Der Bayerische Landesbeauftragte
für den Datenschutz

Daten-Governance-Rechtsakt

Auf dem Weg zu einem europäischen Binnenmarkt für Daten

Orientierungshilfe

Herausgeber:

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18
Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de
https://www.datenschutz-bayern.de

Bearbeiterin:

Dr. Verena Guttenberg

Version 1.0 | Stand: 1. Mai 2024

Diese Orientierungshilfe wird ausschließlich in elektronischer Form bereitgestellt. Sie kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Vorwort

Die Europäische Kommission wirkt auf einen „Binnenmarkt für Daten in der Europäischen Union“ hin. Darauf zielen unterschiedliche legislative Maßnahmen. Daten sollen verstärkt wirtschaftlich genutzt und datengetriebene Innovationen gefördert werden – soweit personenbezogene Daten betroffen sind, allerdings auf Basis der Datenschutz-Grundverordnung.

Teil dieser Strategie ist der Daten-Governance-Rechtsakt (im Folgenden: DGA), der durch unionseinheitliche Vorgaben das Vertrauen in den Datenaustausch stärken und gleichzeitig die Datenverfügbarkeit erhöhen soll. Hierdurch soll perspektivisch die Einrichtung und Entwicklung gemeinsamer europäischer Datenräume in strategischen Bereichen unterstützt werden. Die Verordnung zur Schaffung eines europäischen Raums für Gesundheitsdaten[1] bildet ein prominentes Beispiel.

Der Daten-Governance-Rechtsakt enthält vier Regelungsbereiche: Neben Mechanismen zur Erleichterung der Weiterverwendung bestimmter geschützter Daten des öffentlichen Sektors statuiert er Rahmenbedingungen für Datenvermittlungsdienste und Datenaltruismus sowie für den Transfer von nicht personenbezogenen Daten in und den Zugang zu solchen Daten durch Drittstaaten.

Der vorliegende Beitrag stellt den Daten-Governance-Rechtsakt in seiner Bedeutung für die bayerischen öffentlichen Stellen vor. Er beleuchtet zudem das Verhältnis zur Datenschutz-Grundverordnung und gibt Handlungsempfehlungen.

Der Daten-Governance-Rechtsakt gilt seit dem 24. September 2023 und wurde bislang noch nicht in nationales Recht umgesetzt; vor diesem Hintergrund kann die Orientierungshilfe nur eine Momentaufnahme bieten. Vorschläge zu Ausbau und Verbesserung sind daher besonders willkommen und erreichen den Bayerischen Landesbeauftragten für den Datenschutz unter der Adresse **orientierungshilfen@datenschutz-bayern.de**.

[1] Kommissionsvorschlag Mai 2022 (Internet: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:52022PC0197), Trilog-Einigung März 2024 (2022/0140[COD], Internet: https://www.consilium.europa.eu/media/70909/st07553-en24.pdf), aktueller Verfahrensstand unter https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0140(COD).

Inhaltsverzeichnis

I. Einführung

Durch Förderung von Datenaustausch und -nutzung unter gleichzeitiger Wahrung hoher Datenschutz-, Sicherheits- und Ethikstandards möchte die Europäische Kommission einen „europäischen Weg" für die Entwicklung der Datenwirtschaft begründen. Damit soll auch ein Gegenentwurf zum Druck einiger weniger großer Akteure mit erheblicher Marktmacht sowie zur – weniger reglementierten – Konkurrenz aus den Vereinigten Staaten von Amerika sowie aus China etabliert werden. Die am 19. Februar 2020 vorgestellte neue **europäische Datenstrategie** verfolgt daher das Ziel, durch **Schaffung eines Binnenmarkts für Daten** in der Europäischen Union vorhandene hochwertige Daten besser teilen und nutzen zu können. Hierfür soll insbesondere **mittels horizontaler Rechtsakte ein sektorübergreifender Governance-Rahmen** etabliert werden. 1

Hinweis: Sogenannte „**horizontale Rechtsakte**" treffen allgemeine sektorübergreifende Regelungen für ein spezifisches Rechtsgebiet, hier das Datennutzungsrecht. 2

Zu diesen horizontalen Rechtsakten zählt bereits der **europäische Datenschutz-Rechtsrahmen** mit der Datenschutz-Grundverordnung[2] (DSGVO), welche Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten enthält, sowie mit der Verordnung (EU) 2018/1807 betreffend nicht-personenbezogene Daten.[3] Daneben treten sukzessive weitere horizontale Rechtsakte, von denen für die öffentliche Hand unter anderem der **Daten-Governance-Rechtsakt**[4] von besonderer Relevanz ist. 3

Der Daten-Governance-Rechtsakt wurde am 30. Mai 2022 verabschiedet, trat am 23. Juni 2022 in Kraft und **gilt seit dem 24. September 2023** (Art. 38 DGA). In Deutschland ist zum Zeitpunkt der Veröffentlichung dieser Orientierungshilfe nicht klar, wann und in welcher Form die Verordnung national ausgestaltet werden soll, so dass die den Mitgliedstaaten obliegenden Fragen derzeit nicht geregelt sind und die nationalen Umsetzungsregelungen auch nicht bewertet werden können. 4

Der Daten-Governance-Rechtsakt soll Strukturen etablieren, welche die Verfügbarkeit von – **sowohl personenbezogenen als auch nicht personenbezogenen**[5] – **Daten in digitalen** 5

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU L 119 vom 4. Mai 2016, S. 1.

[3] 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, ABl. EU L 303 vom 28. November 2018, S. 59.

[4] Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. EU L 152 vom 3. Juni 2022, S. 1.

[5] Zur – redundanten, da offensichtlichen – Definition „nicht personenbezogener Daten" vergleiche Art. 2 Nr. 4 DGA.

Formaten (vergleiche Art. 2 Nr. 1 DGA)[6] zur wirtschaftlichen Nutzung erhöhen und datengetriebene Innovationen ermöglichen und fördern. Gleichzeitig soll er die Einhaltung des bestehenden Datenschutz-Rechtsrahmens gewährleisteten. Insbesondere soll diese Datennutzung in Einklang gebracht werden mit dem Schutz von personenbezogenen Daten sowie von Geschäftsgeheimnissen, Urheberrechten und gewerblichen Schutzrechten, um das Vertrauen in eine sichere und rechtmäßige Datennutzung zu steigern.

6 Die Verordnung enthält dabei keine umfassende Regulierung der Datennutzung. Vielmehr begnügt sich der unionale Gesetzgeber mit der **sektorübergreifenden Regelung einzelner Bausteine**: So umfasst der Daten-Governance-Rechtsakt Vorgaben für die Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen (Kapitel II), die Erbringung von Datenvermittlungsdiensten (Kapitel III), für Datenaltruismus (Kapitel IV) sowie für die Einrichtung eines Europäischen Dateninnovationsrats (Kapitel VI). Dazu treten als Teil der EU-Datenstrategie **weitere „Schwesterverordnungen“** wie das Datengesetz (Entwurf),[7] das Gesetz über digitale Märkte[8] sowie das Gesetz über digitale Dienste.[9] Zudem wurden in der Vergangenheit mit der Datenschutz-Grundverordnung und der Richtlinie über offene Daten[10] bereits wesentliche Eckpfeiler für die Datennutzung etabliert.

6 Die Datenschutz-Grundverordnung als Regelung zum Schutz personenbezogener Daten erfasst dagegen nach Art. 4 Nr. 1 DSGVO sämtliche Formen von Daten.

7 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM(2022) 68 final, Internet: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2022)68&lang=de.

8 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. EU L 265 vom 12. Oktober 2022, S. 1.

9 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. EU L 277 vom 27. Oktober 2022, S. 1.

10 Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors, ABl. EU L 172 vom 26. Juni 2019, S. 56.

II. Anwendungsbereich

Aufgrund der zahlreichen Berührungspunkte mit anderen europäischen und nationalen Rechtsakten finden sich in **Art. 1 DGA** umfangreiche **Beschränkungen des Anwendungsbereichs**, die im Rahmen der Trilog-Beratungen in ihrer Deutlichkeit verschärft wurden: 7

- **Art. 1 Abs. 2 UAbs. 1 DGA** stellt ausdrücklich klar, dass die Verordnung für öffentliche Stellen **keine Verpflichtung begründet, die Weiterverwendung von Daten zu erlauben**, und öffentliche Stellen auch **nicht von ihren Geheimhaltungspflichten** (beispielsweise dem Steuergeheimnis nach § 30 Abs. 1 Abgabenordnung oder dem Geheimnisschutz im Verwaltungsverfahren gemäß Art. 30 BayVwVfG) **befreit**. 8

- Sektorspezifisches Unionsrecht oder nationales Recht, das **zusätzliche** technische, administrative oder organisatorische **Anforderungen an öffentliche Stellen, Anbieter von Datenvermittlungsdiensten oder anerkannte Erbringer datenaltruistischer Dienste** enthält, ist gemäß **Art. 1 Abs. 2 UAbs. 3 DGA** ergänzend anwendbar, vorausgesetzt, die zusätzlichen Anforderungen sind nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt. 9

- **Europäische und nationale Rechtsakte über den Schutz personenbezogener Daten** einschließlich der Befugnisse der Aufsichtsbehörden, insbesondere die Datenschutz-Grundverordnung und die ePrivacy-Richtlinie,[11] finden nach **Art. 1 Abs. 3 Satz 1 DGA** für die Verarbeitung personenbezogener Daten auf der Grundlage des Daten-Governance-Rechtsaktes **Anwendung** und haben **gemäß Art. 1 Abs. 3 Satz 2 DGA im Konfliktfall Vorrang**. Dies gilt ausweislich **Erwägungsgrund (EG) 4 Satz 1 DGA** auch in den Fällen, in denen **personenbezogene und nicht personenbezogene Daten in einem Datensatz untrennbar** miteinander verbunden[12] sind. Zudem schafft der Daten-Governance-Rechtsakt „**keine Rechtsgrundlage** für die Verarbeitung personenbezogener Daten" (**Art. 1 Abs. 3 Satz 4 DGA**) und **berührt** auch **nicht** die **in der Datenschutz-Grundverordnung festgelegten Rechte und Pflichten** (**Art. 1 Abs. 3 Satz 4 DGA**). 10

- Schließlich sollen neben den datenschutzrechtlichen Bestimmungen auch die Anwendung des Wettbewerbsrechts sowie die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten im Bereich der öffentlichen Sicherheit, der Landesverteidigung und der nationalen Sicherheit unberührt bleiben, **Art. 1 Abs. 4 und 5 DGA**. 11

[11] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG L 201 vom 31. Juli 2022, S. 37.

[12] Zum Begriff „untrennbar miteinander verbunden" vergleiche Mitteilung der Kommission an das Europäische Parlament und den Rat, Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, COM(2019) 250 final, Internet: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2019)250&lang=de, S. 9 f.

II. Anwendungsbereich

12 Der Daten-Governance-Rechtsakt soll also die Regelungen insbesondere der Datenschutz-Grundverordnung unangetastet lassen[13] und übernimmt sogar die Begriffsbestimmungen für „personenbezogene Daten" (Art. 2 Nr. 3 DGA), „Einwilligung" (Art. 2 Nr. 5 DGA), „betroffene Person" (Art. 2 Nr. 7 DGA)[14] und „Verarbeitung" (Art. 2 Nr. 12 DGA). Demnach ist das Verhältnis Datenschutz-Grundverordnung – Daten-Governance-Rechtsakt auf den ersten Blick eindeutig zugunsten der Datenschutz-Grundverordnung geregelt. Dem widerspricht allerdings die Verordnungs-Realität: Der Daten-Governance-Rechtsakt reguliert den Umgang mit personenbezogenen sowie mit nicht personenbezogenen Daten gleichermaßen und bringt für personenbezogene Daten, die von der Datenschutz-Grundverordnung geschützt werden, bei grundlegenden Fragen Überschneidungen, Widersprüche, begriffliche Inkohärenzen und Regelungslücken mit sich, die im Folgenden im Zusammenhang mit der jeweiligen Vorschrift besprochen werden.[15]

[13] Bemerkenswert ist in diesem Zusammenhang, dass die Europäische Union die Datenschutz-Grundverordnung offenbar nicht mehr für ausreichend zur Vertrauensbildung und -förderung hält, siehe EG 5 DGA: „Es muss auf Unionsebene gehandelt werden, um das Vertrauen in die gemeinsame Datennutzung zu stärken, indem geeignete Mechanismen geschaffen werden, die es den betroffenen Personen und Dateninhabern ermöglichen, Kontrolle über die sie betreffenden Daten auszuüben, und sonstige Hemmnisse für eine gut funktionierende und wettbewerbsfähige datengesteuerte Wirtschaft abzubauen."

[14] Zu unterscheiden vom „Dateninhaber" nach Art. 2 Nr. 8 DGA.

[15] Für eine geltungserhaltend restriktive Auslegung der Vorgaben des Daten-Governance-Rechtsaktes Brink/v. Ungern-Sternberg, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 11/2023, Art. 1 DGA Rn. 53.

III. Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz öffentlicher Stellen

1. Konzept der Weiterverwendung von Daten im Besitz öffentlicher Stellen

Eines der Ziele des Daten-Governance-Rechtsaktes ist die Förderung der Weiterverwendung von bestimmten Kategorien geschützter Daten im Besitz öffentlicher Stellen im Sinne einer technisch-faktischen Herrschaft über die Daten[16] (englische Sprachfassung: „data held by public sector bodies"). Begründet wird dies damit, dass Daten, die von öffentlichen Stellen unter Einsatz öffentlicher Mittel erhoben oder generiert wurden, auch der Gesellschaft zugutekommen sollen (EG 6 Satz 1 DGA), selbst wenn sie bestimmten Schutzrechten unterliegen. Bislang würden solche Daten nur unzureichend genutzt (EG 6 Satz 6 DGA). Daher sollen mit dem Daten-Governance-Rechtsakt in der gesamten Union einheitliche Bedingungen für den Zugang zu solchen und die Nutzung solcher Daten etabliert werden (EG 6 Satz 8 DGA). 13

Auf unionsrechtlicher Ebene gab es mit der 2019 novellierten und 2021 in Deutschland durch das Datennutzungsgesetz[17] umgesetzten **Richtlinie (EU) 2019/1024** bis jetzt nur eine Regelung der Weiterverwendung von für jedermann frei verwendbaren „offenen" Daten des öffentlichen Sektors auf der Grundlage nationaler Zugangsansprüche. Der Daten-Governance-Rechtsakt soll nun eine **komplementäre** Regelung für die Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz der öffentlichen Hand treffen. 14

Ein Zugang zu solchen geschützten Daten der öffentlichen Hand war bisher nur unter den Voraussetzungen der Datenschutz-Grundverordnung möglich und in Deutschland vor allem für die Wissenschaft im Zusammenhang mit Daten der gesetzlichen Krankenversicherung (sogenannte **„Datentransparenz" nach § 303a bis § 303f Fünftes Buch Sozialgesetzbuch - Gesetzliche Krankenversicherung** [SGB V]), mit Inkrafttreten des **Gesundheitsdatennutzungsgesetzes** am 26. März 2024 erweitert auf die Nutzung von Gesundheitsdaten zu gemeinwohlorientieren Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens, sowie mit den **Forschungsdatenzentren** (zum Beispiel § 16 Abs. 6 Gesetz über die Statistik für Bundeszwecke) etabliert. 15

Die Zielsetzung des Daten-Governance-Rechtsakts ist institutioneller Natur: er beschränkt sich auf die einheitliche Regelung grundlegender Bedingungen für eine Weiterverwendung. Er begründet **weder eine Verpflichtung, die Weiterverwendung von Daten zu erlauben**, die sich im Besitz öffentlicher Stellen befinden, **noch bewirkt er eine Erweiterung entsprechender Zugangsrechte** (**Art. 1 Abs. 2 UAbs. 1**, **EG 11 Satz 1 DGA**). Es obliegt mithin den einzelnen Mitgliedstaaten – vorbehaltlich Transparenzvorgaben für öffentliche Stellen – 16

[16] Brink/v. Ungern-Sternberg, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 11/2023, Art. 1 DGA Rn. 23.

[17] Gesetz für die Nutzung von Daten des öffentlichen Sektors vom 16. Juli 2021 (Datennutzungsgesetz – DNG), BGBl. I S: 2941, 2942; 4114.

grundsätzlich zu entscheiden, ob geschützte Daten im Besitz öffentlicher Stellen zur Weiterverwendung zugänglich gemacht werden, und auch, inwieweit ein solcher Zugang hinsichtlich des Zwecks und des Umfangs begrenzt wird. Der Daten-Governance-Rechtsakt schafft keine neuen Zugangs- und Weiterverwendungsrechte hinsichtlich geschützter Daten der öffentlichen Hand. Er enthält auch **keine Rechtsgrundlagen für eine Verarbeitung personenbezogener Daten, Art. 1 Abs. 3 Satz 4 DGA**. Zugangsrechte zu bestimmten Datensätzen oder Dokumenten richten sich damit (weiterhin) ausschließlich nach nationalem Recht; insbesondere bleibt der Ausgleich von Grundrechtspositionen in Zugangsrechten und ihren Grenzen allein den Mitgliedstaaten überlassen.

17 **Informationszugangsrechte allgemein:**
In **Deutschland und Bayern** kommen als Zugangsrechte beispielsweise **§ 12a E-Government-Gesetz** (EGovG), **§ 1 Informationsfreiheitsgesetz** (IFG), **Art. 39 Abs. 1 Satz 1 Bayerisches Datenschutzgesetz** (BayDSG) sowie bereichsspezifische Informationszugangsrechte wie **§ 2 Abs. 1 Verbraucherinformationsgesetz** (VIG) und **Art. 3 Abs. 1 Satz 1 Bayerisches Umweltinformationsgesetz** (BayUIG) in Betracht.[18]

Sind Gegenstand des Zugangsanspruchs für jedermann frei verwendbare „**offene" Daten** des öffentlichen Sektors beziehungsweise öffentlich finanzierte Daten, gelten neben den Voraussetzungen und Beschränkungen des jeweiligen Zugangsanspruchs die Vorgaben des **Datennutzungsgesetzes** (§ 2 DNG).

Geht es um Zugangs- und Weiterverwendungsrechte hinsichtlich **geschützter Daten der öffentlichen Hand**, findet als „übergeordneter Rahmen" der **Daten-Governance-Rechtsakt** Anwendung (vergleich auch § 2 Abs. 3 Nr. 1 Buchst. 1 DNG), wobei er die nationalen Bestimmungen unberührt lässt, Art. 1 Abs. 2 UAbs. 2, UAbs. 3 DGA.

18 **Insbesondere die Informationszugangsrechte im bayerischen Landesrecht:**
Der bayerische Gesetzgeber hat einen anderen Regelungsansatz als der Bund und andere Länder gewählt und statt Erlass eines spezifischen Informationsfreiheitsgesetzes in **Art. 39 BayDSG** ein **allgemeines Auskunftsrecht** etabliert, welches von § 9 Abs. 1 Satz 1 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern (AGO) als verwaltungsvorschriftliches Gegenstück ergänzt wird.[19] Nach Art. 39 Abs. 1 Satz 1 BayDSG hat jeder grundsätzlich das Recht auf Auskunft über den Inhalt von Dateien und Akten öffentlicher Stellen, soweit ein berechtigtes, nicht auf eine entgeltliche Weiterverwendung gerichtetes Interesse glaubhaft dargelegt wird und (Nr. 1) bei personenbezogenen Daten eine Übermittlung an nicht öffentliche Stellen zulässig ist sowie (Nr. 2) Belange der öffentlichen Sicherheit und Ordnung nicht beeinträchtigt werden. Weder der Kreis der Berechtigten noch die in Betracht kommenden Informationen sind dabei begrenzt. Art. 39 Abs. 3 und 4 BayDSG regeln inhaltliche (Verschlusssachen, Berufs- oder Amtsgeheimnisse sowie persönlicher Lebensbereich oder Betriebs- und Geschäftsgeheimnisse) und institutionelle Ausnahmen.

Dieses allgemeine Auskunftsrecht ist gemäß Art. 39 Abs. 2 BayDSG grundsätzlich nachrangig zu anderen Informationszugangsrechten wie beispielsweise

[18] Überblick bei Engelbrecht, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 4/2023, Art. 39 BayDSG Rn. 150 ff.

[19] Umfassend hierzu Engelbrecht, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 4/2023, Art. 39 BayDSG Rn. 150 ff.

- dem voraussetzungslos gewährten **Anspruch auf Zugang zu Umweltinformationen**[20] nach **Art. 3 Abs. 1 Satz 1 BayUIG** mit Einschränkungen nach Art. 7 (Schutz öffentlicher Belange) und Art. 8 BayUIG (Schutz sonstiger Belange) sowie
- dem **Anspruch auf freien Zugang zu gesundheitsbezogenen Verbraucherinformationen**[21] nach **§ 2 Abs. 1 VIG**, vorbehaltlich der Ausschluss- und Beschränkungsgründe nach § 3 VIG.

Bestehen nach nationalem Recht Zugangs- und Weiterverwendungsrechte für bestimmte Datensätze oder Dokumente im Besitz der öffentlichen Hand, gelten für die Ausgestaltung dieser Rechte nun die Vorgaben des Kapitels II DGA. Besondere Bestimmungen des nationalen Rechts und damit insbesondere nationale Zugangsvoraussetzungen und -beschränkungen bleiben allerdings unberührt, Art. 1 Abs. 2 UAbs. 2, UAbs. 3 DGA. 19

Praxistipp: Bayerische öffentliche Stellen sollten sich zunächst vergegenwärtigen, ob und, wenn ja, welche nationalrechtlichen Informationszugangsansprüche neben dem allgemeinen Auskunftsrecht aus Art. 39 Abs. 1 Satz 1 BayDSG ihren jeweiligen Aufgabenbereich betreffen und welche Voraussetzungen, welchen Umfang und welche Beschränkungen diese haben. Anschließend sollten die öffentlichen Stellen die im Folgenden detaillierten neuen Vorgaben des Daten-Governance-Rechtsaktes prüfen und diese – soweit erforderlich – praktisch umsetzen. 20

Grundvoraussetzung für eine Weiterverwendung bestimmter Kategorien geschützter Daten im Besitz der öffentlichen Hand ist somit weiterhin ein entsprechender nationalrechtlicher Anspruch, der gegebenenfalls nur unter bestimmten Voraussetzungen gewährt wird. Durch den Daten-Governance-Rechtsakt **neu eingeführt sind verschiedene Instrumente, mittels derer die betreffende öffentliche Stelle Zugang zu an sich geschützten Daten gewähren kann und die im Zusammenhang mit der Entscheidung über die Zugangsgewährung Berücksichtigung finden**: Bisher konnten öffentliche Stellen bestimmte Anspruchshindernisse (zum Beispiel Art. 39 Abs. 1 Satz 2 BayDSG) auf Grund einer Ermessensentscheidung dem Anspruch entgegensetzen und diesen nicht erfüllen. Nunmehr stehen nach dem Daten-Governance-Rechtsakt zusätzlich verschiedene – differenzierte – Methoden der Zugangsgewährung zur Verfügung (siehe Art. 5 DGA, Rn. 35 ff.). 21

[20] „Umweltinformationen" sind nach Art. 2 Abs. 2 BayUIG „alle Daten über 1. den Zustand von Umweltbestandteilen […] sowie die Wechselwirkungen zwischen diesen Bestandteilen, 2. Faktoren […], die sich auf die Umweltbestandteile im Sinn der Nr. 1 auswirken oder wahrscheinlich auswirken, 3. Maßnahmen oder Tätigkeiten, die a) sich auf die Umweltbestandteile im Sinn der Nr. 1 oder Faktoren im Sinn der Nr. 2 auswirken oder wahrscheinlich auswirken oder b) den Schutz von Umweltbestandteilen im Sinn der Nr. 1 bezwecken; […] 4. Berichte über die Umsetzung des Umweltrechts, 5. Kosten-Nutzen-Analysen oder sonstige wirtschaftliche Analysen und Annahmen […], und 6. den Zustand der menschlichen Gesundheit und Sicherheit, die Lebensbedingungen des Menschen sowie Kulturstätten und Bauwerke, soweit sie jeweils vom Zustand der Umweltbestandteile im Sinn der Nr. 1 oder von Faktoren, Maßnahmen oder Tätigkeiten im Sinn der Nrn. 2 und 3 betroffen sind oder sein können; […]".

[21] Gegenstand des Zugangsanspruchs sind gemäß § 1 VIG die „bei informationspflichtigen Stellen vorliegenden Informationen über 1. Erzeugnisse im Sinne des Lebensmittel- und Futtermittelgesetzbuches (Erzeugnisse) sowie 2. Verbraucherprodukte, die dem § 2 Nummer 25 des Produktsicherheitsgesetzes unterfallen (Verbraucherprodukte)" mit Konkretisierungen in § 2 Abs. 1 VIG.

III. Weiterverwendung bestimmter Kategorien geschützter Daten

22 Vorbehaltlich verfahrensrechtlicher Sonderregelungen (wie beispielsweise im Informationsfreiheitsgesetz oder im Bayerischen Umweltinformationsgesetz) werden diese Zugangsansprüche zumindest bei **Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen und damit Behörden** im Sinne des Art. 1 Abs. 2 Bayerisches Verwaltungsverfahrensgesetz (BayVwVfG) sind, als Teil der **öffentlich-rechtlichen Verwaltungstätigkeit** nach den **allgemeinen Regeln des Verwaltungsverfahrens** realisiert, in Bayern auf der Grundlage des **Bayerischen Verwaltungsverfahrensgesetzes** mit insbesondere Antragsverfahren, Anhörungserfordernissen und Bescheid.[22] Die Entscheidung über die Zugangsgewährung erfolgt in Form eines **Verwaltungsaktes im Sinne des Art. 35 Abs. 1 Satz 1 BayVwVfG**,[23] gegebenenfalls mit **Nebenbestimmungen nach Art. 36 BayVwVfG** (siehe unten Rn. 36 ff., 64), dessen Ausgestaltung je nach Rechtsgrundlage einem gewissen Ermessensspielraum der zuständigen öffentlichen Stelle unterliegt.

23 **Sonstigen öffentlichen Stellen** fehlt es dagegen an der für ein hoheitliches Handeln erforderlichen Rechtsmacht; das **Verfahren** richtet sich bei diesen ausschließlich nach der **jeweiligen Rechtsgrundlage für den Informationszugangsanspruch**.

24 Für die zeitliche Bearbeitung der Anträge auf Weiterverwendung enthält Art. 9 DGA eine spezielle Fristenregelung (näher Rn. 55).

2. Bedingungen für die Weiterverwendung geschützter Daten

25 Zur Verbesserung der Rahmenbedingungen für die gemeinsame Datennutzung im Binnenmarkt (EG 3 DGA) legt der Daten-Governance-Rechtsakt in Art. 4 ff. DGA die Anforderungen für die Weiterverwendung geschützter Daten im Besitz öffentlicher Stellen fest.

26 Unter einer „**Weiterverwendung**“ ist dabei gemäß **Art. 2 Nr. 2 DGA** die „Nutzung von Daten, die im Besitz öffentlicher Stellen sind, durch natürliche oder juristische Personen für kommerzielle oder nichtkommerzielle Zwecke, die sich von dem ursprünglichen Zweck […] unterscheiden“ und nicht den Austausch von Daten zwischen öffentlichen Stellen zur Erfüllung ihres öffentlichen Auftrags betreffen, zu verstehen.

