer zu verbessern und zu erweitern sowie der Öffentlichkeit den Zugang zu Schutzrechtsdaten beider Ämter zum Zwecke der Schutzrechtsinformation zu ermöglichen.
- **Art. 2 Nr. 5 VO-E:** Es wird um Klarstellung des Begriffs „Dateninhaber“ gebeten. Die Kommission wird gebeten, den Begriff des „Besitzes von Daten“ (vgl. Art. 3 Abs. 1 VO-E) zu vermeiden und einen einheitlichen Wortlaut mit dem Begriff des Dateninhabers/Inhaberschaft („data holder“) auch in der deutschen Sprachfassung zu gewährleisten. Die Verwendung des Begriffs „Dateninhaber“ scheint zudem nicht immer konsistent zu sein bzw. geht der Entwurf möglicherweise von verschiedenen Dateninhabern aus – einmal die öffentliche Stelle und einmal der Betroffene. Die Unterscheidung zwischen Dateninhaberschaft und dem in Art. 3 Abs. 1 VO-E geregelten „Besitz“ an Daten ist bislang nicht klar. Im Einzelnen ist zudem unklar, woraus sich eine „Berechtigung“ zur Zugangsgewährung oder Datenweitergabe ergibt und wer originärer Dateninhaber ist – die Person, die die Daten generiert, oder die Person, die die Daten „betreffen“? Kann die Dateninhaberschaft übertragen werden, und wenn ja, wie? Gibt es eine „Mit-Dateninhaberschaft“? Ab wann sind die Daten der Dateninhaber „unter ihrer Kontrolle“? Bedarf es hier einer faktischen Exklusivität des Zugriffs oder ist eine „geteilte Kontrolle“ möglich? Zudem erschließt sich nicht, warum hier (nur) vom „Dateninhaber“ die Rede ist und nicht wie in Nummer 6 allgemeiner von natürlicher Person. Eine natürliche Person kann auch „Dateninhaber“ sein, ohne selbst betroffene Person zu sein. Es ist darauf zu achten, dass die Begriffsbestimmung sowohl Sachverhalte adäquat erfasst, in

denen ausschließlich nicht-personenbezogene Daten vorliegen, als auch Sachverhalte, in denen es um personenbezogene Daten oder sog. Mischdatensätze geht. Sofern die Annahme zutrifft, dass der in Art. 3 Abs. 1 VO-E erwähnte „Besitz“ an Daten eigentlich „Dateninhaberschaft“ meint, sind diese Fragen für die Anwendbarkeit des Kapitels II von entscheidender Bedeutung.

- **Art. 2 Nr. 6 VO-E:** Eine Präzisierung des Begriffs „Datennutzer“ ist erforderlich, um den Einklang mit dem Datenschutzrecht sicherzustellen. So ist z.B. der Begriff des „rechtmäßigen Zugangs“ missverständlich, da er einen Zugangsanspruch bzw. eine Bereitstellungsverpflichtung suggeriert (vgl. nur Art. 3 Abs. 3 S. 3 VO-Entwurf). Im Regelungsteil wird der Begriff „Datennutzer“ allerdings bislang ausschließlich in Kapitel III verwendet. In Kapitel III geht es aber von vornherein nicht um Zugangsansprüche oder Bereitstellungspflichten, sondern um freiwillige Vereinbarungen über die „gemeinsame Datennutzung“.
- **Art. 2 Nr. 7 VO-E:** Eine Präzisierung des Begriffs „gemeinsame Datennutzung“ ist erforderlich; auch hier ist die Einhaltung der gemeinsamen Datenschutzverantwortlichkeit sicherzustellen.
- **Art. 2 Nr. 8 VO-E:** Eine Präzisierung und kohärente Verwendung des Begriffs „Zugang“ ist erforderlich. „Zugang“ wird hier als ein bestimmter Datenverarbeitungsvorgang definiert. Demgegenüber wird in Art. 7 Abs. 1 der Begriff „Zugang“ eher im Sinne einer Berechtigung verstanden, auf bestimmte Daten zugreifen zu dürfen, um sie sodann zu verarbeiten.
- **Art. 2 Nr. 10 VO-E:** Bezüglich der Definition von „Datenaltruismus“ in Art. 2 Nummer 10 VO-Entwurf wird um Erläuterung zur „Erlaubnis“ zur Nutzung von nicht-personenbezogenen Daten gebeten. Ein Ausschließlichkeitsrecht im Sinne eines „Dateneigentums“ an nicht-personenbezogenen Daten existiert in Deutschland und auch in vielen anderen Mitgliedstaaten nicht. Der Zugang zu Daten hängt indes häufig entscheidend von der technisch-faktischen Kontrolle des Dateninhabers ab. Es sollte klargestellt werden, ob mit „Erlaubnis“ die Einräumung der faktischen Verfügungsgewalt über Daten gemeint ist (also die Übermittlung von Daten) und/oder eine Erlaubnis zum Beispiel im Sinne des Geschäftsgeheimnisrechts, Urheberrechts oder Patentrechts.

  Der Begriff des „allgemeinen Interesses“ erscheint weiter erklärungs- und konkretisierungsbedürftig. So ist auch denkbar, dass relevante Belange nur eine kleine Gruppe von Menschen betreffen, denen aber durch Zugang zu Daten gut geholfen werden könnte (Beispiel: Verwendung de-identifizierter Registerdaten zur Bekämpfung seltener Krankheiten). Es sollte geprüft werden, ob der Begriff „allgemeines Interesse“ durch den Begriff „öffentliches Interesse“ (public interest) ersetzt werden sollte.

- **Art. 2 Nr. 11 und 12 VO-E**: Einrichtungen des öffentlichen Rechts sollen unter den Begriff der öffentlichen Stelle fallen. Es wird um Klärung gebeten, ob auch Berufskammern (Körperschaften des öffentlichen Rechts) unter die Definition des Art. 2 Nr. 12 VO-E fallen. In diesem Zusammenhang ist zu beachten, dass sich Berufskammern, wie z.B. die Bundessteuerberaterkammer, durch Mitgliedsbeiträge selbst finanzieren und nur der Rechtsaufsicht des Staates unterliegen. Klärungsbedürftig erscheint insbesondere die Formulierung des Art. 2 Nr. 12 Buchst. c VO-E.
- **Art. 2 Nr. 14 VO-E:** Ausdrücklich wird unterstützt, dass die öffentliche Stelle die Datenverarbeitungsvorgänge in der sicheren Verarbeitungsumgebung nicht nur „beaufsichtigt", sondern auch dahingehend „bestimmt", welche Verarbeitungsvorgänge zulässig sind und welche nicht. Die derartige „Bestimmung" ist im Normtext von Art. 5 Abs. 5 VO-E, der die materiellen Regelungen zur sicheren Verarbeitungsumgebung enthält, bislang allerdings nicht abgebildet und muss dort ergänzt werden. Außerdem sollten im Normtext oder den Erwägungsgründen Kriterien aufgestellt werden, an denen sich die öffentliche Stelle bei ihrer Bestimmung der zulässigen Verarbeitungsvorgänge orientieren muss. In der Definition von Art. 2 Nr. 14 VO-E sollte zudem ergänzt werden, dass die Beaufsichtigung auch praktisch wirkungsvoll sein muss und dass die sichere Verarbeitungsumgebung so ausgestaltet sein muss, dass die öffentliche Stelle die Ergebnisse der Datenverarbeitungsvorgänge überprüfen kann (vgl. Art. 5 Abs. 5 VO-E).
- In **Art. 2** sollte **darüber hinaus** klargestellt werden, dass die Definitionen der DSGVO für den Anwendungsbereich des VO-E ebenfalls Geltung haben (z.B. die Definition von „Einwilligung").
- Es wird darum gebeten, zudem eine Legaldefinition des Begriffs „Vermittlungsdienste (intermediation services)" in den Katalog des Art. 2 aufzunehmen, der in diesem VO-E eine zentrale Rolle einnimmt (vgl. Erwägungsgrund 22).

2. Kapitel II „Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen"

Die Bundesregierung begrüßt, dass der Vorschlag in Kapitel 2 einen Rahmen für die Nutzung besonders „geschützter Daten im Besitz öffentlicher Stellen" vorsieht und hebt zugleich hervor, dass die Datennutzung in diesem Bereich nur mit einem kohärenten Rechtsrahmen sowie einer vertrauenswürdigen technischen und personellen Infrastruktur in Betracht kommen kann.

Mit den **Forschungsdatenzentren** verfügt Deutschland über langjährige Erfahrung mit der Bereitstellung und Nutzung von Daten, die der statistischen Geheimhaltung unterliegen, für die Zwecke von Wissenschaft und Forschung. Die Bundesregierung begrüßt, dass das bisherige deutsche Modell der Forschungsdatenzentren vom Verordnungsvorschlag aufgegriffen wird. Gleichzeitig geht der Verordnungsvorschlag aber über das Modell der Forschungsdatenzentren

hinaus, indem zum Beispiel auch kommerzielle Formen der Weiterverwendung grundsätzlich erfasst werden. Der Verordnungsvorschlag wirft daher spezifische Fragen auf. Die Bundesregierung möchte mit ihren Erfahrungswerten zu der Entwicklung eines angemessenen europäischen Rahmenwerks beitragen.