27 „**Öffentliche Stellen**“ in diesem Sinne sind gemäß **Art. 2 Nr. 17 DGA** der Staat, Gebietskörperschaften, Einrichtungen des öffentlichen Rechts oder Verbände, die aus einer oder mehreren dieser Körperschaften oder einer oder mehreren dieser Einrichtungen des öffentlichen Rechts bestehen. „**Einrichtungen des öffentlichen Rechts**“ weisen dabei die in **Art. 2 Nr. 18 DGA** aufgeführten Eigenschaften auf. **Forschungseinrichtungen und Forschungsfördereinrichtungen** können auch als öffentliche Stellen oder Einrichtungen des öffentlichen Rechts aufgestellt sein. Für diese gilt der Daten-Governance-Rechtsakt nur in Bezug auf ihre Funktion als Forschungs(förder)einrichtung, EG 12 UAbs. 2 Satz 1 DGA. **Keine Einrichtungen des öffentlichen Rechts** nach dem Verständnis des Daten-Governance-Rechtsaktes sind dagegen ausweislich des Definitionsmerkmals des Art. 2 Nr. 18 Buchst. c DGA **Innungen, Handwerks-, Berufs- sowie Industrie- und Handelskammern**, da diese zwar der

[22] Zum Ganzen Engelbrecht, in: Wilde/Ehmann/Niese/Knoblauch, Datenschutz in Bayern, Stand 4/2023, Art. 39 BayDSG Rn. 177 ff.

[23] BayVGH, Urteil vom 13. Mai 2019, 4 B 18.1515, Rn. 27.

Rechtsaufsicht des Staates unterliegen, aber nicht überwiegend staatlich, sondern durch Mitgliedsbeiträge und gegebenenfalls Gebühren und Entgelte finanziert werden.[24]

Gegenstand einer Weiterverwendung nach dem Daten-Governance-Rechtsakt sind „**bestimmte Kategorien geschützter Daten**". Diesen **geschützten Datenkategorien** unterfallen gemäß der abschließenden Regelung des **Art. 3 Abs. 1 DGA** Daten im Besitz öffentlicher Stellen, die geschäftlicher oder statistischer Geheimhaltung (Buchstabe a und b), dem Schutz geistigen Eigentums Dritter (Buchstabe c) oder dem Schutz personenbezogener Daten außerhalb des Anwendungsbereichs der Richtlinie (EU) 2019/1024 (Buchstabe d) unterliegen. **Nicht erfasst** sind dagegen nach **Art. 3 Abs. 2 DGA** Daten im Besitz öffentlicher Unternehmen, öffentlich-rechtlicher Rundfunkanstalten oder Kultur- und Bildungseinrichtungen, aus Gründen der öffentlichen Sicherheit, der Landesverteidigung oder der nationalen Sicherheit geschützte Daten sowie Daten, deren Bereitstellung nicht unter den öffentlichen Auftrag der betreffenden öffentlichen Stelle fällt. **28**

Die Tatsache, dass von der Weiterverwendung nach dem Daten-Governance-Rechtsakt gemäß **Art. 3 Abs. 1 Buchst. d DGA** auch **personenbezogene Daten** erfasst sind, die dem Regime der **Datenschutz-Grundverordnung** unterliegen, öffnet den Problemkreis von Zusammenspiel und Wechselwirkung der beiden Rechtsakte. Der Begriff der „Weiterverwendung" ähnelt dem in Art. 5 Abs. 1 Buchst. b DSGVO verwendeten Begriff der „Weiterverarbeitung" und erweist sich bei einer Gegenüberstellung als Unterfall. In der Konsequenz müssen die Vorgaben der Datenschutz-Grundverordnung für „Weiterverarbeitungen" in Art. 5 Abs. 1 Buchst. b und Art. 6 Abs. 4 DSGVO auch für „Weiterverwendungen" personenbezogener Daten auf der Grundlage des Daten-Governance-Rechtsaktes beachtet werden. **29**

Art. 4 Abs. 1 DGA statuiert ein **grundsätzliches Verbot von Ausschließlichkeitsvereinbarungen** für die Weiterverwendung. Eine – zeitlich begrenzte – **Ausnahme** gilt nach **Art. 4 Abs. 2 ff. DGA**, soweit ein solches ausschließliches Recht für die Erbringung eines Dienstes oder die Bereitstellung eines Produkts im allgemeinen Interesse erforderlich ist, vorausgesetzt die Erbringung oder Bereitstellung wären ohne die Ausschließlichkeitsvereinbarung nicht möglich. **30**

Art. 5 DGA listet sodann als Kern des Kapitels II – unter Berücksichtigung datenschutzrechtlicher Belange – eine Vielzahl von einzelnen **Möglichkeiten und Bedingungen für die Weiterverwendung** auf. Die für die Gewährung oder Verweigerung des Zugangs zur Weiterverwendung von geschützten Daten zuständigen öffentlichen Stellen können dabei gemäß Art. 5 Abs. 1 Satz 2 DGA von den in Art. 7 Abs. 1 DGA genannten zuständigen Stellen unterstützt werden (siehe Rn. 70). **31**

Zusammengefasst stellen sich die neuen Instrumente für Zugang und Weiterverwendung auf der Grundlage eines gestuften Schutzkonzepts nach Art. 5 DGA folgendermaßen dar: **32**

[24] Infolge einer Änderung des Verordnungsentwurfs wurden Innungen, Handwerks-, Berufs- sowie Industrie- und Handelskammern vom Definitionsbereich des Art. 2 Nr. 18 DGA gezielt ausgeschlossen.

III. Weiterverwendung bestimmter Kategorien geschützter Daten

Grundvoraussetzungen für alle Weiterverwendungen

- **Art. 5 Abs. 1 DGA:** Pflicht zur Publikation der Bedingungen für die Weiterverwendung sowie des Antragsverfahrens bei der zentralen Informationsstelle (Rn. 34)
- **Art. 5 Abs. 2 DGA:** Festlegung von nichtdiskriminierenden, transparenten, verhältnismäßigen und objektiv gerechtfertigten Bedingungen für die Weiterverwendung (Rn. 33)
- **Art. 5 Abs. 3 DGA:** Pflicht zur Sicherstellung des Schutzes der Daten (Rn. 35)
- **Art. 5 Abs. 7 DGA:** Wahrung der Rechte des geistigen Eigentums (Rn. 48)
- **Art. 5 Abs. 8 DGA:** Gewährleistung geschäftlicher oder statistischer Geheimhaltung (Rn. 50)
- **Art. 5 Abs. 5 DGA:** Geheimhaltungsverpflichtung für die Weiterverwendung, sofern nicht im nationalen Recht vorgesehen (Rn. 45)

Stufe 1: Weiterverwendungen nach Art. 5 Abs. 3 und 4 DGA

- **Art. 5 Abs. 3 Satz 2 Buchst. a DGA:** Zugang zur Weiterverwendung von Daten (Rn. 36)
  - **Art. 5 Abs. 3 Satz 2 Buchst. a Ziff. i DGA:** Anonymisierung personenbezogener Daten (Rn. 36)
  - **Art. 5 Abs. 3 Satz 2 Buchst. a Ziff. ii DGA:** Veränderung, Aggregation oder Aufbereitung nach einer anderen Methode der Offenlegungskontrolle für vertrauliche Geschäftsinformationen (Rn. 36)
- **Art. 5 Abs. 3 Satz 2 Buchst. b DGA:** Zugang durch Fernzugriff in einer sicheren Verarbeitungsumgebung (Rn. 36)
- **Art. 5 Abs. 3 Satz 2 Buchst. c DGA:** Zugang innerhalb der physischen Räumlichkeiten der sicheren Verarbeitungsumgebung (Rn. 36)
- **Art. 5 Abs. 4 DGA:** Bedingungen zur Sicherstellung der Integrität der technischen Systeme sowie zur Überprüfung und ggf. zum Verbot der Verwendung der Ergebnisse der Weiterverwendung (Rn. 43)

Wenn keine Weiterverwendungen nach Art. 5 Abs. 3 und 4 DGA:

Stufe 2: Weiterverwendungen nach Art. 5 Abs. 6 DGA auf der Grundlage einer Einwilligung oder Erlaubnis (Rn. 47)

Stufe 3: Übertragung von Daten in ein Drittland im Zusammenhang mit der Weiterverwendung

- **Art. 44 ff. DSGVO** für personenbezogene Daten
- **Art. 5 Abs. 9 bis 14 DGA** für nicht personenbezogene Daten
  - **Art. 5 Abs. 9 DGA:** Unterrichtungspflicht des Weiterverwenders (Rn. 62)
  - **Art. 5 Abs. 14 DGA:** Drittlandübermittlung nur nach Abs. 10, 12 und 13 – **Art. 5 Abs. 12 DGA:** Angemessenheitsbeschluss (Rn. 67) – **Art. 5 Abs. 10 DGA:** vertragliche Verpflichtungen des Weiterverwenders (Rn. 63) – **Art. 5 Abs. 13 DGA:** hochsensible Kategorien nicht personenbezogener Daten (Rn. 68)

33 Grundlegend bestimmt **Art. 5 Abs. 2 DGA**, dass die Bedingungen für die Weiterverwendung in Bezug auf die Datenkategorien, die Zwecke der Weiterverwendung und die Art der Daten, deren Weiterverwendung erlaubt wird, **nichtdiskriminierend, transparent, verhältnismäßig und objektiv gerechtfertigt** sein müssen und den **Wettbewerb nicht behindern** dürfen. Mit dieser Regelung **ergänzt** der Daten-Governance-Rechtsakt für personenbezogene Daten die Bestimmung des **Art. 6 Abs. 4 DSGVO**, wonach eine Rechtsvorschrift der Mitgliedstaaten, die die zweckändernde Weitverarbeitung erlaubt, eine „in einer demokratischen

Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele“ darstellen muss. Allerdings wären diskriminierende, intransparente, unverhältnismäßige, objektiv nicht gerechtfertigte und wettbewerbshindernde Weiterverwendungsbedingungen nach deutschem Recht ohnehin unzulässig. Fraglich ist nur, ob die verstärkte Weiterverwendung von Daten des öffentlichen Sektors als „sonstiges wichtiges Ziel des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaates“ im Sinne von Art. 23 Abs. 1 Buchst. e DSGVO angesehen werden könnte, wodurch der Geltungsbereich des Art. 6 Abs. 4 DSGVO erweitert würde. Dies ist aber aufgrund eines Vergleichs mit den in Art. 23 Abs. 1 Buchst. e DSGVO genannten Interessen („etwa […] Währungs-, Haushalts- und Steuerbereich sowie […] Bereich der öffentlichen Gesundheit und der sozialen Sicherheit“) sowie dem Gebot einer engen Auslegung des vagen Beschränkungstatbestands im Kontext des abschließenden Zweckkatalogs des Art. 23 Abs. 1 DSGVO zu verneinen.

Diese Bedingungen für die Weiterverwendung müssen ebenso wie das Verfahren für die Beantragung einer Weiterverwendung über die zentrale Informationsstelle nach Art. 8 DGA **öffentlich zugänglich sein**, **Art. 5 Abs. 1 DGA**. Für personenbezogene Daten ist die Publikationspflicht wohl nur deklaratorischer Natur, da die Weitergabe personenbezogener Daten an Dritte ohnehin gesetzlich geregelt sein muss und Gesetze öffentlich zugänglich sind, vergleiche auch Art. 6 Abs. 4 DSGVO. Neu ist die Verpflichtung zur zentralen Zugänglichmachung des Verfahrens zur Beantragung. 34

Die öffentlichen Stellen sind gemäß **Art. 5 Abs. 3 Satz 1 DGA** verpflichtet **sicherzustellen**, dass die **jeweiligen Daten geschützt** bleiben. **Art. 5 Abs. 3 Satz 2 DGA** sieht dabei **drei zusätzliche Anforderungen** für den Schutz der Daten vor, die die öffentlichen Stellen an die Weiterverwendung vorschreiben können. Diese sind dem Wortlaut nach fakultativ („können“), werden aufgrund der Verpflichtung öffentlicher Stellen zum Schutz zumindest der personenbezogenen Daten nach Art. 6 Abs. 4, Art. 5 Abs. 1 DSGVO in der Praxis aber zumeist zwar situationsangemessen, jedoch obligatorisch umgesetzt werden müssen. Die Auswahl des konkreten Schutzinstruments erfolgt dabei auf der Grundlage einer Risikoanalyse, gegebenenfalls in Form einer Datenschutz-Folgenabschätzung im Sinne des Art. 35 DSGVO. 35

Die Anforderungen in Art. 5 Abs. 3 Satz 2 DGA setzen dabei primär auf **technische und organisatorische Maßnahmen** zum Datenschutz, welche jeweils von der öffentlichen Stelle selbst[25] – gegebenenfalls unter Einsatz eines Dienstleisters – vor Gewährung des Zugangs zur Weiterverwendung veranlasst werden müssen: 36

– Nach **Buchstabe a Ziff. i** kann der Zugang zu personenbezogenen Daten von einer vorherigen **Anonymisierung** abhängig gemacht werden. Was unter einer solchen „Anonymisierung“ zu verstehen und wie diese von „anderen Methoden der Offenlegungskontrolle“ nach Buchstabe a Ziff. ii abzugrenzen ist, ist mangels Begriffsdefinition nicht klar. **EG 26 Satz 5 DSGVO** verweist nur darauf, dass „anonyme Informationen“ „sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten […] in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann“ und daher die **Grundsätze des Datenschutzes** für 37

[25] Nach Auffassung von Schemmel, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 11/2023, Art. 5 DGA Rn. 47 kann dies dagegen durch den nationalen Gesetzgeber im Zusammenhang mit der nationalen Zuständigkeitsnorm geregelt werden.

solche anonymen Informationen – auch im Zusammenhang mit der Weiterverwendung – **nicht (mehr) gelten**.