Zum Umgang mit Daten im Besitz öffentlicher Stellen, die auf Grund geschäftlicher oder statistischer Geheimhaltung, geistigen Eigentums Dritter oder eines Personenbezugs besonders geschützt sind, stellt sich eine Reihe von Fragen, die der Verordnungsentwurf nicht vollständig klärt. Eine Präzisierung der betroffenen Datenkategorien ist ebenso erforderlich wie eine Klärung des Verhältnisses der Bedingungen zur Weiterverwendung von Daten zu anderen EU-Rechtsakten, insb. der DSGVO und des bereichsspezifischen Datenschutzrechts. Dabei muss auch der Umgang mit Forschungsdaten präzisiert werden.

Ergänzungsbedarf besteht darüber hinaus hinsichtlich des Verhältnisses der „zuständigen Stellen“ zur „zentralen Informationsstelle“.

Nach dem Bekunden der Kommission soll mit Kapitel 2 des VO-E kein weitergehender Zugang zu Daten geschaffen werden (Frage des „ob“), sondern nur die Bedingungen für die Weiterverwendung bereits zugänglicher Daten unionsrechtlich harmonisiert werden (Frage des „wie“). Art. 3 Abs. 3 VO-Entwurf besagt nur, dass das Unionsrecht und nationale Rechtsvorschriften bezüglich des Zugangs und von Weiterverwendungsverpflichtungen unberührt bleiben. Darüber hinaus muss aber auch in geeigneter Weise klargestellt werden, dass der Data Governance Act seinerseits keine eigenen Ansprüche oder Verpflichtungen auf die Bereitstellung von Daten enthält. In der Sache drängt sich jedoch die Frage auf, ob der VO-Entwurf nicht schon weitergehende Zugangsregelungen trifft, wenn er gerichtlich durchsetzbare „Anträge auf Weiterverwendung“ von personenbezogenen oder sonst geschützten Daten schafft (Art. 8 Abs. 3 und 4 VO-E). Die Kommission wird dazu um Erläuterung gebeten.

Die Bundesregierung sieht – wie auch in ihrer Datenstrategie beschlossen – gleichzeitig eine **verbesserte Zugänglichkeit zu Daten** für wesentlich an, um die Ziele einer gesteigerten Datenbereitstellung und -nutzung für sämtliche Akteure zu erreichen. In ihrer Datenstrategie hat die Bundesregierung daher beschlossen, bei neuen Gesetzgebungsvorhaben künftig zu prüfen, in welchem Umfang forschungsfreundliche, barrierefreie Zugangsregelungen (sog. Forschungsklauseln) für die unabhängige wissenschaftliche Forschung geschaffen werden können. **Sie fordert die Kommission auf, in ihren künftigen Gesetzgebungsvorschlägen diese Forschungsbelange angemessen zu berücksichtigen**. Forschung und Wissenschaft sind unerlässlich, um die Datenbestände jenseits von Individualinteressen besser für Gemeinwohl und Wohlstand nutzen und die Risiken minimieren zu können. Der Zugang zu wichtigen Datenbeständen und -verknüpfungen ist für die Wissenschaft aber bisher oftmals nur sehr eingeschränkt. Die Bundesregierung bittet die Kommission um eine Konkretisierung der

Zeitplanung und der geplanten Inhalte des angekündigten Datengesetzes, um die Kohärenz mit dem Data Governance Act zu gewährleisten.

Eingedenk der Tatsache, dass keine Zugangsrechte mit dem Data Governance Act geschaffen werden, sollte der Data Governance Act mit forschungsfreundlichen und möglichst barrierefreien Regeln für die unabhängige wissenschaftliche Forschung ausgestaltet werden.

In einzelnen Artikeln zeigt sich dieser Klärungsbedarf wie folgt:

Art. 3 VO-E:

- **Art. 3 Abs. 1 VO-E:** Es wird darauf hingewiesen, dass für viele Daten eine zeit- und kostenintensive Prüfung erforderlich ist, um festzustellen, ob es sich um urheberrechtlich oder in anderer Weise geschützte Daten handelt. Für ein einheitliches Verständnis sollte bei Daten mit geschäftlicher und statistischer Geheimhaltung eine gesetzliche Inbezugnahme dieser Schutzgründe zugrunde gelegt werden, d.h. bei Daten mit geschäftlicher Geheimhaltung insbesondere die Richtlinie (EU) 2016/943 und bei statistischer Geheimhaltung entsprechende Spezialgesetze. Entsprechende Klarstellungen sollten zumindest in den Erwägungsgründen vorgenommen werden.
- **Art. 3 Abs. 1 Buchst. a VO-E:** Es muss geklärt werden, ob die Definition der „geschäftlichen Geheimhaltung" der des „Geschäftsgeheimnisses" in der Richtlinie (EU) 2016/943 entspricht und damit auch Berufsgeheimnisse umfasst. Weiter stellt sich die Frage, unter welchen Bedingungen eine Weiterverwendung von Geschäftsgeheimnissen in Einklang mit der Richtlinie (EU) 2016/943 zulässig sein kann und wie dieser Prozess in der Praxis konkret erfolgen kann – insbesondere ohne dass damit ein Verlust der Einstufung als Geschäftsgeheimnis einhergeht. Gemäß Erwägungsgrund 7 soll die Weiterverwendung von Daten, die möglicherweise Geschäftsgeheimnisse enthalten, unbeschadet der Richtlinie (EU) 2016/943 erfolgen, die den Rahmen für die Rechtmäßigkeit von Erwerb, Nutzung oder Offenlegung von Geschäftsgeheimnissen festlegt. Nach hiesigem Verständnis dürfte eine Preisgabe nur mit Einwilligung des Inhabers zulässig sein. Im Falle einer vorbehaltlosen Einwilligung in die Preisgabe durch den Inhaber dürften die Daten aber ihren Charakter als Geschäftsgeheimnis verlieren (*e contrario* Art. 2 Abs. 1 Buchst. c Richtlinie 2016/943: „Geschäftsgeheimnisse müssen Gegenstand angemessener Geheimhaltungsmaßnahmen sein").
- **Art. 3 Abs. 1 Buchst. b VO-E:** Unklar bleibt, wie die Privilegierung der Datenverarbeitung zu statistischen Zwecken und die Verpflichtung natürlicher Personen und Unternehmen zu umfangreichen Angaben zur statistischen Erhebung weiter gerechtfertigt werden können, wenn Daten, die dem Statistikgeheimnis unterliegen, von Dritten - auch privaten Dritten - zu anderen Zwecken weiterverwendet werden dürfen (s. oben).

- **Art. 3 Abs. 2 Buchst. c VO-E:** Es stellt sich die Frage, ob die Bereichsausnahme für Bildungseinrichtungen auf universitäre Forschung sowie außeruniversitäre Forschungseinrichtungen ausgeweitet werden sollte. Nach aktuellem Stand können diese Einrichtungen des öffentlichen Rechts (Art. 2 Nr. 11 VO-E) oder öffentliche Unternehmen sein (Art. 2 Nr. 12 VO-E), aber auch privatrechtlich organisiert sein. Nach der jetzigen Textfassung bestehen erhebliche Abgrenzungsprobleme.
- **Art. 3 Abs. 2 Buchst. d VO-E** knüpft – anders als Buchst. a bis c – nicht an den Besitz an. Das könnte dahingehend ausgelegt werden, dass bei Buchst. d bei Herausgabeverlangen Dritter ein besonderes Begründungsbedürfnis für diese Daten durch die besitzende Stelle (z. B. der Nachrichtendienste) erforderlich ist. Wäre es im Hinblick auf Art. 4 Abs. 2 EUV, der die nationale Sicherheit in der Zuständigkeit der Mitgliedstaaten belässt, möglich, Buchst. d insoweit klarer zu fassen?
- Aus Sicht der Bundesregierung sollte im Normtext oder den Erwägungsgründen, etwa zum allgemeinen Anwendungsbereich oder zu Artikel 3 Absatz 3, ausdrücklich klargestellt werden, dass es jedem Mitgliedstaat überlassen bleiben muss, den Zugang oder die Erlaubnis der Weiterverwendung insbesondere in Bezug auf Registerdaten zu bestimmen. Die VO darf nur dann auf Registerdaten anwendbar sein, wenn und soweit – auch hinsichtlich der gesetzlich bestimmten Zwecke und des Umfangs – nach nationalem Recht ein Zugang zu den geschützten Daten eröffnet und ihre Weiterverwendung im Sinne des Art. 2 Nr. 2 VO-E erlaubt ist.
- In Deutschland werden sehr sensible Daten in den Registern u.a. der Sozial- und Steuerverwaltung, den Handels-, Genossenschafts-, Partnerschafts-, Vereins-, Transparenz- und Unternehmensregistern, dem Insolvenzregister und Ausländerzentralregister vorgehalten. Die betroffenen Personen müssen diese Daten aufgrund verpflichtender Vorgaben in Rechtsvorschriften regelmäßig nur zu bestimmten Zwecken bereitstellen, etwa um dem Informationsinteresse des Rechtsverkehrs im Einzelfall Rechnung zu tragen, nicht aber für eine Weiterverwendung zu jedem anderen kommerziellen oder nicht-kommerziellen Zweck durch dritte Personen.
- Unter anderem das Bundeszentral-, das Gewerbezentralregister und das Zentrale staatsanwaltliche Verfahrensregister dienen außerdem rechts- und sicherheitspolitischen Zwecken und unterliegen deshalb aufgrund des sensiblen Datenbestands besonderen fachlichen Anforderungen und Zugangsbeschränkungen. Die Bundesregierung geht davon aus, dass diese genannten Register gem. Art. 3 Abs. 2 Buchst. d (öffentliche Sicherheit) nicht den Regelungen des Kapitels II unterfallen.
- **Art. 4 VO-E:** Es ist zu prüfen, ob das Verbot von Ausschließlichkeitsvereinbarungen für Forschungseinrichtungen angemessen ist. Forschungseinrichtungen arbeiten mit einer Vielzahl von Kooperationsmodellen. Insbesondere im Bereich klinischer Prüfungen für die Entwicklung und Zulassung von Arzneimitteln werden Forschungseinrichtungen als

Prüfzentrum tätig und können Ausschließlichkeitsvereinbarungen nicht verhindern. Ebenso dürfte ein Großteil der Auftragsforschung Ausschließlichkeitsvereinbarungen enthalten, die nicht verzichtbar sind. Für Forschungsdaten hat sich seit Jahren das Modell des Datennutzungsvertrages international etabliert. Es ist daher zu prüfen, ob die Forschung vom Verbot von Ausschließlichkeitsvereinbarungen auszunehmen ist, um den Forschungsstandort Europa nicht zu schwächen.