38 – Im Fall von **Geschäftsgeheimnissen oder durch Rechte des geistigen Eigentums geschützten Inhalten** kann die öffentliche Stelle **deren Veränderung, Aggregation oder Aufbereitung** nach einer anderen Methode der Offenlegungskontrolle verlangen, **Buchstabe a Ziff. ii**. Was der Daten-Governance-Rechtsakt von diesen „anderen Methoden der Offenlegungskontrolle" konkret umfasst sehen will, lässt er offen. Aus **Art. 7 Abs. 4 Buchst. c DGA** lässt sich allerdings ersehen, dass dem Verordnungsgeber insoweit unter anderem Pseudonymisierung, Generalisierung, Unterdrückung und Randomisierung vorschweben. Die technik- und methodenoffene Klausel des Art. 5 Abs. 3 Satz 2 Buchst. a Ziff. ii DGA erfasst aber auch andere denkbare (zukünftige) Methoden zur Wahrung der Privatsphäre. Für die für den Datenschutz typische **Pseudonymisierung** von Daten sieht der Daten-Governance-Rechtsakt ebenfalls keine Definition vor; insoweit kann aber auf die Begriffsbestimmung in Art. 4 Nr. 5 DSGVO zurückgegriffen werden. Dabei ist zu beachten, dass pseudonymisierte personenbezogene beziehungsweise generell auf der Grundlage von Buchstabe a Ziff. ii veränderte personenbezogene Daten **weiterhin dem Rechtsregime der Datenschutz-Grundverordnung** unterliegen, vergleiche EG 26 Satz 2 DSGVO.[26]

39 – Ferner können die öffentlichen Stellen bestimmen, dass der Zugang zu den Daten und deren Weiterverwendung durch Fernzugriff oder nötigenfalls vor Ort in einer von der öffentlichen Stelle bereitgestellten oder kontrollierten „**sicheren Verarbeitungsumgebung**" erfolgen muss, **Art. 5 Abs. 3 Satz 1 Buchst. b und c, Abs. 4 Satz 1 in Verbindung mit Art. 2 Nr. 20 und Art. 7 Abs. 4 Buchst. d DGA**. Die öffentlichen Stellen werden nach Art. 7 Abs. 4 DGA insoweit durch die zuständigen Stellen unterstützt.

40 **Hinweis:** Die Geltung des Bayerischen Verwaltungsverfahrensgesetzes für Informationszugangsanträge bei Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen und damit Behörden im Sinne des Art. 1 Abs. 2 BayVwVfG sind, gewährleistet eine gleichförmige transparente Umsetzung des Zugangs zur Weiterverwendung von geschützten Daten im Besitz der öffentlichen Hand.

Sonstige öffentliche Stellen, bei denen sich das Verfahren ausschließlich nach der jeweiligen Rechtsgrundlage für den Informationszugangsanspruch richtet, sollten zur Erreichung dieser Gleichförmigkeit und Transparenz jeweils ein bestimmtes allgemeingültiges Verfahren für die Bearbeitung der Informationszugangsanträge etablieren und die hierfür erforderlichen Schutz- und Sicherungsmaßnahmen treffen.

Zugangs- und Weiterverwendungsbedingungen im oben genannten Sinn können als Nebenbestimmungen zum zugangsgewährenden Verwaltungsakt nach Art. 36 BayVwVfG oder als Ausführungsbestimmungen zur Gestattung festgelegt werden.

41 In Bezug auf die im Zusammenhang mit einer Weiterverwendung personenbezogener Daten erforderliche Einhaltung der datenschutzrechtlichen Vorschriften gilt, dass sowohl die Anonymisierung als auch andere Methoden der Offenlegungskontrolle, wie etwa eine Pseudonymisierung, sowie die Weiterverwendung in einer sicheren Verarbeitungsumgebung als **jeweils**

[26] EuGH, Urteil vom 19. Oktober 2016, C-582/14 (Breyer). Differenzierend EuG, Urteil vom 26. April 2023, T-557/20, für den Fall, dass der Datenempfänger nicht über die Mittel zur Rückidentifizierung verfügt.

eigenständige Datenverarbeitungsvorgänge nach **Art. 6 Abs. 1 UAbs. 1, Abs. 3 DSGVO** einer **Rechtsgrundlage bedürfen**. Insbesondere für den Fall, dass die Weiterverwendung auf eine Einwilligung im Sinne der Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DSGVO gestützt werden soll, stellen sich Fragen der praktischen Umsetzbarkeit, unter anderem in Bezug auf die Information über die Zwecke einer späteren Weiterverwendung, Zweckänderungen sowie die Rechte auf Widerruf der Einwilligung (Art. 7 Abs. 3 Satz 1 DSGVO) und Löschung personenbezogener Daten (Art. 17 DSGVO). Möchten sich die öffentlichen Stellen darauf berufen, dass die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO oder zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe nach Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO erfolgt, muss deren Rechtsgrundlage gemäß Art. 6 Abs. 3 Satz 1 DSGVO durch Unionsrecht oder durch das Recht der Mitgliedstaaten gesondert festgelegt sein. Es bleibt abzuwarten, ob der deutsche Gesetzgeber hierzu im DGA-Umsetzungsgesetz eine spezifische Regelung trifft; der Daten-Governance-Rechtsakt selbst schafft keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, Art. 1 Abs. 3 Satz 4 DGA.

Praxistipp: Soll die Offenlegungskontrolle oder die Weiterverwendung in einer sicheren Verarbeitungsumgebung auf eine **Einwilligung** gestützt werden, müssen bereits bei Einholung der Einwilligung im Datenerhebungsformular sowohl die Offenlegungskontrolle beziehungsweise die sichere Verarbeitungsumgebung als auch die spätere Weiterverwendung in die Zweckbestimmung aufgenommen werden. Zudem muss klargestellt werden, gegenüber wem die Rechte auf Widerruf der Einwilligung und Löschung personenbezogener Daten geltend zu machen sind. **42**

Beruft sich die öffentliche Stelle auf eine **andere Rechtsgrundlage** wie beispielsweise Art. 6 Abs. 1 UAbs. 1 Buchst. c oder e, Abs. 3 DSGVO, sind die entsprechenden Informationen betreffend die Weiterverwendung in die Information nach Art. 13 und 14 DSGVO aufzunehmen, zumindest in Form eines Portalverweises.

Nach **Art. 5 Abs. 4 Satz 2 DGA** behält sich die öffentliche Stelle das Recht vor, die Verfahren, Mittel und Ergebnisse der **vom Weiterverwender durchgeführten Datenverarbeitung** zur Wahrung der Integrität des Datenschutzes zu **überprüfen** sowie die **Verwendung der Ergebnisse zu verbieten**, wenn diese die Rechte und Interessen Dritter gefährden. Art. 5 Abs. 4 Satz 2 DGA nimmt insoweit eine – dem Datenschutzrecht weitgehend fremde – Unterscheidung zwischen der Datenverarbeitung und den Ergebnissen der Datenverarbeitung vor und **eröffnet eine Verbotsbefugnis** in einem Bereich, für den nach Art. 58 Abs. 2 DSGVO ansonsten die **Datenschutz-Aufsichtsbehörden zuständig** sind. Hier sind Zuständigkeitskonflikte vorprogrammiert, die Art. 1 Abs. 3 Satz 3 DGA jedoch zugunsten des Datenschutzrechts entscheidet. **43**

Hinweis: Art. 5 Abs. 4 Satz 2 DGA enthält zwar keine detaillierten Vorgaben zu deren Ausübung, statuiert aber eine klare Prüf- und gegebenenfalls Verbotspflicht für die öffentlichen Stellen. **44**

Jede öffentliche Stelle, die Zugang zur Weiterverwendung von in ihrem Besitz befindlichen geschützten Daten gewährt, sollte daher Nebenbestimmungen im Sinne des Art. 36 BayVwVfG zum zugangsgewährenden Verwaltungsakt beziehungsweise ausgestaltende Regelungen im Zusammenhang mit der Gewährung des Informationszugangsanspruchs zur

Ausübung dieser Prüf- und gegebenenfalls Verbotspflicht erlassen und insbesondere darlegen, wann und in welchen Fällen (allgemein und anlassbezogen) sie das Verfahren, die Mittel und die Ergebnisse der vom Weiterverwender durchgeführten Datenverarbeitung überprüft und unter welchen Voraussetzungen sie die Verwendung der Ergebnisse verbietet.

45 Die öffentliche Stelle soll – formal wiederum verortet in Nebenbestimmungen oder Ausgestaltungsregelungen – den Zugriff auf die Daten von der **Abgabe einer Geheimhaltungsverpflichtung** abhängig machen, **Art. 5 Abs. 5 Satz 1 DGA**, sofern nicht bereits im nationalen Recht für die Weiterverwendung entsprechende Geheimhaltungspflichten vorgesehen sind. Betreffend personenbezogene Daten wird eine Re-Identifizierung betroffener Personen im Rahmen der Weiterverwendung nach Art. 5 Abs. 5 Satz 2 DGA ausdrücklich untersagt, was der „Weiterverwender" durch technisch-organisatorische Maßnahmen (vergleiche EG 7 Satz 1 DGA) abzusichern hat. Im Fall eines Datenschutzverstoßes bestehen Mitteilungspflichten, gegebenenfalls auch nach Art. 33 und 34 DSGVO. Falls Interessen juristischer Personen betroffen sind, besteht eine entsprechende Informationspflicht auch bei einer unbefugten Weiterverwendung nicht personenbezogener Daten, Art. 5 Abs. 5 Satz 3 DGA.

46 **Praxistipp:** Öffentliche Stellen sollten eine einheitliche Geheimhaltungsverpflichtung verwenden und im Übrigen die Weiterverwender mittels standardisierter Informationen im Rahmen des Art. 5 Abs. 1 Satz 1 DGA auf die diesen obliegenden Pflichten hinweisen, gegebenenfalls zusätzlich in einem gesonderten Portal auf ihrer Homepage.

47 Kann die Weiterverwendung nicht erlaubt werden und fehlt eine andere Rechtsgrundlage für die Übermittlung von personenbezogenen Daten,[27] soll sich die öffentliche Stelle gemäß **Art. 5 Abs. 6 Satz 1 DGA** „nach besten Kräften" bemühen, mögliche Weiterverwender bei der **Einholung entsprechender Einwilligungen der betroffenen Personen oder Erlaubnisse der Dateninhaber zu unterstützen**. „Erlaubnis" meint dabei, „dass Datennutzern das Recht auf Verarbeitung nicht personenbezogener Daten eingeräumt wird", Art. 2 Nr. 6 DGA.[28] Dies ist mangels „Dateneigentums" an nicht personenbezogenen Daten als Einräumung der faktischen Verfügungsgewalt über die betreffenden Daten, gegebenenfalls mit entsprechender Freigabe nach beispielsweise Geschäftsgeheimnis-, Urheber- oder Patentrecht, zu verstehen. Die im Kommissionsentwurf noch vorgesehene harte Unterstützungspflicht ist mit dieser Regelung bewusst abgeschwächt worden. Die Unterstützung kann mit Blick auf EG 15 UAbs. 2 Satz 8 DGA etwa darin bestehen, dass die öffentliche Stelle – soweit praktikabel – technische Mechanismen schafft, mit denen Einwilligungs- oder Erlaubnisanfragen der Weiterverwender weitergeleitet werden können. Eine direkte Kontaktaufnahme des potentiellen Weiterverwenders mit betroffenen Personen oder Dateninhabern soll aber ausgeschlossen sein, EG 15 UAbs. 2 Satz 9 DGA. Dabei ist zu beachten, dass **auch die Weiterleitung einer Einwilligungsanfrage ein datenschutzrechtlich erheblicher Vorgang** ist, für den es gemäß Art. 6 Abs. 1 UAbs. 1, Abs. 3 DSGVO einer Rechtsgrundlage – außerhalb des Daten-Governance-Rechtsaktes, Art. 1 Abs. 3 Satz 4 DGA – bedarf. Insoweit bleibt ebenfalls abzuwarten, ob der deutsche Gesetzgeber im DGA-Umsetzungsgesetz in Ausfüllung der Regelungsspielräume des Art. 6 Abs. 1 UAbs. 1, Abs. 3 DSGVO eine spezifische Regelung für die

[27] Der Wortlaut von Art. 5 Abs. 6 Satz 1 DGA ist insoweit unglücklich formuliert, da der – unzutreffende – Eindruck entstehen könnte, dass Art. 5 Abs. 3 DGA eine Rechtsgrundlage für die Verarbeitung gewähren soll.

[28] Zu Erteilung und Reichweite der Erlaubnis vgl. Schild/Richter/Schmidt-Wudy, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 11/2023, Art. 2 DGA Rn. 20 mit weiteren Nachweisen.

Weiterleitung von Einwilligungsanfragen trifft oder ob die öffentlichen Stellen bereits existierende – andere – Rechtsgrundlagen durch entsprechende Auslegung zur Anwendung bringen müssen.

Art. 5 Abs. 7 Satz 1 DGA stellt klar, dass die Weiterverwendung von Daten nur unter Wahrung der Rechte des geistigen Eigentums zulässig ist. Öffentliche Stellen sollen, sofern sie Rechtsinhaber des sui-generis-Rechts der Hersteller von Datenbanken nach **Art. 7 Abs. 1 Richtlinie 96/9/EG**[29] sind, dieses Recht nicht in Anspruch nehmen, Art. 5 Abs. 7 Satz 2 DGA. 48

Hinweis: Das **sui-generis-Recht für Datenbanken** (auch **Datenbankherstellerrecht**) ist ein Recht zum Schutz von Investitionen in Datenbankwerke. Es beruht auf der Richtlinie 96/9/EG und ist in Deutschland in §§ 87a bis e Gesetz über Urheberrechte und verwandte Schutzrechte geregelt. Es soll verhindern, dass Investitionen in Datenbanken ohne Rechtsverstoß abgeschöpft werden können. Aus diesem Grund sind Datenbanken, das heißt Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, deren Beschaffung, Überprüfung oder Darstellung eine wesentliche Investition erfordert hat, gegen Entnahme und Weiterverwendung wesentlicher Teile geschützt. 49

So kann beispielsweise der Ersteller einer Datenbank für Kartenmaterial dessen Nutzung vom Besitz einer gültigen Lizenz abhängig machen.