Art. 5 VO-E:

Verhältnis Art. 5 VO-E zu anderen datenschutzrechtlichen Anforderungen

In Art. 5 VO-E wird die bereits oben aufgeworfene allgemeine Frage nach dem Verhältnis einzelner Bestimmungen des Entwurfs zu den allgemeinen datenschutzrechtlichen Anforderungen aus der DSGVO sowie dem bereichsspezifischen Datenschutzrecht der Mitgliedstaaten besonders deutlich. Dies wird im Folgenden konkret für das Verhältnis zur DSGVO aufbereitet. Ähnliche Fragen würden sich aber auch im Verhältnis zum bereichsspezifischen Datenschutzrecht (wie etwa Richtlinie (EU) 2016/680) stellen, sofern dieser Bereich nicht vom Anwendungsbereich der VO insgesamt ausgenommen würde.

- Es ist insgesamt unklar, wie bei einer Weiterverwendung personenbezogener Daten die Einhaltung der datenschutzrechtlichen Vorschriften konkret gewährleistet werden soll. Sowohl die in Art. 5 Abs. 3 VO-E geregelte Anonymisierung als auch die Weiterverwendung in einer sicheren Verarbeitungsumgebung gem. Art. 5 Abs. 4 und 5 VO-E bedarf als eigenständiger Datenverarbeitungsvorgang einer Einwilligung oder einer anderen Rechtsgrundlage nach der DSGVO. Insbesondere in Hinblick eine Weiterverwendung auf Grundlage einer Einwilligung i.S.d. Art. 6 Abs. 1 Buchst. a, Art. 7 DSGVO wirft Fragen bezüglich der praktischen Umsetzbarkeit auf: Wie soll die Einholung einer Einwilligung der betroffenen Personen konkret erfolgen? Wenn die Einholung einer Einwilligung (Art. 6 Abs. 1 Satz 1 Buchst. a DSGVO) bei den betroffenen Personen schon bei Erhebung der Daten erfolgen soll, müssten die betroffenen Personen außerdem schon zum Zeitpunkt der Erhebung über die Zwecke einer späteren Weiterverwendung informiert sein, bevor sie ihre Einwilligung erteilen. Dies dürfte zu Problemen führen, je weiter die ursprüngliche Erhebung und spätere Weiterverwendung zeitlich auseinanderliegen, da Zwecke dann ggf. nicht hinreichend konkret absehbar sind. Bei geänderten Zwecken müssten jeweils alle Betroffenen erneut um ihre Einwilligung gebeten werden. Zudem müssten die Rechte betroffener Personen auch für solche Daten gewährleistet sein, die weiterverwendet werden sollen. Wie ist in diesem Zusammenhang umzugehen insbesondere mit dem Widerruf der Einwilligung (der auch zu einem Ende der Weiterverwendung führen müsste) und dem Recht auf Löschung (Art. 17 DSGVO) – wäre dieses dann gegenüber der weiterverwendenden Stelle geltend zu machen?

- Die Bundesregierung bittet um explizite Klarstellung in den Erwägungsgründen, dass die Daten unter den Voraussetzungen des Kapitel 2 für Forschungszwecke genutzt werden können, wenn ein Zugang zu diesen Daten besteht. Zudem wäre eine stärkere Harmonisierung in den Mitgliedsstaaten zur verbesserten Verknüpfung von Daten insbesondere für Forschungszwecke durchaus wünschenswert.
- **Art. 5 Abs. 3 VO-E:** Es wird gebeten, die Abgrenzung zwischen Pseudonymisierung und Anonymisierung klarzustellen. Im Gegensatz zur Anonymisierung kann bei pseudonymisierten Daten der Personenbezug durch Hinzuziehung zusätzlicher Informationen wiederhergestellt werden, so dass nicht ersichtlich ist, wie durch eine bloße Pseudonymisierung die Weiterverwendung von personenbezogenen Daten nach diesem Absatz ermöglicht werden soll. Darüber hinaus ist zu prüfen, ob Vorgaben zu Zeitpunkt und Technik gemacht werden müssen (vgl. auch Erwägungsgrund 26 DSGVO). Ferner ist im Bereich der Forschung sicherzustellen, dass die Ergebnisse der Datenverarbeitung auch nach erfolgter Anonymisierung nachvollziehbar und reproduzierbar bleiben.
- **Art. 5 Abs. 3 VO-E:** Die Bestimmung des Art. 5 Abs. 3 VO-E soll nach hiesigem Verständnis und auch entsprechend der Ausführungen in Erwägungsgrund 11 regeln, dass öffentliche Stellen geschützte Daten anonymisieren oder sonst „aufbereiten" dürfen, um sie anschließend in derart aufbereiteter Form dem Weiterverwender zur Verfügung zu stellen. Die Kommission wird um Erläuterung gebeten, ob dieses Verständnis so zutreffend ist oder ob die Anonymisierung bzw. sonstige Aufbereitung auch durch den Weiterverwender erfolgen soll. Falls ausschließlich die öffentliche Stelle die Anonymisierung/Aufbereitung durchführen soll, kommt dies im Wortlaut des Art. 5 Abs. 3 VO-E bislang nicht hinreichend zum Ausdruck (der Satzteil „können die Verpflichtung auferlegen, dass nur aufbereitete Daten weiterverwendet werden dürfen" ist missverständlich, da er suggeriert, dass es einen Dritten gibt, dem eine derartige „Verpflichtung" „auferlegt" werden könnte). Es ist darüber hinaus fraglich, was – jedenfalls in Bezug auf personenbezogene Daten – der eigenständige Regelungsgehalt dieser Bestimmung ist, da eine Anonymisierung bereits nach der DSGVO bei Vorliegen einer Rechtsgrundlage zulässig ist.
- **Art. 5 Abs. 3 VO-E:** Nach dem Wortlaut von Art. 5 Absatz 6 VO-E könnte der falsche Eindruck entstehen, dass Art. 5 Absatz 3 VO-E eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten gewähren soll („Wenn die Weiterverwendung von Daten nicht *gemäß Absatz 3* erlaubt werden kann und es *keine anderen Rechtsgrundlagen* gibt."). Die Regelungsintention der KOM, keine eigenständigen Rechtsgrundlagen des Unionsrechts für die Verarbeitung von personenbezogenen Daten zu schaffen, muss klarer im Wortlaut von Art. 5 VO-E zum Ausdruck kommen.
- **Art. 5 Abs. 3 VO-E**: Art. 5 Abs. 3 VO-E definiert als „Aufbereitung" die Anonymisierung personenbezogener Daten sowie die Löschung von Geschäftsgeheimnissen. Es werden insoweit bislang nur die Fälle des Art. 3 Abs. 1 Buchstabe a und d VO-E von der Regelung

erfasst. Die Kommission wird um Klarstellung gebeten, ob Art. 5 Abs. 3 VO-E auch auf Daten Anwendung findet, die der statistischen Geheimhaltung (Art. 3 Abs. 1 Buchstabe b VO-E) und dem Schutz geistigen Eigentums Dritter (Art. 3 Abs. 1 Buchstabe c VO-E) unterliegen und, wenn ja, welche Maßnahme in diesen Fällen als „Aufbereitung“ anzusehen ist.

- **Art. 5 Abs. 9 bis 13 VO-E:** Die Kommission hält sich offen, Durchführungsrechtsakte zu einzelnen Drittländern und deren adäquatem Schutz geistigen Eigentums und von Geschäftsgeheimnissen zu erlassen. Die Absicherung von IP-Rechten und Geschäftsgeheimnissen ist ein wichtiges und berechtigtes Interesse. Es wird um Klarstellung gebeten, auf welche Initiative hin die Kommission tätig wird und Durchführungsrechtsakte erwägt und erlässt. Die Bedingungen, die Art. 5 Abs. 10 VO-E an eine Weiterleitung sensibler nicht-personenbezogener Daten in Drittländer stellt, dürften in der Praxis, sofern keine Durchführungsrechtsakte i.S.v. Abs. 9 vorliegen, aufgrund ihrer Komplexität und der zusätzlichen Prüfpflichten insbesondere für kleinere Weiterverwender mit begrenzten Ressourcen (z.B. KMUs) nur schwer erfüllbar sein. Da die Kommission im Vorfeld ausgeführt hat, dass die vorgeschlagenen Regelungen insbesondere mit dem GATS vereinbar seien, erbitten wir um Erläuterung, inwieweit Art. 5 Abs. 9 bis 13 von den WTO-rechtlichen Verpflichtungen der EU bzw. von den Rechtfertigungstatbeständen des WTO-Rechts gedeckt sind. Zur Klarstellung der Vereinbarkeit der geplanten Verordnung mit den bestehenden Pflichten und Verpflichtungen der Europäischen Union in internationalen Handelsabkommen erbitten wir, am Ende des vierten Erwägungsgrunds folgenden Satz zu ergänzen: „Diese Maßnahmen erfolgen unbeschadet der Pflichten und Verpflichtungen aus internationalen Handelsabkommen.“ Diese Klarstellung wäre auch ein wichtiges Signal an andere WTO-Mitglieder und verhinderte eine mögliche Schwächung der Glaubwürdigkeit der EU auch in ihrem Eintreten für einen wirksamen Schutz gegen ungerechtfertigte Datenlokalisierungsanforderungen in den plurilateralen Verhandlungen zu e-Commerce in Genf.
- **Art. 5 Abs. 11 VO-E:** Wir bitten die Kommission um Erläuterung, nach welchen Kriterien Daten als hochsensibel eingestuft werden sollen. Die Bundesregierung ist außerdem der Auffassung, dass im Falle des Art. 5 Abs. 11 VO-E ein Durchführungsrechtsakt nach dem Verfahren des Art. 29 VO-E besser geeignet ist, um den betroffenen Interessen gerecht zu werden. Sie bittet daher um entsprechende Korrektur des Verordnungsentwurfs. Die Verfahrensweise mit den von diesem Absatz möglicherweise erfassten Daten dürfte oftmals nationale Interessen berühren, weshalb eine angemessene mitgliedstaatliche Beteiligung im Rahmen des Komitologieverfahrens angezeigt ist. Dies gilt umso mehr, als die Einführung von spezifischen Beschränkungen des grenzüberschreitenden Verkehrs nicht-personenbezogener Daten angesichts bestehender internationaler Pflichten und Verpflichtungen der Europäischen Union sehr vielschichtig ist. Eine sorgfältige Prüfung im Rahmen eines Komitologieverfahrens erscheint daher diesen Fällen angemessen.

Sonstige Fragen:

- **Forschungsfreundliche Ausgestaltung:** Forschungs- und innovationspolitisch sowie aus Gründen der Rechtssicherheit sollte im Data Governance Act insbesondere in Bezug auf Art. 5 Abs. 2 und Abs. 5 klargestellt werden, dass die Bedingungen für die Weiterverwendung der Daten öffentlicher Stellen insgesamt forschungsfreundlich auszugestalten sind. Die BReg bittet um Ergänzung in Erwägungsgrund 11 wie folgt „Die Bedingungen der Weiterverwendung müssen forschungsfreundlich ausgestaltet werden, z.B. sollte die Privilegierung der Forschung als nicht-diskriminierend im Sinne von Art. 5 Abs. 2 VO-E angesehen werden."**Art. 5 Abs. 3 und 4 VO-E**: Die Kommission wird um Erläuterung gebeten, in welchem Verhältnis Art. 5 Abs. 3 und 4 VO-E zueinanderstehen. In Erwägungsgrund 11 wird ausgeführt, dass die Einrichtung einer sicheren Verarbeitungsumgebung dann in Betracht kommt, wenn die Bereitstellung bloß aufbereiteter Daten „nicht dem Bedarf des Weiterverwenders [entspricht]". Wenn Art. 5 Abs. 4 VO-E daher nur subsidiär gegenüber Art. 5 Abs. 3 VO-E zur Anwendung kommt, sollte dies ausdrücklich geregelt werden. Es bedarf weiterer Konkretisierung, wann aufbereitete Daten „nicht dem Bedarf des Weiterverwenders [entsprechen]".
- **Art. 5 Abs. 3 bis 6 VO-E**: Allgemein stellt sich zunächst die Frage, ob die in Art. 5 Abs. 3-6 VO-E geregelten Weiterverwendungsmodalitäten (z.B. die Anonymisierung von Daten, die Einrichtung einer sicheren Verarbeitungsumgebung) für eine öffentliche Stelle fakultativ sind (siehe Wortlaut von Art. 5 Abs. 3 und 4 VO-E: „können") oder ob öffentliche Stellen unionsrechtlich verpflichtet werden, potentiellen Weiterverwendern entsprechende Modalitäten gegen Gebühren (dazu Art. 6 VO-E) anzubieten bzw. ob es sogar einen rechtlich durchsetzbaren Anspruch von potentiellen Weiterverwendern gibt, dass eine öffentliche Stelle bestimmte Daten anonymisiert, eine sichere Verarbeitungsumgebung einrichtet und ggf. sogar Unterstützungsleistungen bei der Erlangung von Einwilligungen erbringt. Diese Frage erfolgt vor dem Hintergrund der weitgehenden Regelungen in Art. 8 Abs. 3 und Abs. 4 VO-E. Sofern ein rechtlich durchsetzbarer Anspruch eingeführt werden soll bedarf es der näheren Prüfung, ob ein solcher Anspruch angemessen und praxistauglich wäre. Außerdem müsste dann geregelt werden, was im Falle des Art. 5 Abs. 3 und der Abs. 4 und 5 VO-E zulässige Ablehnungsgründe sind, so wie dies in Art. 5 Abs. 6 VO-E erfolgt ist („unverhältnismäßig hohe Kosten"). Auch hinsichtlich Art. 5 Abs. 6 VO-E ist zweifelhaft, ob die dort geregelte Unterstützungspflicht als subjektiver Anspruch ausgestaltet werden sollte, da dadurch letztlich die Gefahr bestünde, dass die öffentliche Stelle für den Weiterverwender die Einwilligung Dritter beschaffen müsste.
- **Art. 5 Abs. 4 VO-E:** Im Hinblick auf die Möglichkeit, den Fernzugriff unter bestimmten Voraussetzungen auszuschließen und die Weiterverwendung nur in physischen Räumlichkeiten zu erlauben (Art. 5 Abs. 4 Buchst. b VO-E), wird um Erläuterung gebeten, an

welche Sachverhalte hier gedacht wird, in denen ein Fernzugriff die Rechte und Interessen Dritter gefährden würde.

- **Art. 5 Abs. 4 VO-E:** Es wird um Erläuterung gebeten, was mit „Bereitstellung“ und „Kontrolle“ einer sicheren Verarbeitungsumgebung in Art. 5 Abs. 4 Buchst. a VO-E genau gemein ist. Dies stellt auch im Hinblick auf die in Art. 5 Abs. 5 S. 1 VO-E genannten Anforderungen einen erheblichen technischen Aufwand
  insb. für die IT-Sicherheit dar, der nicht näher berücksichtigt wird.
- **Art. 5 Abs. 5 VO-E:** Inwieweit werden die Befugnisse der öffentlichen Stellen durch Art. 5 Abs. 5 des VO-E erweitert, wo es heißt, dass sich diese das Recht vorbehalten, die Verwendung der Ergebnisse zu verbieten, wenn darin Informationen enthalten sind, die die Rechte und Interessen Dritter gefährden? Bei Art. 5 Abs. 5 S. 2 ist darauf zu achten, dass die sowohl die schutzwürdigen Interessen Dritter als auch die Belange der Wissenschaft angemessen berücksichtigt werden.
- **Art. 5 Abs. 5 S. 2 VO-E**: Es wird ausdrücklich begrüßt, dass die öffentliche Stelle die Datenverarbeitung des Weiterverwenders in der sicheren Verarbeitungsumgebung „überprüft“. Diese Überprüfbarkeit ist wichtige Voraussetzung dafür, dass der sicheren Verarbeitungsumgebung von den betroffenen Personen ausreichend Vertrauen entgegengebracht wird. Es muss daher gewährleistet sein, dass öffentliche Stellen ihrer Aufgabe der Überprüfung in der Praxis wirksam nachkommen können. Dies stellt hohe Anforderungen an die personelle Ausstattung und an die technische Expertise von öffentlichen Stellen. Es sollten Möglichkeiten geprüft werden, wie die EU die Mitgliedstaaten beim Aufbau dieser Expertise gezielt unterstützen kann; der Dateninnovationsrat könnte beauftragt werden, dazu Vorschläge zu entwickeln. Die BReg unterstützt die Änderungen der Vorschrift, sodass die Überprüfung sich auch auf statistische Modelle erstrecken kann, wie im Kompromisstext der Ratspräsidentschaft vom 22. Februar.
  Die Kommission wird ungeachtet dessen um nähere Erläuterung gebeten, ob es ausreichend ist, dass die öffentliche Stelle nach dem Normtext von Art. 5 Abs. 5 S. 2 VO-E lediglich zur Überprüfung „in der Lage“ sein muss oder ob in begründeten Einzelfällen eine Überprüfung im Einzelfall in einem angemessenen Umfang vorgeschrieben werden kann.
- **Art. 5 Abs. 6 VO-E**: Das Verhältnis zwischen Art. 5 Abs. 6 VO-E und den Regelungen zur sicheren Verarbeitungsumgebung in Art. 5 Abs. 4 und 5 VO-E ist unklar. Art. 5 Abs. 6 VO-E bestimmt, dass die öffentliche Stelle den potentiellen Weiterverwender bei der Einholung einer Einwilligung unterstützt „wenn die Weiterverwendung von Daten nicht gemäß den in den Absätzen 3 bis 5 festgelegten Verpflichtungen erlaubt werden kann“. Dabei sind doch jedenfalls Fälle denkbar, in denen eine Verarbeitung von personenbezogenen Daten auch in einer sicheren Verarbeitungsumgebung datenschutzrechtlich nur dann zulässig ist, wenn die betroffene Person eingewilligt hat. Es stellt sich daher die Frage, ob es der in Art. 5 Abs. 6 VO-E geregelten „Unterstützung“ des Weiterverwenders durch die öffentliche Stellen nicht

auch in den Fällen des Art. 5 Abs. 4 und 5 VO-E (sichere Verarbeitungsumgebung) bedürfte. Zudem stellt sich die Frage, wer die Verantwortung einer unrechtmäßigen Datenverarbeitung trägt, falls die mit Unterstützung der öffentlichen Stelle eingeholten Einwilligungen nicht den Anforderungen entsprechen und somit nicht rechtmäßig waren.