Art. 5 Abs. 8 DGA regelt die Konstellation, dass angeforderte Daten nach den Bestimmungen des Unionsrechts oder des nationalen Rechts über die geschäftliche oder statistische Geheimhaltung als **vertraulich** angesehen werden. In diesem Fall müssen die öffentlichen Stellen sicherstellen, dass die vertraulichen Daten infolge der Gestattung der Weiterverwendung nicht offengelegt werden, es sei denn, die Weiterverwendung ist gemäß Art. 5 Abs. 6 DGA zulässig. Fraglich ist allerdings, mit welchen technischen oder rechtlichen Maßnahmen diese Sicherstellung der Vertraulichkeit erfolgen soll. Öffentliche Stellen dürften über Vertraulichkeitsvereinbarungen hinaus vielfach keine Möglichkeit haben, Einfluss auf den Weiterverwender zu nehmen. Dies ist von besonderer Bedeutung, da nach dem offenen Gesetzwortlaut sogar eine Haftung der öffentlichen Stelle bei Verletzung der Sicherstellungspflicht in Betracht kommt. 50

Praxistipp: Öffentliche Stellen sollten die von ihnen vorgenommenen Sicherungsmaßnahmen im Fall vertraulicher Daten besonders umfangreich und sorgfältig dokumentieren, um eine Haftung bei – vermeintlicher – Verletzung der Sicherstellungspflichten zu vermeiden. 51

Öffentliche Stellen, die eine Weiterverwendung von in ihrem Besitz befindlichen geschützten Daten erlauben, können aufgrund von national festgelegten und veröffentlichten Kriterien und Methoden **Gebühren für die Erlaubnis der Weiterverwendung** dieser Daten erheben, vorausgesetzt, die Gebühren sind transparent, nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt und beschränken nicht den Wettbewerb, **Art. 6 Abs. 1, 2, 5 und 6 DGA**.[30] Dabei müssen nach Art. 6 Abs. 3 DGA auch online-Bezahlungen ermöglicht werden. Gemäß Art. 6 Abs. 4 Sätze 1 und 2 DGA kann eine ermäßigte Gebühr oder Gebührenfreiheit 52

[29] Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, ABl. EG L 77 vom 27. März 1996, S. 20.

[30] Siehe Art. 1 Abs. 1 Kostengesetz.

vorgesehen werden, sofern die Weiterverwendung zu nichtkommerziellen Zwecken wie der wissenschaftlichen Forschung oder durch KMU und Start-up-Unternehmen erfolgt.

53 Keine Regelung trifft der Daten-Governance-Rechtsakt zu der **datenschutzrechtlich relevanten Frage, in welchem Verhältnis die öffentliche Stelle**, die eine Weiterverwendung personenbezogener Daten ermöglicht, **und der Weiterverwender stehen**. Da die betreffenden Daten gerade nicht allgemein zugänglich sind, dürfte bei der öffentlichen Stelle eine Restverantwortlichkeit verbleiben – zumindest für den Fall, dass die Daten nicht vorab anonymisiert wurden. Für eine fortbestehende datenschutzrechtliche Verantwortlichkeit der öffentlichen Stelle sprechen auch die Pflicht zur Ergebniskontrolle nach Art. 5 Abs. 4 Satz 2 DGA sowie die Möglichkeit der Einforderung einer Geheimhaltungsverpflichtung nach Art. 5 Abs. 5 Satz 1 DGA. Im Ergebnis haben sowohl die öffentliche Stelle als auch der Weiterverwender in solchen Fällen Einfluss auf die Zwecke der und die Mittel zur Verarbeitung und sind somit als **gemeinsam Verantwortliche im Sinne von Art. 26 DSGVO** anzusehen. Eine Zweckidentität ist gerade nicht erforderlich; vielmehr genügt die Verfolgung des gemeinsamen übergeordneten Interesses „Weiterverwendung der Daten". In der Konsequenz müssen die öffentliche Stelle und der Weiterverwender gemäß Art. 26 Abs. 1 Satz 2, Abs. 2 Satz 1 DSGVO in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtungen der Datenschutz-Grundverordnung erfüllt. Ob diese Anforderungen die Bereitschaft der Mitgliedstaaten steigern, Zugangsansprüche zu im Besitz öffentlicher Stellen befindlichen Daten zu etablieren, mag bezweifelt werden.

54 **Hinweis**: Gewährt eine öffentliche Stelle Zugang zu geschützten personenbezogenen Daten in ihrem Besitz und werden diese Daten vor Zugangsgewährung nicht anonymisiert, werden die öffentliche Stelle und der Weiterverwender mit der Zugangswahrnehmung zu gemeinsam Verantwortlichen im Sinne von Art. 26 DSGVO – mit allen damit verbundenen Folgen. Die öffentlichen Stellen sollten sich dieses Risiko bewusst machen und die geschützten personenbezogenen Daten entweder nur in anonymisierter Form weitergeben oder mit den Weiterverwendern Vereinbarungen zur gemeinsamen Verantwortlichkeit abschließen.

3. Anträge auf Weiterverwendung

55 Wie unter Rn. 22 ausgeführt, werden die Zugangsansprüche gegenüber bayerischen öffentlichen Stellen nach den allgemeinen Regeln des Verwaltungsverfahrens auf der Grundlage des Bayerischen Verwaltungsverfahrensgesetzes beziehungsweise nach der jeweiligen Rechtsgrundlage für den Informationszugangsanspruch realisiert. **Art. 9 DGA** enthält insoweit für die Antragsbearbeitung spezifische **Fristen**: Vorbehaltlich kürzerer nationaler Fristen[31] müssen die zuständigen öffentlichen Stellen nach **Absatz 1 UAbs. 1** regelmäßig **innerhalb von zwei Monaten nach Eingang** eine Entscheidung über den Antrag auf Weiterverwendung geschützter Daten treffen. Diese Frist kann gemäß **Art. 9 Abs. 1 UAbs. 2 DGA** bei außergewöhnlich umfangreichen und komplexen Anträgen ausnahmsweise um 30 Tage verlängert werden. Die öffentliche Stelle trifft insofern eine Informations- und Begründungspflicht gegenüber dem Antragsteller.

[31] Solche kürzeren Fristen finden sich beispielsweise in Art. 3 Abs. 3 Satz 2 BayUIG.

Praxistipp: Um die Zwei-Monats-Frist für die Antragsbearbeitung zu wahren, sollten öffentliche Stellen standardisierte Verfahren für die Antragsbearbeitung etablieren und ihren Datenbestand so aufbereiten, dass mögliche Zugangsansprüche frist- und formgerecht gewährt werden können. 56

Schon wegen **Art. 39 BayVwVfG**, aber auch mit Blick auf den in **Art. 9 Abs. 2 DGA** (siehe folgende Randnummer) geregelten Rechtsbehelfsanspruch, umfasst die Pflicht zur Entscheidung über die Weiterverwendungsanträge (**implizit**) **eine Begründungspflicht** der öffentlichen Stellen für insbesondere die Nicht-Herausgabe von geschützten Daten, auch dahingehend, dass eine Weiterverwendung nicht unter den in Art. 5 Abs. 3 bis 5 DGA genannten Bedingungen beziehungsweise Verpflichtungen oder dass keine Unterstützung bei der Einholung von Einwilligungen oder Erlaubnissen gemäß Art. 5 Abs. 6 DGA möglich ist. Den öffentlichen Stellen wird dadurch in Abkehr von der bisherigen datenschutzrechtlichen Prämisse, dass ein potentieller Datennutzer ein Zugangsbegehren zu bestimmten (personenbezogenen) Daten begründen muss, eine neue öffentliche Aufgabe auferlegt. 57

Praxistipp: Zur Gewährleistung einer zeitgerechten und gleichförmigen Entscheidungspraxis sollten öffentliche Stellen in Bezug auf die von ihnen zu treffenden Entscheidungen Muster entwickeln beziehungsweise Formalvorgaben etablieren und insbesondere Begründungsbausteine anwenden. 58

Nach **Art. 9 Abs. 2 Satz 1 DGA** hat jede natürliche oder juristische Person, die von einer Entscheidung über einen Weiterverwendungsantrag direkt betroffen ist, in dem Mitgliedstaat, in dem die entscheidende Stelle ihren Sitz hat, einen **wirksamen Rechtsbehelfsanspruch**. Der Rechtsbehelfsanspruch bestimmt sich nach **nationalem Recht** – bei Fehlen bereichsspezifischer Regelungen nach allgemeinem Verwaltungsrecht – und umfasst die Möglichkeit der Überprüfung durch eine unparteiische Stelle mit entsprechender Sachkenntnis, beispielsweise ein Gericht oder auch die Aufsichtsbehörde nach der Datenschutz-Grundverordnung, Art. 9 Abs. 2 Satz 2 DGA. Insoweit bedarf es noch einer nationalrechtlichen Umsetzungsregelung. 59

4. Besondere Vorgaben zum Transfer von nicht personenbezogenen Daten in und zum Zugang zu solchen Daten durch Drittstaaten

Als **spezieller Unterfall** der allgemeinen Regelung betreffend internationalen Zugang zu und internationale Übertragung von nicht personenbezogenen Daten in **Art. 31 DGA** (hierzu näher Rn. 121 ff.) enthalten **Art. 5 Abs. 9 bis 14 DGA** zusätzliche Vorgaben für den Fall, dass im Rahmen der Weiterverwendung **nicht personenbezogene vertrauliche Daten oder durch Rechte des geistigen Eigentums geschützte Daten in ein Drittland übertragen werden** – nicht zuletzt zum Schutz vor Diebstahl geistigen Eigentums oder Industriespionage. Diese neuartigen Bestimmungen für die Übertragung nicht personenbezogener Daten in ein Drittland sind als **Gegenstück** zu den für den Drittstaatentransfer **personenbezogener Daten** vorrangigen Grundsätzen der **Art. 44 ff. DSGVO** konzipiert. Werden im Zusammenhang 60

mit der Weiterverwendung sowohl personenbezogene als auch nicht personenbezogene Daten in ein Drittland übermittelt, sind daher differenziert nach Datenart parallel zwei verschiedene Regelungsregime zu beachten,

61 **Generell** dürfen nach **Art. 5 Abs. 14 DGA** nicht personenbezogene vertrauliche oder durch Rechte des geistigen Eigentums geschützte Daten nur in solche **Drittländer** übertragen werden, bei denen die **Voraussetzungen der Absätze 10, 12 und 13** vorliegen und somit angemessene Schutzvorkehrungen für die Nutzung der Daten getroffen wurden.

62 **Vor einer Übertragung** nicht personenbezogener vertraulicher oder durch Rechte des geistigen Eigentums geschützter Daten in Drittstaaten muss der Weiterverwender die öffentliche Stelle nach **Art. 5 Abs. 9 Satz 1 DGA bei Beantragung der Weiterverwendung** über diese Transferabsicht sowie den Zweck des Datentransfers **unterrichten**. Liegt einer der Fälle des Art. 5 Abs. 6 DGA vor, muss der Weiterverwender zusätzlich, gegebenenfalls mit Unterstützung der öffentlichen Stelle, die juristische Person und über den Wortlaut hinaus auch die natürliche Person[32], deren Rechte und Interessen beeinträchtigt werden können, über die Transferabsicht, den Zweck und die angemessenen Schutzvorkehrungen informieren, Art. 5 Abs. 9 Satz 2 DGA. In diesen Fällen gestattet die öffentliche Stelle eine Weiterverwendung der Daten gemäß Art. 5 Abs. 9 Satz 3 DGA auf der Grundlage von entsprechenden Nebenbestimmungen im Sinne des Art. 36 BayVwVfG beziehungsweise Ausgestaltungsregelungen nur dann, wenn die juristische Person den Datentransfer in ein Drittland erlaubt.

63 Beabsichtigt ein Weiterverwender, nicht personenbezogene vertrauliche oder durch Rechte des geistigen Eigentums geschützte Daten in einen nicht gemäß Art. 5 Abs. 12 DGA benannten Drittstaat zu übertragen, muss er sich „**vertraglich**“ **dazu verpflichten**, die **Verpflichtungen nach den Art. 5 Abs. 7 und 8 DGA** auch nach der Übertragung der Daten in das Drittland weiter zu erfüllen sowie die Zuständigkeit der Gerichte des Mitgliedstaates, in dem sich die übermittelnde öffentliche Stelle befindet, für alle Streitigkeiten in diesem Zusammenhang anzuerkennen, **Art. 5 Abs. 10 DGA**.

64 Für die **verfahrensrechtliche Umsetzung** dieser vertraglichen Verpflichtung ist zu **differenzieren**: Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen und damit **Behörden** im Sinne des Art. 1 Abs. 2 BayVwVfG sind, verbescheiden Informationszugangsansprüche durch Verwaltungsakt (Rn. 22). Im Fall der geplanten Drittstaatenübermittlung ist die Wirksamkeit des zugangsgewährenden Verwaltungsaktes von der **aufschiebenden Bedingung (Art. 36 Abs. 2 Nr. 2 BayVwVfG) des Abschlusses eines entsprechenden öffentlich-rechtlichen Vertrages im Sinne des Art. 54 BayVwVfG** zwischen öffentlicher Stelle und Weiterverwender mit dem Regelungsinhalt des Art. 5 Abs. 10 DGA abhängig zu machen. Für **sonstige öffentliche Stellen** findet das Bayerische Verwaltungsverfahrensgesetz keine Anwendung; das Verfahren richtet sich ausschließlich nach der jeweiligen Rechtsgrundlage für den Informationszugangsanspruch (Rn. 23). Das Handlungsinstrument des öffentlich-rechtlichen Vertrages nach Art. 54 BayVwVfG steht daher schon gar nicht zu Verfügung; vielmehr erfolgt der Vertragsschluss nach Privatrecht, §§ 145 ff. Bürgerliches Gesetzbuch (BGB).

[32] Diese kann mit Blick auf Art. 2 Nr. 8 DGA ebenfalls „Dateninhaber“ sein, vgl. Schemmel, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 11/2023, Art. 5 DGA Rn. 73.

Hinweis: Ausweislich Art. 7 Abs. 4 Buchst. e DGA dürfen sich die öffentlichen Stellen nicht allein auf diese vertragliche Verpflichtung des Weiterverwenders verlassen, sondern müssen – gegebenenfalls mit Unterstützung der zuständigen Stellen im Sinne von Art. 7 Abs. 1 DGA – eine Beurteilung vornehmen, ob die von dem Weiterverwender eingegangenen vertraglichen Zusagen angemessen sind. 65

Zur Gewährleistung von Gleichförmigkeit und Transparenz sollten die öffentlichen Stellen entsprechende Vertragsmuster ausarbeiten.

Um die Erfüllung der Verpflichtungen des Art. 5 Abs. 10 DGA zu erleichtern, kann die Kommission auf der Grundlage von **Art. 5 Abs. 11 UAbs. 2 in Verbindung mit Art. 33 Abs. 3 DGA Durchführungsrechtsakte mit Mustervertragsklauseln** erlassen. 66

Analog zu Art. 45 DSGVO kann die Kommission überdies gemäß **Art. 5 Abs. 12 UAbs. 1 DGA** in **Angemessenheitsbeschlüssen** die Adäquanz des Schutzes nicht personenbezogener Daten in Drittstaaten feststellen, vorausgesetzt, ein Drittstaat bietet ein Schutzniveau für nicht personenbezogene Daten, das im Vergleich zu dem in der Europäischen Union herrschenden Schutzniveau als wesentlich gleichwertiges anzusehen ist (vergleiche EG 21 DGA). 67

Für **bestimmte hochsensible Kategorien nicht personenbezogener Daten** kann zudem auf der Grundlage von **Art. 5 Abs. 13 DGA** die Übertragung und Weiterverwendung in Drittstaaten an zusätzliche Bedingungen geknüpft oder in Ausnahmefällen sogar vollständig untersagt werden, etwa wenn dadurch die Sicherheit oder öffentliche Gesundheit gefährdet erscheint. 68

Weitere Einschränkungen für den internationalen Zugang zu und die internationale Übertragung von nicht personenbezogenen Daten sind in **Art. 31 DGA** vorgesehen, siehe Rn. 121 ff. 69

5. Zuständige Stellen und Zentrale Informationsstellen

Die öffentlichen Stellen, die Zugang zur Weiterverwendung von geschützten Daten gewähren oder verweigern, werden nach **Art. 7 Abs. 1 Satz 1 DGA durch eine oder mehrere von jedem Mitgliedstaat benannte sogenannte „zuständige Stellen" unterstützt**, die gegenüber den öffentlichen Stellen nicht ausschließlich weisungsgebunden sind.[33] Die Mitgliedstaaten können dafür neue Stellen einrichten oder sich auf bestehende öffentliche Stellen oder interne Dienste öffentlicher Stellen stützen, welche sie der Kommission bis zum 24. September 2023 mitgeteilt haben sollten, Art. 7 Abs. 1 Satz 2 und Abs. 5 Satz 1 DGA.[34] Für Deutschland ist diese Benennung bislang nicht erfolgt. 70

Die Unterstützung umfasst nach **Art. 7 Abs. 4 DGA technische Unterstützungsleistungen** in Bezug auf die Bereitstellung einer sicheren Verarbeitungsumgebung (Buchstabe a), die Strukturierung und Speicherung von Daten (Buchstabe b), die Pseudonymisierung sowie die Techniken zur Anonymisierung, Generalisierung, Unterdrückung und Randomisierung personenbezogener Daten oder andere dem Stand der Technik entsprechende Methoden 71

[33] Hilgers, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 11/2023, Art. 7 DGA Rn. 12.

[34] Beachte in diesem Zusammenhang EG 4 Satz 4 DGA: „Es sollte möglich sein, Datenschutzbehörden als gemäß dieser Verordnung zuständige Behörden zu betrachten."

(Buchstabe c) **sowie die Beratung und Mitwirkung bei der Einholung von Einwilligungen oder Erlaubnissen**. Die zuständigen Stellen können gemäß **Art. 7 Abs. 2 Satz 1 DGA** im Zusammenhang mit einer unionsrechtlichen oder nationalen Zugangsgewährung auch **befugt werden**, unter den Voraussetzungen der Art. 4, 5, 6 und 9 DGA **selbst den Zugang** zur Weiterverwendung von geschützten Daten zu gewähren (zum Teil als „One-Stop-Shop-Prinzip" bezeichnet).

72 Nach **Art. 8 Abs. 1 Satz 1 DGA** soll die Weiternutzung von Daten in jedem Mitgliedstaat zudem durch eine „**zentrale Informationsstelle**" unterstützt werden, die Interessenten den Zugang zu **allen einschlägigen Informationen** erleichtert. Die Informationsstelle kann entweder neu eingerichtet oder in eine vorhandene Stelle eingebunden werden oder mit sektoralen, regionalen oder lokalen Informationsstellen verknüpft sein, Art. 8 Abs. 1 Satz 2 DGA. Auch diesbezüglich gibt es in Deutschland bisher keine Regelung.

73 Diese zentrale Informationsstelle soll befugt sein, **Anträge auf Weiterverwendung** von geschützten Daten im Besitz der öffentlichen Hand **entgegenzunehmen und** an die zuständigen öffentlichen Stellen **zu übermitteln**, **Art. 8 Abs. 2 Satz 1 DGA**. Nach **Art. 8 Abs. 2 Satz 2, Abs. 4 DGA** stellt sie zudem auf elektronischem Wege eine **durchsuchbare Bestandsliste mit einer Übersicht aller verfügbaren Datenressourcen** bereit, die auch über ein europaweites zentrales Zugangsportal recherchierbar ist. Hierdurch soll es Interessenten erleichtert werden, potenziell relevante verfügbare Datensätze zu finden und nutzbar zu machen.

74 **Hinweis:** Um eine solche durchsuchbare Bestandsliste mit einer Übersicht aller verfügbaren Datenressourcen erstellen zu können, bedarf die zentrale Informationsstelle der Zuarbeit der einzelnen öffentlichen Stellen. Öffentliche Stellen, die geschützte Daten in ihrem Besitz für eine Weiterverwendung zugänglich machen, sollten daher nach Benennung der zentralen Informationsstelle im deutschen DGA-Umsetzungsgesetz eine den dort gegebenenfalls festgelegten Kriterien entsprechende Übersicht der verfügbaren Datenressourcen erstellen und aktuell halten.

6. Zusammenfassung

75 Der **tatsächliche Regelungsgehalt** von Kapitel II des Daten-Governance-Rechtsaktes ist **überschaubar**. Die Schaffung der zentralen Informationsstelle als zentralem Ansprechpartner senkt möglicherweise die „Hemmschwelle" zur tatsächlichen Nutzung der Datenzugangsangebote. Das grundsätzliche Dilemma bei solchen Datenzugangsmöglichkeiten adressiert der Daten-Governance-Rechtsakt dagegen nicht; vielmehr überlässt er die Gewährung und Ausgestaltung von Zugangsansprüchen zu Daten der öffentlichen Hand den Mitgliedstaaten und nimmt in Kauf, dass die **nationalen Regelungen sehr unterschiedlich** ausfallen. Zum Ziel der Schaffung eines unionalen Datenraums trägt dieser Ansatz damit faktisch wenig bei und bietet zudem datenschutz- und grundrechtliches Konfliktpotenzial.

76 **Auch innerhalb des Kapitels II** des Daten-Governance-Rechtsaktes verbleibt an vielen Stellen ein **erheblicher Gestaltungsspielraum** sowohl für die Mitgliedstaaten als auch für die einzelnen öffentlichen Stellen, beispielsweise in Bezug auf die konkreten Bedingungen für die

Weiterverwendung (vergleiche nur Art. 5 Abs. 3 und 4 DGA) oder die Erhebung von Gebühren für die Erlaubnis der Weiterverwendung (Art. 6 Abs. 1 DGA).

Es bleibt also den öffentlichen Stellen überlassen, den Spagat zwischen der Sicherstellung des Schutzes der Daten einerseits und der Ermöglichung der Weiterverwendung andererseits zu schaffen. Dies sollten die Mitgliedstaaten und/oder öffentlichen Stellen bei der Entscheidung über die Zulassung der Weiterverwendung von geschützten Daten im Besitz der öffentlichen Hand bedenken. 77

IV. Datenvermittlungsdienste

1. Konzept Datenvermittlungsdienste

78 Eine **Schlüsselrolle** in der Datenwirtschaft kommt aus Sicht des Verordnungsgebers Datenvermittlungsdiensten (auch: Datenintermediäre) zu, vergleiche EG 27 DGA. Diese können dazu beitragen, Daten zu bündeln und den Austausch personenbezogener und nicht personenbezogener Daten zu erleichtern. In seinem **dritten Kapitel** legt der Daten-Governance-Rechtsakt daher harmonisierte Rahmenbedingungen für diese Dienste fest, um die Datenwirtschaft durch Neutralität des Datenzugangs sowie Sicherstellung von Datenübertragbarkeit und Interoperabilität für alle Datennutzer, insbesondere auch für kleinere Unternehmen zu öffnen und Lock-in-Effekte[35] zu vermeiden: So setzt die Erbringung bestimmter, in Art. 10 DGA aufgelisteter Datenvermittlungsdienste eine Anmeldung nach Art. 11 DGA voraus und unterliegt den Anforderungen des Art. 12 DGA, deren Einhaltung nach Art. 14 DGA von der zuständigen Behörde überwacht wird (Rn. 93).

79 „Datenvermittlungsdienste" sind nach **Art. 2 Nr. 11 DGA** solche Dienste, mit denen „durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von Personen oder Dateninhabern einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung […] zu ermöglichen". Eine „**Geschäftsbeziehung**" in diesem Sinne bezeichnet unter Berücksichtigung der Beispiele in **EG 27 Satz 6 und EG 29 UAbs. 1 Satz 4 DGA** eine längerfristig angelegte, an wirtschaftlichen Zielen ausgerichtete Beziehung zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und potenziellen Datennutzern andererseits, die Leistung und Gegenleistung, nicht notwendigerweise finanzieller Art, austauschen. „**Dateninhaber**" umfassen gemäß **Art. 2 Nr. 8 DGA** juristische Personen, einschließlich öffentlicher Stellen und internationaler Organisationen, oder natürliche Personen, die in Bezug auf die betreffenden Daten keine betroffene Person sind und „welche nach geltendem […] Recht berechtigt [sind], Zugang zu bestimmten personenbezogenen Daten oder nicht personenbezogenen Daten zu gewähren oder diese Daten weiterzugeben".[36] Unter „**Datennutzer**" ist nach **Art. 2 Nr. 9 DGA** eine natürliche oder juristische Person zu verstehen, „die rechtmäßig Zugang zu bestimmten personenbezogenen oder nicht personenbezogenen Daten hat und […] berechtigt ist, diese Daten für kommerzielle oder nichtkommerzielle Zwecke zu nutzen".

80 Im weiteren Verlauf des Art. 2 Nr. 11 DGA erfolgt eine ausdrückliche **Negativabgrenzung**, wonach Dienste zur Datenaufbereitung und -lizenzierung (Buchstabe a), Content-Intermedi-

[35] Der Wirtschaftsbegriff bezeichnet ein Leistungsverhältnis, bei dem Kunden derart von Produkten oder Dienstleistungen eines Anbieters abhängig sind, dass der Wechsel zu einem Mitbewerber mit hohem Aufwand und hohen Kosten verbunden wäre und deshalb in der Regel unterbleibt. Entscheidend sind dabei meist technische, prozessuale oder vertragliche Abhängigkeiten zwischen einzelnen Produkten oder Leistungsteilen des Anbieters, die auf diese Weise ein mehr oder weniger in sich geschlossenes System bilden.

[36] Die Legaldefinition des „Dateninhabers" in Art. 2 Nr. 8 DGA entspricht dabei nicht der Definition des „Dateninhabers" in Art. 2 Nr. 6 der Entwurfsfassung des Datengesetzes.

äre (Buchstabe b), geschlossene Datensysteme (Buchstabe c) sowie Datenvermittlungsdienste, die von öffentlichen Stellen ohne die Absicht der Herstellung von Geschäftsbeziehungen angeboten werden (Buchstabe d), vom Anwendungsbereich des Kapitels III DGA ausgenommen werden. Ebenso soll es nach **EG 28 Satz 3 DGA** in Ausfüllung der Definition des „Datenvermittlungsdienstes" bereits an einer **„gemeinsamen Datennutzung" fehlen**, wenn Dienste die bloße Bereitstellung technischer Werkzeuge zur gemeinsamen Datennutzung bezwecken, wie beispielsweise die Bereitstellung von Cloud-Speicher, Analysediensten, Software zur gemeinsamen Datennutzung, von Internetbrowsern oder Browser-Plug-ins oder von E-Mail-Diensten. Schließlich fallen nach **Art. 15 DGA** die Tätigkeiten anerkannter datenaltruistischer Organisationen und anderer Einrichtungen ohne Erwerbszwecke ausdrücklich **nicht in den Anwendungsbereich** des Kapitels III DGA, es sei denn, diese sind bestrebt, Geschäftsbeziehungen zwischen einer unbestimmten Zahl von betroffenen Personen und Dateninhabern einerseits und Datennutzern andererseits herzustellen. Zu solchen „anderen Einrichtungen ohne Erwerbszwecke" könnten beispielsweise Forschungsdatenzentren und andere wissenschaftliche Forschungseinrichtungen zählen.