- **Art. 5 Abs. 7 VO-E**: Es wird gebeten, die Regelung (in Verbindung mit Erwägungsgrund 13) zu erläutern: Hiernach sollen öffentliche Stellen, sofern sie Rechtsinhaber des sui-generis-Datenschutzrechts nach Artikel 7 Absatz 1 Datenbank-Richtlinie 96/9/EG sind, dieses Recht nicht in Anspruch nehmen. Gleichzeitig stipuliert Artikel 3 Absatz 1 Buchstabe c) VO-E, dass diese Vorschrift nur für Daten gilt, an denen geistiges Eigentum Dritter besteht. Besteht insoweit überhaupt ein Anwendungsbereich für Artikel 5 Absatz 7 VO-E.
- **Art. 5 Abs. 8 VO-E:** Es wird zunächst um Erläuterung gebeten, mit welchen technischen oder rechtlichen Maßnahmen die Sicherstellung der in Art. 5 Abs. 8 VO-E geforderten Vertraulichkeit erfolgen soll. In der Sache bestehen aus derzeitiger Sicht Bedenken gegenüber einer derart weitreichenden Sicherstellungspflicht öffentlicher Stellen. Die öffentlichen Stellen dürften über die in Erwägungsgrund 11 erwähnten Vertraulichkeitsvereinbarungen hinaus vielfach keine Möglichkeit haben, Einfluss auf den Weiterverwender zu nehmen. Letztlich könnte sogar eine Haftung bei Verletzung der Sicherstellungspflicht in Betracht kommen.

Art. 6 und Art. 7 VO-E:

- **Art. 6 VO-E:** Es sollte klargestellt werden, dass auch auf privatrechtlicher Grundlage vereinbarte Vergütungen möglich sind. Gegenwärtig schließt das Deutsche Patent- und Markenamt Datenabgabeverträge mit Unternehmen, auf deren Grundlage veröffentlichte Daten zu Schutzrechten zum Zweck der Schutzrechtsinformation zur Verfügung gestellt werden. In diesen werden Entgelte vertraglich vereinbart. Diese bewährte Praxis sollte auch in Zukunft möglich sein.
- **Art. 6 Abs. 4 VO-E**: Wir bitten im Sinne der Rechtssicherheit und -klarheit, die in Erwägungsgrund 20 vorgesehene Option einer ermäßigten Gebühr bzw. einer unentgeltlichen Weiterverwendung für Forschung und Wissenschaft in den VO-Text zu übertragen. Aus diesem Grund bitten wir um folgende Ergänzung nach „nichtkommerziellen Zwecken“: „wie Zwecke der wissenschaftlichen Forschung“. Zudem sollte Art. 6 Abs. 4 um folgenden Satz ergänzt werden: „Dies umfasst die Zurverfügungsstellung von Daten zu niedrigeren Gebühren oder unentgeltlich.“

  Darüber hinaus sollte in den Erwägungsgründen klargestellt werden, dass zu den Bereichen, in denen gemäß Erwägungsgrund 20 günstigere Modalitäten vorgesehen werden können, auch die wissenschaftliche Forschung gehört. Wir bitten hierzu um Aufnahme folgender Formulierung in Satz 1 von Erwägungsgrund 20 hinter „etwa für nichtkommerzielle Zwecke“: „wie Zwecke der wissenschaftlichen Forschung“. Zudem bitten

wir um Einfügung eines Satz 2: „Zwecke der wissenschaftliche Forschung umfasst sämtliche Forschungszwecke, unabhängig von der organisatorischen Struktur und Finanzierung der betreffenden Einrichtung, allerdings nicht die Forschung, die ein auf die Erzielung von Gewinnen gerichtetes Unternehmen betreibt, um Waren oder Dienstleistungen zu entwickeln, weiterzuentwickeln oder zu optimieren."

- **Art. 7 Abs. 1 und 5 VO-E**: Es wird um Erläuterung gebeten, warum die Kommission zusätzliche zuständige Stellen zu den öffentlichen Stellen für sinnvoll erachtet. Es sollte die Möglichkeit erhalten bleiben, keine zusätzlichen Stellen mit den in Art. 7 genannten Aufgaben zu befassen, wenn diese auch durch die öffentlichen Stellen selbst erbracht werden können. Alternativ sollten die Unterstützungsleistungen auf Unionsebene erbracht werden. Wir bitten um Streichung des Art. 7 Abs. 5.
- **Art. 7 Abs. 2 VO-E:** Bei der technischen Unterstützung bzgl. der Datennutzung sollten die Belange der Forschung, z.B. im Hinblick auf die gute, wissenschaftliche Praxis, berücksichtigt werden.
- **Art. 7 Abs. 2 Buchst. a VO-E:** Die Rolle der „sicheren Verarbeitungsumgebung" ist unklar. Es scheint so, dass die Weiterverwendung der Daten durch dritte Stellen innerhalb einer Umgebung stattfinden soll, die die öffentlichen Stellen (ggf. mit Unterstützung von „zuständigen Stellen") aufzubauen haben. Diese wären dann ferner aktuell zu halten, die Rechte der Betroffenen auch diesbezüglich zu gewährleisten und die Weiterverwendung wäre insgesamt zu kontrollieren. Darüber hinaus stellt sich die Frage, wer für die „sichere Verarbeitungsumgebung" datenschutzrechtlich verantwortlich ist, wenn die „zuständigen Stellen" ggf. mehrere solcher Umgebungen für mehrere öffentliche Stellen und unterschiedliche Weiterverwendungszwecke betreuen.
- **Art. 7 Abs. 2 Buchst. b VO-E:** In dieser Bestimmung werden verschiedene Privacy-Enhancing-Technologies referenziert (Pseudonymisierung, Anonymisierung, Generalisierung, Unterdrückung, Randomisierung). Es stellt sich zum einen die Frage, welche weiteren Techniken als derart „erprobte Techniken" anzusehen sind. Zum anderen wirft die Bestimmung die Frage auf, in welchem Verhältnis die Techniken zu den in Art. 5 VO-E genannten Verfahren stehen. In Art. 5 Abs. 3 VO-E wird z.B. lediglich auf Anonymisierung und Pseudonymisierung, nicht aber auf die anderen Techniken abgestellt, so dass diese Diskrepanz erläutert werden sollte. Haben die Techniken auch Relevanz für die in Art. 5 Abs. 4 und 5 VO-E geregelte sichere Verarbeitungsumgebung?
- **Art. 7 Abs. 2 Buchst. c VO-E:** Auch hier stellt sich die Frage, wie ein Assistieren beim Einholen von Einwilligungen aussehen soll (siehe bereits oben) und wie sich dies auf die Bewertung der datenschutzrechtlichen Verantwortlichkeit im Verhältnis von „zuständigen Stellen" zu öffentlichen Stellen auswirkt.
- **Art. 8 VO-E:** Die Regelungssystematik ist unklar. Absätze 3 und 4 regeln das Antragsverfahren und daher Anforderungen, die sich nicht an die in der Überschrift genannte

„Zentrale Informationsstelle“ richten, sondern an die jeweils zuständigen öffentlichen Stellen. Wir bitten um Streichung des Absatzes 3 (s.u.). Absatz 4 sollte in einen eigenen Artikel ausgegliedert werden.