Zusätzliche Voraussetzung für die Annahme einer Vermittlertätigkeit als essentielles Merkmal von Datenvermittlungsdiensten ist mit Blick auf **EG 28 Satz 3 DGA** somit, dass der Anbieter die **Vermittlungstätigkeit als Hauptzweck verfolgen** muss. Die bloße Ermöglichung des Austauschs von Daten als Reflexwirkung einer Leistung (beispielsweise Bereitstellung eines Cloud-Dienstes) beziehungsweise der Datenaustausch als Mittel zum Zweck genügen nicht. Eine Stelle kann demzufolge ohne entsprechende Vermittlungsabsichten **nicht „zufällig"** zum Datenvermittlungsdienst werden. 81

Der Verordnungsgeber selbst nennt als Beispiele für Datenvermittlungsdienste in diesem Sinne in **EG 27 Satz 6 und EG 28 UAbs. 1 Satz 4 DGA** unter anderem **Datenmarktplätze, Ökosysteme zur gemeinsamen Datennutzung sowie Anbieter von Datenbeständen auf Lizenzbasis**. Mit Blick auf **Art. 10 Buchst. b und c DGA** umfassen Datenvermittlungsdienste zudem die **Ermöglichung der in der Datenschutz-Grundverordnung verankerten Rechte** betroffener Personen sowie **Datengenossenschaften** (vergleiche Art. 2 Nr. 15 DGA). Bieten Unternehmen oder sonstige Stellen eine **Vielzahl von datenbezogenen Diensten** an, so fallen gemäß **EG 28 Satz 2 DGA** nur diejenigen Tätigkeiten unter den Daten-Governance-Rechtsakt, die unmittelbar die Bereitstellung von Datenvermittlungsdiensten betreffen. 82

Beispiele: Die Europäische Kommission führt im Zusammenhang mit ihrer Erklärung des Daten-Governance-Rechtsaktes als konkrete Beispiele für Datenvermittler das Data Intelligence Hub der Deutschen Telekom, das französische Unternehmen Dawex sowie das landwirtschaftliche Datenaustausch-Hub API-AGRO an.[37]

Hinweis: Im Kontext der Datenvermittlungsdienste kommen auch **Innungen, Handwerks-, Berufs- sowie Industrie- und Handelskammern** als Anbieter in Betracht. Richtet eine Industrie- und Handelskammer beispielsweise eine Plattform oder eine Datenbank ein, auf der 83

[37] Europäische Kommission, Data Governance Act erklärt, Internet: https://digital-strategy.ec.europa.eu/de/policies/data-governance-act-explained.

IV. Datenvermittlungsdienste

Unternehmen Informationen wie unter anderem Produktionsdaten bereitstellen (und monetarisieren) können, um Prozesse oder ganze Wertschöpfungsketten zu optimieren, handelt sie insoweit als Datenvermittler im Sinne des Daten-Governance-Rechtsaktes.

84 Bei den Anbietern von Datenvermittlungsdiensten kann es sich nach dem Gesetz **auch um öffentliche Stellen** handeln, **EG 27 Satz 3 DGA**, vorausgesetzts sie verfolgen die Absicht der Herstellung von Geschäftsbeziehungen (vergleiche Art. 2 Nr. 11 Buchst. d DGA).

85 **Hinweise:** Öffentliche Stellen sind mithin dann als Datenvermittlungsdienste einzustufen, wenn sie als neutrale Dritte eine unbestimmte Anzahl von betroffenen Personen oder Dateninhabern mit potenziellen Datennutzern durch Herstellung einer Leistungsbeziehung verbinden.

Derartige Modelle zur Erleichterung des Datenaustauschs sind **aus dem (bayerischen) öffentlichen Bereich nicht bekannt**. Insbesondere sind **Open-Data-Portale** der öffentlichen Hand **nicht** als Datenvermittlungsdienste im Sinne des Daten-Governance-Rechtsaktes einzustufen, da die öffentlichen Stellen insoweit schon nicht als neutrale Datenintermediäre fungieren; vielmehr stellen die öffentlichen Stellen die offenen (Verwaltungs-)Daten selbst voraussetzungslos für alle interessierten Nutzer zur Verfügung.

Bayerische öffentliche Stellen können aber sowohl als Dateninhaber als auch als Datennutzer einen **Datenvermittlungsdienst in Anspruch** nehmen. Handelt es sich um einen Datenvermittlungsdienst im Sinne des Art. 10 DGA, sollten sie nur solche Dienste nutzen, die im unionsweiten Register aller Anbieter von Datenvermittlungsdiensten (vergleiche Art. 11 Abs. 10 Satz 2 DGA, Rn. 89) aufgeführt sind oder sogar das Label „in der EU anerkannter Datenvermittler" und das gemeinsame Logo verwenden (vergleiche Art. 11 Abs. 9 UAbs. 1 Satz 2 DGA, Rn. 90). Nur für diese Datenvermittlungsdienste gelten die besonderen Bedingungen des Art. 12 DGA zum Schutz von Dateninhaber und -nutzer.

86 Für personenbezogene Daten sind solche Vermittlungsdienste grundsätzlich **schon auf der Grundlage der Datenschutz-Grundverordnung** zulässig, sofern sie den dortigen Vorgaben genügen. Die Vermittlung nicht personenbezogener Daten war bislang nicht gesetzlich geregelt. Der Daten-Governance-Rechtsakt etabliert nun spezifische Anforderungen, insbesondere ein **Verbot mit Anmeldevorbehalt** in Form einer **Anmeldepflicht** für die in Art. 10 DGA genannten Datenvermittlungsdienste als – bürokratische und kostenrelevante – Voraussetzung für die Aufnahme ihrer Tätigkeit, **Art. 11 Abs. 1 und 4 DGA**. Damit lässt der Daten-Governance-Rechtsakt das Modell der Meldepflicht für automatisierte Verarbeitungen in Art. 18 ff. Richtlinie 95/46/EG[38] wieder aufleben, dessen Abschaffung durch die Datenschutz-Grundverordnung vom Normgeber im Jahr 2016 noch als Fortschritt bewertet worden war.[39]

[38] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG L 281 vom 23. November 1995, S. 31.

[39] EG 89 Sätze 2 und 3 DSGVO. Vergleiche auch Mitteilung der Kommission an das Europäische Parlament und den Rat, Besserer Schutz und neue Chancen – Leitfaden der Kommission zur unmittelbaren Geltung der Datenschutz-Grundverordnung, COM(2018) 43 final, Internet: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2018)43&lang=de, S. 4: „Die Meldepflicht wird vom Grundsatz der Rechenschaftspflicht abgelöst".

2. Anmeldung der Anbieter von Datenvermittlungsdiensten

Wer beabsichtigt, einen der in Art. 10 DGA aufgeführten Datenvermittlungsdienste anzubieten, muss sich gemäß **Art. 11 Abs. 1 und 2 DGA** bei der für seine Hauptniederlassung zuständigen Behörde im Sinne des Art. 13 DGA (Rn. 92) **anmelden**. Ist ein Anbieter von Datenvermittlungsdiensten nicht in der Union niedergelassen, benennt er einen **gesetzlichen Vertreter in einem der Mitgliedstaaten**, in denen er die Datenvermittlungsdienste anbietet, **Art. 11 Abs. 3 DGA**. 87

Hinweis: Nur die in **Art. 10 DGA genannten Datenvermittlungsdienste** unterliegen einem Anmeldeverfahren nach Art. 11 DGA und müssen die Bedingungen des Art. 12 DGA erfüllen. Dies sind: 88

- **Buchstabe a**: Vermittlungsdienste zwischen Dateninhabern und potenziellen Datennutzern, einschließlich Bereitstellung der technischen oder sonstigen Mittel als Voraussetzung solcher Dienste; zu diesen Diensten können auch der zwei- oder mehrseitige Austausch von Daten oder die Einrichtung von Plattformen oder Datenbanken, die den Austausch oder die gemeinsame Nutzung von Daten ermöglichen, sowie die Einrichtung anderer spezieller Infrastrukturen für die Vernetzung von Dateninhabern mit Datennutzern gehören;
- **Buchstabe b**: Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zugänglich machen wollen, oder natürlichen Personen, die nicht personenbezogene Daten zugänglich machen wollen, und potenziellen Datennutzern, einschließlich Bereitstellung der technischen und sonstigen Mittel als Voraussetzung dieser Dienste sowie insbesondere Ermöglichung der Ausübung der in der Datenschutz-Grundverordnung verankerten Rechte betroffener Personen;
- **Buchstabe c**: Dienste von Datengenossenschaften.[40]

Nicht erfasst sind dagegen die in **Art. 2 Nr. 11 und EG 28 Satz 3 DGA** ausgenommenen Dienste.

Das Anmeldeverfahren muss **nichtdiskriminierend** ausgestaltet sein und darf nicht zu Wettbewerbsverzerrungen führen, **Art. 11 Abs. 7 DGA**. Die Anmeldung muss die in **Art. 11 Abs. 6 DGA** aufgeführten **Angaben** enthalten, deren Änderung der national zuständigen Behörde im Sinne des Art. 13 DGA nach Art. 11 Abs. 12 und 13 DGA fristgerecht mitzuteilen ist. Die zuständige Behörde kann nach Maßgabe des nationalen Rechts **verhältnismäßige und objektive Gebühren** für die Anmeldung erheben, **Art. 11 Abs. 11 DGA**. Die Kommission führt ein **zentrales**, teilweise öffentliches, regelmäßig aktualisiertes **Register** aller Anbieter von Datenvermittlungsdiensten in der Union, Art. 11 Abs. 10 und 14 DGA. 89

Nach der Anmeldung können Anbieter von Datenvermittlungsdiensten nach **Art. 11 Abs. 4 und 5 DGA** ihre Tätigkeit – unter Einhaltung der Vorgaben aus insbesondere Art. 12 DGA – in allen Mitgliedstaaten aufnehmen. **Es bedarf weder einer Genehmigung noch erfolgt eine (Vorab-)Kontrolle** der Behörden, ob die Anforderungen des Daten-Governance-Rechtsaktes eingehalten werden. Eine solche **Überprüfung** wird **nach Art. 11 Abs. 9 UAbs. 1 DGA lediglich auf Antrag** vorgenommen. Bestätigt die zuständige Behörde die Er- 90

[40] Hierzu ausführlich Schild/Richter/Schmidt-Wudy, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 11/2023, Art. 2 DGA Rn. 67 ff.

füllung der Anforderungen der Art. 11 und 12 DGA, kann der betreffende Anbieter von Datenvermittlungsdiensten das **Label „in der EU anerkannter Datenvermittler“** führen und ein gemeinsames Logo (etabliert durch Durchführungsverordnung (EU) 2023/1622,[41] vergleiche Art. 11 Abs. 9 UAbs. 2 DGA) verwenden. Wie viele Anbieter von Datenvermittlungsdiensten sich tatsächlich dieser freiwilligen „Compliancеprüfung“ unterwerfen, weil sie sich hiervon Vorteile im Wettbewerb versprechen, wird die Praxis zeigen. Alternativ kann die zuständige Behörde auf Antrag des Anbieters von Datenvermittlungsdiensten nach Art. 11 Abs. 8 DGA auch nur das Vorliegen einer ordnungsgemäßen und vollständig abgeschlossenen Anmeldung bestätigen.

3. Bedingungen für die Erbringung von Datenvermittlungsdiensten

91 **Art. 12 DGA** legt die **materiellen Bedingungen** fest, unter denen die in Art. 10 DGA benannten Datenvermittlungsdienste erbracht werden dürfen. Diese umfassen neben spezifisch **datenschutzrechtlichen Aspekten** (Zweckbestimmung und Neutralitätsgebot – Buchstabe a,[42] Verwendung von Metadaten – Buchstabe c,[43] Verhinderung der rechtswidrigen Übertragung von nicht personenbezogenen Daten oder des rechtswidrigen Zugangs zu diesen Daten durch angemessene technische, rechtliche und organisatorische Maßnahmen – Buchstabe j, Meldepflicht bei unbefugten Verarbeitungen nicht personenbezogener Daten – Buchstabe k,[44] Maßnahmen zur Sicherstellung des erforderlichen Sicherheitsniveaus – Buchstabe l) auch **technisch-organisatorische Vorgaben** (Formatumwandlungen – Buchstabe d,[45] Verwendung zusätzlicher spezifischer Werkzeuge und Dienste – Buchstabe e,[46] Gewährleistung von Interoperabilität mit anderen Datenvermittlungsdiensten – Buchstabe i,

41 Durchführungsverordnung (EU) 2023/1622 der Kommission vom 9. August 2023 über die Ausgestaltung gemeinsamer Logos für die in der Union anerkannten Anbieter von Datenvermittlungsdiensten und datenaltruistischen Organisationen, ABl. EU L 200 vom 10. August 2023, S. 1.

42 Verbot der Datennutzung zu anderen Zwecken, als sie den Datennutzern zur Verfügung zu stellen, sowie Gebot des Handelns als neutrale Dritte mittels einer gesonderten juristischen Person als maßgebliche Anforderungen für die Schaffung von Vertrauen und Anreizen zur Datenweitergabe, EG 33 DGA.

43 Die aufgeführten Metadaten dürfen nur für die Entwicklung des jeweiligen Datenvermittlungsdienstes verwendet werden, etwa zur Aufdeckung von Betrug oder im Interesse der Cybersicherheit, und müssen den Dateninhabern auf Anfrage zur Verfügung gestellt werden.

44 Für personenbezogene Daten gilt bei Datenschutzvorfällen das Regime der Datenschutz-Grundverordnung, insbesondere Art. 33 und 34 DSGVO.

45 Das erhaltene Datenformat darf nur in den vier aufgeführten Fallgruppen, unter anderem zur Verbesserung der Interoperabilität, geändert werden.