- **Art. 8 Abs. 2 VO-E:** Es wird um Erläuterung gebeten, welchen Mehrwert die Kommission in der Einrichtung einer zentralen Informationsstelle sieht und welche Behörde für diese Aufgabe passend erscheint. Die Kommission wird um Einschätzung gebeten, ob die Bündelung dieser Aufgaben auf Unionsebene nicht sinnvoll erscheint. Es sollte zumindest die Möglichkeit geschaffen werden, dass die Aufgaben der Unterstützungsstelle und die der zentralen Informationsstelle in einer Stelle zusammengefasst werden. Dies kann den Gesamtaufwand für die Behörden verringern. Zudem sollte betont werden, dass die Möglichkeit zur Antragstellung bei der zentralen Informationsstelle nur eine weitere Möglichkeit zur Antragstellung ist, und die Option, dies bei der eigentlich zuständigen Stelle zu tun, nicht beeinträchtigt wird. Eine Präzisierung der Art der Bereitstellung wäre wünschenswert, insbesondere aufgrund der Möglichkeit, das Verzeichnis maschinenlesbar zu gestalten.
- **Art. 8 Abs. 3 VO-E:** Mit der vorgeschlagenen Pflicht zur Bescheidung von Weiterverwendungsanträgen wären öffentliche Stellen für die Nicht-Herausgabe von (u.a. personenbezogenen) Daten begründungspflichtig – und zwar auch dahingehend, dass eine Weiterverwendung auch nicht unter den in Art. 5 Abs. 3 bis 5 VO-E genannten Bedingungen bzw. Verpflichtungen oder eine Unterstützung bei der Einholung von Einwilligungen gemäß Art. 5 Abs. 6 VO-E möglich ist. Art. 8 Abs. 3 VO-Entwurf enthält somit Elemente eines subjektiven Anspruchs auf Datenzugang sowie Regelungen bezüglich des Verwaltungsverfahrens. Den öffentlichen Stellen wird dadurch eine neue öffentliche Aufgabe auferlegt. Sie müssen zukünftig die Nicht-Herausgabe bestimmter Daten begründen und rechtfertigen, wohingegen bislang ein potentieller Datennutzer die Gründe angeben musste, warum er Zugang zu bestimmten Daten begehrt. Darin ist – jedenfalls in Bezug auf den Umgang mit personenbezogenen Daten – ein elementarer Wandel zu sehen. Die Kommission wird gebeten, die Erforderlichkeit dieser Regelung näher darzulegen sowie die Vereinbarkeit mit der DSGVO näher zu erläutern.

  Die Maximalfrist für die Bescheidung von Weiterverwendungsanträgen innerhalb von zwei Monaten erscheint zu kurz bemessen. Die Gründe für ein Prüfungsverfahren von mehr als zwei Monaten können vielfältig sein. So kann im Rahmen der Prüfung von Anspruchsvoraussetzungen z.B. eine tatsächliche Überprüfung der vom Antragsteller behaupteten Umstände erforderlich sein. Möglicherweise ist eine umfangreiche Prüfung des Re-Identifikationsrisikos samt Überarbeitung zur Gewährleistung der Anonymisierung oder Pseudonymisierung der zur Verfügung zu stellenden Daten nötig. Der VO-E verdeutlicht in Art. 5 Abs. 2, 3 gerade, dass solche Maßnahmen zulässig und oft auch unerlässlich sind. Es ist widersprüchlich, dass im Entwurf einerseits die Bearbeitung des Antrags in einer

angemessenen Frist gefordert wird, im gleichen Satz jedoch eine zu kurze Maximalfrist festgelegt wird. Schließlich ist auch zu berücksichtigen, dass die Anträge nach Art. 8 Abs. 2 VO-Entwurf bei der Zentralen Informationsstelle eingereicht werden können, die die Anträge dann noch an die zuständige Stelle nach Art. 7 VO-Entwurf weiterleiten muss. Art. 8 Abs. 3 VO-E sollte daher gestrichen werden.

3. Kapitel III „Anforderungen an Dienste für die gemeinsame Datennutzung“

Der Vorschlag der Kommission zur Harmonisierung der rechtlichen Anforderungen an „Dienste für die gemeinsame Datennutzung“ (im Folgenden entsprechend Erwägungsgrund 22: Datenmittler) wird grundsätzlich begrüßt. Derartige Dienste können wesentliche Akteure sein, um das Innovationspotential von Daten zu erschließen. Sie ermöglichen, qualitativ hochwertige Daten auf freiwilliger Basis und unter Wahrung ggf. vorliegenden Schutzrechte zugänglich zu machen.

Der konkrete Rechtsrahmen für Datenmittler sollte das Datenschutzrecht sicherstellen. Ein wichtiges Kriterium ist hierbei, dass solche Datenmittler ausschließlich im Interesse der betroffenen Person tätig sind und entsprechend der Vorgaben des Datenschutzrechts handeln. Bei privatwirtschaftlich organisierten Datenmittlern muss ausgeschlossen werden, dass die Datenmittler an der kommerziellen Nutzung dieser Daten verdienen. Alle Betreibermodelle müssen mit den Vorgaben der Unabhängigkeit, Neutralität und dem erforderlichen Nutzervertrauen in Einklang zu bringen sein.

Daher sollte geprüft werden, ob die vorgeschlagenen Regelungen einen hinreichenden Anreiz zum Angebot sowie zur Inanspruchnahme der Dienste von Datenmittlern bieten, bzw. wie noch stärkere positive Anreize für solche Dienste gesetzt werden können. Zudem sollte an geeigneter Stelle in den Erwägungsgründen (z.B. Erwägungsgrund 22 oder 25) explizit klargestellt werden, dass auch Forschungsorganisationen Dienste von Datenmittlern als Datennutzer in Anspruch nehmen können. Für Forschende in ihrer Rolle als Datennutzer sollten im Rahmen der näheren Ausgestaltung des Datenmittlermodells eine forschungsfreundliche Ausgestaltung im Einklang mit der guten wissenschaftlichen Praxis sichergestellt werden. Es gibt eine Vielzahl von Modellen der Datenmittlerschaft. Es sollte sichergestellt sein, dass die Regelungen dieser Vielfalt gerecht werden. Dazu gehört einerseits, dass Vertrauen in die Tätigkeit von Datenmittlern hergestellt wird, und dass andererseits überschießende Auflagen vermieden werden, um eine Tätigkeit als Datenmittler auch kleineren oder neu auf den Markt kommenden Anbietern zu ermöglichen. Daher sollte geprüft werden, ob die im VO-E enthaltenen Anforderungen geeignet sind, um das Vertrauen der Dateninhaber in die Dienste selbst sowie in die Qualität der vermittelten Daten zu schaffen. Es sollte auch **geprüft werden, welche Rolle Zulassungsverfahren, Akkreditierung, Zertifizierung oder Codes of Conduct in diesem Zusammenhang** spielen könnten. Es müsste

im weiteren Verlauf der Verhandlungen herausgearbeitet werden, wo Lösungen auf **freiwilliger Basis** ausreichend sind und wo **Verpflichtungen** angezeigt sind. Die Bundesregierung behält sich auf Grundlage der Prüfung vor, **weitere Anforderungen** für Datenmittler zu formulieren.

In Artikel 9 ist zur Klarstellung ein neuer Absatz wie folgt zu ergänzen: "Ungeachtet der allgemeinen Regelungen zum Anwendungsbereich dieser Verordnung, gilt Kapitel III nicht für öffentliche Verkündungs-, Bekanntmachungs- und Veröffentlichungsorgane, Datenbanken und Register, es sei denn sie wurden zu dem besonderen Zweck gegründet, Dienste im Sinne dieses Kapitels III zu erbringen."

Darüber hinaus werden folgende Klarstellungen angeregt:

- Die Kommission wird um Erläuterung gebeten, wie die Vielzahl bestehender europäischer Geschäftsmodelle des Datenaustauschs im Industriebereich und im industrienahen Bereich angemessen berücksichtigt wurden. Es besteht die Befürchtung, dass bestehende Industrielösungen (und ihre Weiterentwicklung) nicht mehr angeboten werden können. Es ist unerlässlich, eine klare Definition von Datenmittlern zu schaffen, die der erfolgversprechenden und innovationsfördernden Entwicklung branchenspezifischer und -übergreifender Datenräume im Industriebereich und im industrienahen Bereich nicht entgegensteht und bestehende europäische Konsortien in den Aktivitäten zum Datenteilen nicht unangemessen beeinträchtigt.
- Die Kommission wird um Klarstellung gebeten, dass **Forschungsdatenzentren** und andere wissenschaftliche Forschungseinrichtungen – bzw. Netzwerke nicht von Kapitel III des VO-E betroffen sind. Dies ist ggf. in Art. 14 oder im entsprechenden Erwägungsgrund dann auch explizit klarzustellen.
- **Art. 9 Abs. 1 Buchst. a VO-E:** Es wird um Prüfung gebeten, ob die im Normtext geregelten Voraussetzungen eines Vermittlungsdienstes nach Art. 9 Abs. 1 Buchst. a VO-E hinreichend klar sind, um rechtssicher abzugrenzen, welche Formen der Datenmittlerschaft dem Anwendungsbereich unterfallen, und welche nicht. Auffällig ist, dass Erwägungsgrund 22 zahlreiche Negativabgrenzungen vornimmt (z.B. bzgl. Cloud-Dienste, Werbe- oder Datenmakler, Inhaltsvermittlung etc.), die nicht ohne weiteres mit einem in Art. 9 Abs. 1 Buchst. a VO-E normierten Merkmal in Verbindung zu stehen scheinen.
- **Art. 9 Abs. 1 Buchst. b VO-E:** In Bezug auf Vermittlungsdienste zwischen datenschutzrechtlich Betroffenen und potenziellen Datennutzern fehlen klarstellende Regelungen, wie die Dienste als Interessenswalter von Nutzerinnen und Nutzern tätig sein und ihnen technische Hilfsmittel bieten können, um ihnen die Wahrnehmung ihrer Betroffenenrechte zu ermöglichen. Zu berücksichtigen ist bei der Klarstellung, dass entsprechend der Formulierung in Erwägungsgrund 24 die Entscheidungsbefugnis über

die Ausübung der Rechte gemäß DSGVO bei der Person selbst verbleibt, die Durchführung und Umsetzung aber durchaus durch einen Dritten erfolgen kann, etwa durch eine anwaltliche Vertretung. Dies setzt voraus, dass die Erteilung des Auftrags für den bestimmten Fall den gleichen Anforderungen wie die Erteilung der Einwilligung in die Datenverarbeitung genügt.

- **Art. 10 VO-E**: Die Bundesregierung behält sich vor, die Anmeldepflicht als geeignetes Mittel und die materiellen Anforderungen im weiteren Verhandlungsverlauf näher zu kommentieren. Die vorgeschlagene Anmeldepflicht für Datenmittler, die Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, und Datennutzern anbieten (Art. 9 Abs. 1 Buchst. b), erscheint nicht in allen Fällen angemessen. Die Kommission stellt dar, dass die Geschäftsmodelle sicherstellen müssen, dass keine falschen Anreize bestehen, die den Einzelnen dazu bewegen, mehr Daten für die Verarbeitung zur Verfügung zu stellen, als im Interesse des Einzelnen liegt (vgl. Erwägungsgrund 23 des VO-E). Deshalb muss im weiteren Verlauf der Verhandlungen herausgearbeitet werden, in welchen Fällen die Unabhängigkeit der Dienste nach Art. 9 Absatz 1 Buchst. b – wie bei den datenaltruistischen Organisationen nach Kap. IV – in der Verordnung verankert werden sollte und ggfs. ein anderes Verfahren (Zertifizierung/Akkreditierung/Zulassung) vorzusehen ist. Ein anderes Verfahren könnte eine behördliche Kontrolle von Anfang an gewährleisten und verhindern, dass sich Akteure am Markt etablieren, die die Voraussetzungen nach dieser Verordnung nicht erfüllen. Die Kommission wird gebeten, zu erläutern, weshalb diese Optionen nicht gewählt wurden.
- **Art. 10 Abs. 6 VO-E:** Es wird um Präzisierung gebeten, ob die hier erwähnten Angaben für die Anmeldung öffentlich einsehbar sein sollen und wenn ja, in welcher Form.
- **Art. 10 Abs. 8 VO-E**: Es wird um Erläuterung gebeten, warum die zuständige Stelle zusätzlich zur Meldung an die Kommission (Abs. 9) an alle nationalen zuständigen Stellen der Mitgliedsstaaten die Anmeldung weiterleitet. Die Transparenz scheint mit dem Register der Kommission hinreichend gewährleistet. Wir bitten um Streichung des Absatzes.
- **Art. 10 Abs. 9 VO-E:** Es wird um Klarstellung gebeten, ob das von der Kommission geführte Register öffentlich einsehbar ist. Für die Transparenz eines entstehenden Marktes von Diensteanbietern scheint dies geboten. Darüber hinaus wird um Klärung gebeten, wie das Verfahren durchgeführt wird, wenn die Eigenschaft als Datenmittler nur einen Teil der Tätigkeit darstellt (z.B. bei Hochschulen).
- **Art. 11 VO-E: Anforderungen an die Qualität der Daten.** Es empfiehlt sich, zumindest mit Erwerbszweck handelnden Datenmittler, die im Wissenschaftskontext tätig werden, zu verpflichten, eine Quellen- und Datumsangabe der vermittelten Daten vorzuhalten

sowie möglicherweise auch weiterführende Hinweise, wie die Daten bislang verwendet wurden.

- **Art. 11 Nr. 1 VO-E:** Die Formulierung, dass Anbieter Dienste *für Daten* erbringen, scheint unangemessen bzw. unpräzise. Um eine sprachliche Präzisierung, für wen die Dienste erbracht werden, wird gebeten.
- **Art. 11 Nr. 1 VO-E:** Die Kommission wird um Klarstellung gebeten, dass die Regelung nicht bestimmt, zu welchen Zwecken der Datennutzer die Daten weiterverwenden darf. Art. 11 Nr. 1 schränkt weder ein noch privilegiert, wer als Datennutzer die Daten von dem Datenmittler erhält.
- **Art. 11 Nr. 1 VO-E**: Die Kommission wird um nähere Erläuterung der Rechtfertigung einer strukturellen Trennung (Erwägungsgrund 26) gebeten.
- **Art. 11 Nr. 1 VO-E**: Es sollte in Erwägungsgrund 22 klargestellt werden, dass die Erbringung der Dienste auch die Entwicklung von Methoden sowie technischen und organisatorischen Maßnahmen für die Entwicklung dieses Dienstes umfasst. Hierzu zählt insb. die Sicherstellung der langfristigen Verfügbarkeit der für die Forschung verwendeten Daten einschließlich der physischen Speicherung, Lesbarkeit und Interpretierbarkeit, die Archivierung sowie die Qualitätssicherung von Datensätzen. Hierzu zählenferner etwa die Prüfung der Herkunft und der Vollständigkeit von Daten sowie die Sicherstellung der Nachvollziehbarkeit der Datenaufbereitung (z.B. der Anonymisierung) sowie die Korrektur von Datenfehlern. Wir bitten daher um Aufnahme folgender Passage in Erwägungsgrund 22 nach „(z.B. durch Umwandlung in bestimmte Formate)“: „Der Anbieter darf die Daten, für die er Dienste erbringt, auch für die Entwicklung von Methoden sowie von technischen und organisatorischen Maßnahmen für die Entwicklung dieses Dienstes verwenden. Hierzu zählt insb. die Sicherstellung der langfristigen Verfügbarkeit der verwendeten Daten einschließlich der physischen Speicherung, Lesbarkeit und Interpretierbarkeit, die Archivierung sowie die Qualitätssicherung von Datensätzen. Hierzu zählen ferner etwa die Prüfung der Herkunft und der Vollständigkeit von Daten sowie die Sicherstellung der Nachvollziehbarkeit der Datenaufbereitung (z.B. der Anonymisierung) sowie die Korrektur von Datenfehlern.“
- **Art. 11 Nr. 11 VO-E**: Es ist zu prüfen, ob für Datenmittler analog zum Datenaltruismus (Art. 22 VO-E) ein europäisches Einwilligungsformular bzw. einheitliche Mindestinhalte und Textbausteine entwickelt werden sollte. Dabei sind auch die berechtigten Interessen der wissenschaftlichen Forschung zu berücksichtigen.
- **Art. 13 VO-E:** Es wird um Klärung gebeten, welche Befugnisse die zuständige Behörde hat. Es ist zu erwägen, ob eine Auflistung wie in Kapitel 6 DSGVO möglich ist. Es bleibt bislang noch unklar, was gelten soll, wenn die zuständige Behörde im Rahmen der Überwachung nach Art. 13 VO-E keinen Verstoß gegen die VO feststellt, die zuständige Datenschutzaufsichtsbehörde hingegen zu dem Ergebnis kommt, dass die Tätigkeit eines

Dienstes nach Kapitel III nicht mit der DSGVO vereinbar ist. Eine Klarstellung der datenschutzrechtlichen Verantwortung ist erforderlich.

- **Art. 13 Abs. 4 VO-E:** Die vorgesehene Bußgeldvorschrift ist sehr unbestimmt, um eine einheitliche Umsetzung der VO in den MS zu garantieren. Zudem besteht Klärungsbedarf hinsichtlich der Formulierung „Zwangsgelder mit Rückwirkung". Zwangsgelder sind keine Strafen, sie dienen der Willensbeugung und sind damit notwendigerweise in die Zukunft gerichtet. Lediglich Geldstrafen und Bußgelder sind rückwirkende „Bestrafungen" für einen Verstoß.

4. Kapitel IV „Datenaltruismus"

Regelungen zu einer Vereinfachung von Formen des „Datenaltruismus" („data altruism") sind grundsätzlich zu begrüßen. So wurde auch in der Ratsschlussfolgerungen „COVID-19 lessons learned in health" deren Wichtigkeit bei der Bekämpfung grenzüberschreitender Gesundheitsgefahren betont. Allerdings bedarf es klarerer Abgrenzungen, einem verhältnismäßigem Bürokratie- und Verwaltungsaufwand, einer detaillierten Darstellung des Verhältnisses zur DSGVO und einer expliziten Berücksichtigung der Erfordernisse von Forschung und Wissenschaft.

Im Einzelnen ist die Abgrenzung zum „Dienst für die gemeinsame Datennutzung" nach Kapitel III bisher unklar. Als „Dienst für die gemeinsame Datennutzung" sind gemäß Art. 9 Abs. 1 Buchst. b u.a. „Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, und potenziellen Datennutzern (…)" anzusehen. Derartige „Vermittlungsdienste" scheinen aber zugleich auch zum Tätigkeitsprofil von „datenaltruistischen Organisationen" im Sinne des Kapitels IV zu gehören. Die Beschreibung der Tätigkeit einer „datenaltruistischen Organisation" erscheint widersprüchlich und unklar. In Erwägungsgrund 36 werden „datenaltruistische Organisationen" einerseits als juristische Personen beschrieben, die Daten „zur Verfügung stellen", wohingegen andererseits der Normtext (z.B. in Art. 17 Abs. 4 Buchst. h VO-E) davon spricht, dass datenaltruistische Organisationen Daten „sammeln" und somit offenbar selber verarbeiten. Es wird um Klarstellung gebeten, ob datenaltruistische Organisationen die Daten nur Dritten zur Verfügung stellen, die diese Daten dann für Zwecke von allgemeinem Interesse verwenden, oder ob sie Daten (auch oder ausschließlich?) selber zu Zwecken im allgemeinen Interesse verarbeiten. Zudem muss festgehalten werden, dass durch die Schaffung des neuen Instruments „Datenaltruismus" keine Aussage darüber getroffen wird, dass das Teilen von Daten nur noch über diesen Weg erfolgen darf. Die bisherigen Möglichkeiten, Daten zur wissenschaftlichen Nutzung frei zur Verfügung zu stellen, müssen erhalten bleiben.

Anmerkungen im Einzelnen:

- **Kapitel IV** setzt voraus, dass derjenige, der einer datenaltruistischen Organisation Daten übermittelt, der Dateninhaber ist (vgl. Art. 19 Abs. 1 VO-E). Es wird angeregt, dies ausdrücklich zu regeln. Es ist zu prüfen, ob auch klarer definiert werden sollte, was Gegenstand der datenaltruistischen Verarbeitungserlaubnis ist. Offen bleibt auch, wie die Qualität der Daten gesichert werden soll.
- **Art. 19 Abs. 2 VO-E:** Die rechtliche Funktion von Art. 19 Abs. 2 VO-E ist unklar: Für natürliche Personen (data subjects) besteht ein materieller Zweckbindungsgrundsatz bereits nach Art. 5 Abs. 1 Buchst. b DSGVO, der von einer datenaltruistischen Organisation (die aus deutscher Sicht datenschutzrechtlich verantwortlich sein dürfte) schon nach der DSGVO zu gewährleisten ist. Für juristische Personen (legal persons) gilt hingegen die DSGVO nicht. Art. 19 Abs. 2 VO-E scheint daher sowohl eine Aufgabe der datenaltruistischen Organisation, als auch – gleichzeitig – eine Art materiellen Zweckbindungsgrundsatz für juristische Personen zu regeln. Wir bitten daher um Klarstellung, welche Intention hinter Art. 19 Abs. 2 VO-E steht. Wir würden darüber hinaus bitten, in Ergänzung zu Erwägungsgrund 38 am Ende auch klarzustellen, dass für Daten außerhalb der DSGVO die Weiterverarbeitung für Zwecke der wissenschaftlichen Forschung möglich ist.
- **Art. 19 Abs. 3 VO-E:** Offen bleibt ferner, was die in Art. 19 Abs. 3 VO-E erwähnten „Werkzeuge zur Einholung der Einwilligung betroffener Personen“ praktisch sein sollen und wie sich die Pflichten nach Abs. 3 zu Art. 13, 14 DSGVO verhalten. Die datenaltruistischen Organisationen können hinsichtlich der Einwilligung als Interessenswalter und als technisches Hilfsmittel für Nutzerinnen und Nutzer dienen. Der Einsatz dieser Werkzeuge und die an diese Werkzeuge zu stellenden Anforderungen sollten daher in Kapitel IV detaillierter geregelt werden. Art. 19 Abs. 3 VO-E ist nicht ausreichend, da dort mit der Angabe des Hoheitsgebietes nur ein einzelner Aspekt geregelt ist.
- **Art. 20 Abs. 3 VO-E:** Es ist bislang unklar, wie die Aufgaben zwischen „zuständiger Behörde“ und Datenschutzaufsichtsbehörde geteilt werden sollen. Es bedarf einer klaren Regelung in der Verordnung, dass die Zuständigkeiten der unabhängigen Datenschutzaufsichtsbehörde unberührt bleiben. Insbesondere bedarf es der Klarstellung der Kompetenzen zwischen Behörden nach dem VO-E und den Datenschutzaufsichtsbehörden. Bislang ist unklar, was gelten soll, wenn die „zuständige Behörde“ im Rahmen der Überwachung nach Art. 21 VO-E keinen Verstoß gegen diesen Verordnungsentwurf feststellt, die zuständige Datenschutzaufsichtsbehörde hingegen zu dem Ergebnis kommt, dass eine datenaltruistische Organisation gegen die DSGVO verstößt.

- **Art. 22 VO-E:** In Bezug auf nicht personenbezogene Daten stellt sich die Frage, welche Rechtsnatur die „Einwilligung“ mittels des vorgeschlagenen Europäischen Einwilligungsformulars für Datenaltruismus haben soll (siehe dazu auch schon oben die Anmerkung zu Art. 2 Nummer 10 VO-E – statt „Einwilligung“ wird dort in Bezug auf nicht-personenbezogene Daten der Begriff der „Erlaubnis“ verwendet). Es sollte geprüft werden, ob ein Europäisches Einwilligungsformular auch jenseits von Anwendungen im Bereich des Datenaltruismus eine Regelung erfahren sollte. Es bedarf außerdem näherer Erläuterungen zu den Sicherungsmechanismen zur Einhaltung der DSGVO. Es ist zu prüfen, ob ein einheitliches europäisches Einwilligungsformular zweckmäßig ist, oder ob lediglich Mindestinhalte und Formulierungsbeispiele vorgegeben werden.
- **Art. 22 VO-E:** Ein Europäisches Einwilligungsformular sollte nicht als Durchführungsrechtsakt erlassen, sondern rechtsverbindlich von dem dafür kompetenten und zuständigen Europäischen Datenschutzausschuss beschlossen werden. Es ist bereits gesetzliche Aufgabe des Datenschutzausschusses, Leitlinien, Empfehlungen und Verfahren zu beschließen. Insofern ist hier mit einem Durchführungsrechtsakt kein neues bürokratisches Verfahren erforderlich. Auf jeden Fall sollte der Europäische Datenschutzausschuss umfassend bei dem Formular beteiligt werden.

5. Kapitel V „Zuständige Behörden und Verfahrensvorschriften“

Die Bestimmungen in **Art. 23 VO-E** enthalten eine Vielzahl von detaillierten Regelungen und Vorgaben für die nationalen Behörden. Die Kommission wird um Erläuterung zur Notwendigkeit und Verhältnismäßigkeit dieser Regelungen gebeten, da diese einen Eingriff in die Kompetenz und Organisationshoheit der Mitgliedstaaten bedeuten. Insbesondere das Verhältnis zu den bestehenden Datenschutzaufsichtsbehörden bedarf näherer Prüfung. Parallele Verfahren, unnötige Bürokratie und Zuständigkeiten dürfen nicht geschaffen werden.

6. Kapitel VI „Europäischer Dateninnovationsrat“

Der Vorschlag eines Europäischen Dateninnovationsrates wird grundsätzlich befürwortet, insbesondere da Standardisierung zur Verbesserung der Interoperabilität priorisiert wird. Eine enge Verzahnung mit anderen bereits bestehenden Vorhaben und Initiativen wie z.B. GAIA-X muss sichergestellt werden. Um eine möglichst umfassende Datennutzung zu ermöglichen, sollten auch Vertreter aus Wirtschaft und Gesellschaft sowie aus Wissenschaft und Forschung im Innovationsrat vertreten sein (**Art. 26 Abs. 1 VO-E**). Die Kommission wird gebeten, zu erläutern wer mit „Vertretern einschlägiger Datenräume“ gemeint ist bzw. wie diese bestimmt oder identifiziert werden sollen (**Art. 26 Abs. 1 VO-E**). Die Kommission wird gebeten zu erläutern, weshalb die Aufgaben in **Art. 27 VO-E** auf eine koordinierende Tätigkeit beschränkt sind. Die Bundesregierung regt an, die Aufgaben des Dateninnovationsrates auf **Empfehlungen zur**

innovationsfreundlichen Weiterentwicklung der Datenpolitik zu erstrecken und dabei **Impulse für gesteigerte Dateninnovation** zu fokussieren. Damit einher geht auch eine anwendungsorientierte Zusammensetzung des Rates, die entsprechende Expertise und einschlägige Praxiserfahrung wiederspiegelt.

7. Kapitel VII „Ausschuss und Delegierung“

Die Notwendigkeit des in **Art. 29 VO-E** vorgeschlagene Komitologie-Ausschusses bedarf der näheren Prüfung.

8. Kapitel VIII „Schlussbestimmungen“

Art. 30 VO-E: Es ist zu prüfen, ob die Anforderungen an den internationalen Zugang mit einem vertretbaren Umfang umgesetzt werden können. Des Weiteren ist eine Ausnahme für die Forschung zu erwägen. Es wird darauf hingewiesen, dass eine Vielzahl von Forschungsprojekten nur mit Beteiligung internationaler Wissenschaftler und Forschungseinrichtungen möglich ist. Die Nutzung von Forschungsdaten von Universitäten in den USA und Großbritannien könnte zumindest zeitweise erschwert werden, weil dies Drittstaaten sind, für die es noch keine Regelungen gibt (Art. 5 Abs. 9, 10 VO-E). Es wird um Klarstellung gebeten, ob ein bilaterales Abkommen ausreichen soll, oder ob ein EU-Abkommen/ ein Abkommen mit allen Mitgliedstaaten erforderlich ist.

Die in Art. 30 Abs. 4 VO-E verwendete Formulierung „zulässige Mindestmenge an Daten“ ist zu präzisieren, da es sich bei aggregierten oder verschlüsselten Daten um qualitative und nicht um quantitative Unterschiede handelt.