46 Zusätzliche spezifische Werkzeuge und Dienste, insbesondere um den Datenaustausch zu erleichtern wie beispielsweise vorübergehende Speicherung, Pflege, Konvertierung, Anonymisierung und Pseudonymisierung, werden nur auf ausdrücklichen Antrag oder mit Zustimmung und für keinen anderen Zweck verwendet; in der Praxis muss diese Bedingung trennscharf von der Negativdefinition in Art. 2 Nr. 11 Buchst. a DGA abgegrenzt werden, wonach das Aggregieren, Anreichern oder Umwandeln von Daten gerade nicht Merkmal eines Datenvermittlungsdienstes sein soll.

Werkzeuge zur Einholung von Einwilligungen oder Erlaubnissen – Buchstabe n) und **allgemeine Sorgfalts- und Schutzpflichten** (Koppelungsverbot – Buchstabe b,[47] fairer, transparenter und nichtdiskriminierender Zugang zum Datenvermittlungsdienst – Buchstabe f, Betrugs- und Missbrauchsprävention – Buchstabe g, Gewährleistung der Geschäftskontinuität im Fall einer Insolvenz des Anbieters von Datenvermittlungsdiensten – Buchstabe h, Unterstützung betroffener Personen [„Sorgfaltspflicht"] – Buchstabe m,[48] Protokollierungspflicht der Datenvermittlungstätigkeit – Buchstabe o).

4. Zuständige Behörden und Überwachung der Einhaltung

92 Für die Wahrnehmung der Aufgaben im Zusammenhang mit dem Anmeldeverfahren für Datenvermittlungsdienste benennt jeder Mitgliedstaat nach **Art. 13 Abs. 1 Satz 1 DGA eine oder mehrere „zuständige Behörden"** und teilt deren Namen bis zum 24. September 2023 der Kommission mit. In Deutschland steht deren Benennung derzeit noch aus. Diese zuständigen Behörden müssen den **Anforderungen des Art. 26 DGA** genügen, das heißt insbesondere funktional unabhängig sein (Absatz 1 Satz 1) und ihre Aufgaben unparteiisch, transparent, kohärent und rechtzeitig wahrnehmen (Absatz 2). Die **Befugnisse der Datenschutz-Aufsichtsbehörden**, der nationalen Wettbewerbsbehörden, der für Cybersicherheit zuständigen Behörden und anderer Fachbehörden bleiben **unberührt**, **Art. 13 Abs. 3 Satz 1 DGA**. Dies muss auch für den Fall gelten, dass die zuständige Behörde im Rahmen der Überwachung nach Art. 14 Abs. 3 DGA (hierzu folgende Randnummer) keinen Verstoß gegen Kapitel III DGA feststellt, die zuständige Datenschutz-Aufsichtsbehörde hingegen zu dem Ergebnis kommt, dass die Tätigkeit eines Anbieters von Datenvermittlungsdiensten nicht mit der Datenschutz-Grundverordnung vereinbar ist.

93 Den für Datenvermittlungsdienste zuständigen Behörden obliegt nach **Art. 14 Abs. 1 DGA** – unter Umständen auf Antrag einer natürlichen oder juristischen Person[49] – auch die **Überwachung und Beaufsichtigung** der **Einhaltung der Anforderungen des Kapitels III**. Stellt die zuständige Behörde einen **Verstoß gegen Kapitel III DGA** fest, kann sie – nach Abfrage einer Stellungnahme des betreffenden Anbieters von Datenvermittlungsdiensten (Art. 14 Abs. 3 DGA) – die Beendigung des Verstoßes verlangen und zu diesem Zweck – auf der

47 Die kommerziellen Bedingungen für die Erbringung von Datenvermittlungsdiensten dürfen nicht von der Nutzung anderer Dienste desselben Anbieters abhängig sein.

48 Anbieter von Datenvermittlungsdiensten können betroffene Personen nur bei der Rechteausübung unterstützen, jedoch nicht zur genuinen Geltendmachung der Betroffenenrechte eingesetzt werden. Für die Vertretung von betroffenen Personen gelten insoweit die Vorgaben des Art. 80 DSGVO, die Anbieter von Datenvermittlungsdiensten aufgrund ihrer Gewinnerzielungsabsicht zumeist nicht erfüllen.

49 Missverständlich insoweit die deutsche Sprachfassung, die im Zusammenhang mit dem Antrag in Art. 14 Abs. 1 Satz 2 DGA von der Überwachung und Beaufsichtigung der „Einhaltung der Rechtsvorschriften durch Anbieter von Datenvermittlungsdiensten" spricht und einen weiterreichenden Aufsichtsbereich suggeriert. Aus der englischen Sprachfassung geht dagegen eindeutig hervor, dass Überwachungs- und Beaufsichtigungsgegenstand jeweils die Anforderungen des Kapitels III DGA sind: „The competent authorities for data intermediation services shall monitor and supervise compliance of data intermediation services providers with the requirements of this Chapter. The competent authorities for data intermediation services may also monitor and supervise the compliance of data intermediation services providers, on the basis of a request by a natural or legal person."

Grundlage nationaler Rechtsvorschriften[50] – gegebenenfalls abschreckende Geldstrafen[51] verhängen und/oder eine Verschiebung des Beginns beziehungsweise eine Aussetzung oder sogar eine Einstellung der Erbringung des Datenvermittlungsdienstes anordnen, **Art. 14 Abs. 4 UAbs. 1 DGA**.

5. Zusammenfassung

94 Die Regelungen zu Datenvermittlungsdiensten sollen durch Gewährleistung eines neutralen, fairen und sicheren Datenzugangs die Bündelung und den Austausch personenbezogener und nicht personenbezogener Daten erleichtern. Zu diesem Zweck werden den Anbietern von Datenvermittlungsdiensten vielfältige neue Pflichten auferlegt, die sich in der Praxis zugunsten von betroffenen Personen oder Dateninhabern und Datennutzern auswirken sollen. Allerdings stehen für die Anbieter von Datenvermittlungsdiensten diesen Pflichten – über Label und Logo hinaus – keine substantiellen Anreize zur Aufnahme beziehungsweise Durchführung eines solchen Dienstes gegenüber. Zumindest für Nutzer aus dem öffentlichen Bereich begründen Label- und Logonutzung zwar eine gewisse Vertrauensbasis hinsichtlich der Erfüllung der Anforderungen des Art. 12 DGA. Dessen umfangreiche Vorgaben begünstigen möglicherweise aber auch eine „Flucht" von Anbietern in andere, nicht erfasste und damit weniger „abgesicherte" Geschäftsmodelle.

[50] Hierzu Richter, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 11/2023, Art. 14 DGA Rn. 17 ff.

[51] Nach Art. 14 Abs. 4 UAbs. 1 Buchst. a DGA können „abschreckende Geldstrafen" „Zwangsgelder und Zwangsgelder mit Rückwirkung" umfassen. Zwangsgelder sind nach deutschem Rechtsverständnis allerdings keine Strafen, sondern dienen der Willensbeugung und sind damit notwendigerweise in die Zukunft gerichtet. Lediglich Geldstrafen und Bußgelder sind rückwirkende Bestrafungen für einen Verstoß.

V. Datenaltruismus

1. Konzept Datenaltruismus

Das vierte Kapitel des Daten-Governance-Rechtsaktes enthält unionsrechtliche Regelungen zum Datenaltruismus. In den Trilog-Beratungen hinzugekommen ist **Art. 16 DGA**, wonach die Mitgliedstaaten selbst durch organisatorische und/oder technische Regelungen Datenaltruismus fördern können („**nationale Strategien**"). Deutschland hat bisher (noch) keine solchen nationalen Strategien festgelegt. **95**

„Datenaltruismus" meint nach der Legaldefinition des **Art. 2 Nr. 16 DGA** „**die freiwillige gemeinsame Nutzung von Daten auf der Grundlage von Einwilligungen** betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten **oder einer Erlaubnis** anderer Dateninhaber zur Nutzung ihrer nicht personenbezogenen Daten, **ohne hierfür ein Entgelt zu fordern oder zu erhalten**, […] **für Ziele von allgemeinem Interesse gemäß dem nationalen Recht**. Solche Ziele sind etwa die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die staatliche Entscheidungsfindung oder die wissenschaftliche Forschung im allgemeinen Interesse". Das Konzept des Datenaltruismus soll es erleichtern, Daten für sehr weit gefasste, im allgemeinen Interesse liegende Ziele zur Verfügung zu stellen, wobei die bisherigen Möglichkeiten, Daten zur wissenschaftlichen Nutzung frei zur Verfügung zu stellen, erhalten bleiben. **96**

Dieser Ansatz ist im deutschen datenschutzrechtlichen Diskurs für personenbezogene Daten bislang unter dem Stichwort der **Datenspende** verortet und wurde auf der Grundlage von Einwilligungen nach der Datenschutz-Grundverordnung beispielsweise mit der Datenspende-App des Robert Koch-Instituts in der Corona-Pandemie[52] oder dem Programm „OpenSCHUFA"[53] auch praktisch umgesetzt. Für nicht personenbezogene Daten genügte die Gestattung des Zugangs beziehungsweise der Nutzung durch den berechtigten Dateninhaber. Der Daten-Governance-Rechtsakt etabliert nun erstmals unionsweite Regelungen für die Spende nicht personenbezogener Daten und ermöglicht zur Steigerung des Vertrauens der Datenspender die Eintragung als anerkannte datenaltruistische Organisation. **97**

Bei der in Kapitel IV DGA geregelten Datennutzung zu altruistischen Zwecken handelt es sich aus datenschutzrechtlicher Sicht um eine **Datenverarbeitung** in Form der Erhebung von Daten. Die hierfür erforderliche **Rechtsgrundlage** ergibt sich ausweislich Art. 2 Nr. 16 DGA bei Verarbeitung personenbezogener Daten aus einer Einwilligung der betroffenen Person und bei Verarbeitung nicht personenbezogener Daten aus einer Erlaubnis des Dateninhabers. Für **98**

[52] Nutzer von Fitnessarmbändern oder Smartwatches konnten über diese App bis zum 31. Dezember 2022 Daten zur Verfügung stellen, die auf mögliche Symptome von COVID-19 analysiert wurden, um die Ausbreitung der Pandemie besser erfassen zu können, siehe https://corona-datenspende.de/.

[53] Im Rahmen dieser Kampagne konnten Menschen ihre SCHUFA-Selbstauskunft „spenden", um mögliche diskriminierende Effekte des Scorings aufzudecken, siehe https://openschufa.de/.

die **Einwilligung** gelten **Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 9 Abs. 2 Buchst. a in Verbindung mit Art. 7, Art. 4 Nr. 11 und Art. 5 DSGVO** mit allen damit verbundenen inhaltlichen[54] und zeitlichen[55] Anforderungen, wie insbesondere der Grundsatz der Zweckbestimmtheit, die jederzeitige Widerrufsmöglichkeit und Fragen der Weiterverarbeitung.[56] Diese Anforderungen bedingen aufgrund des Vorrangs der Datenschutz-Grundverordnung (im Konfliktfall) nach Art. 1 Abs. 3 Sätze 1 bis 3 DGA das Institut des Datenaltruismus für personenbezogene Daten und können zur Nichtverwendbarkeit der Daten führen.

Beispiel: Willigt eine betroffene Person lediglich in die Verarbeitung ihrer gespendeten personenbezogenen Daten für einen ganzen Forschungsbereich (beispielsweise die Bekämpfung des Klimawandels) und nicht für ein konkretes Forschungsvorhaben ein, steht damit zum maßgeblichen Zeitpunkt der Erhebung der personenbezogenen Daten (dem Zeitpunkt der Spende) kein eindeutiger Verarbeitungszweck fest. Eine auf dieser Grundlage erteilte Einwilligung ist unwirksam und die darauf gestützte Datenverarbeitung mangels Rechtsgrundlage rechtswidrig.

Aber auch wenn die Einwilligung auf ein konkretes Forschungsvorhaben bezogen ist, kann sich der Verarbeitungszweck während dessen Dauer aufgrund neuer Erkenntnisse ändern, was eine erneute Einholung der Einwilligung erforderlich macht.

In beiden Fällen ist die (erneute) Einholung der Einwilligung zeitaufwendig und gegebenenfalls kostspielig. Fehlt die Einwilligung ganz oder ist sie nicht wirksam, dürfen die betreffenden Daten nicht verarbeitet werden.[57]

99 **Hinweis**: **Spender personenbezogener Daten** kann ausweislich des Gesetzeswortlauts nur eine **betroffene Person**, das heißt eine **identifizierte oder identifizierbare natürliche Person** sein, Art. 2 Nr. 7 DGA in Verbindung mit Art. 4 Nr. 1 DSGVO.

Die **Spende nicht personenbezogener Daten** wird dagegen vom „**Dateninhaber**“ veranlasst – dabei kann es sich gemäß Art. 2 Nr. 8 DGA um eine **juristische Person, einschließlich öffentlicher Stellen und internationaler Organisationen, oder um eine natürliche Person, die in Bezug auf die betreffenden Daten keine betroffene Person** ist, handeln. Damit kommen **auch öffentliche Stellen für nicht personenbezogene Daten als Spender** in Betracht, vorausgesetzt, sie sind nach Unions- oder nationalem Recht berechtigt, Zugang zu diesen nicht personenbezogenen Daten zu gewähren oder diese Daten weiterzugeben.

[54] Im Sinne der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO müssen Erhebungen personenbezogener Daten „dem Zweck angemessen […] sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“. Es sollen also nur Daten erhoben werden, die für die Erreichung des Zwecks notwendig sind.

[55] Da die Allgemeinwohlzwecke des Daten-Governance-Rechtsaktes unter den Forschungsbegriff und damit auch unter die Privilegierung des Art. 5 Abs. 1 Buchst. e Halbsatz 2 DSGVO fallen dürften, ist grundsätzlich eine längere Speicherdauer möglich. Allerdings ist solchen Allgemeinwohlzwecken – wie beispielsweise der Bekämpfung des Klimawandels – meist inhärent, dass ihre Erreichung erst nach langer Zeit oder sogar nie erfolgt. In einer solchen Konstellation könnten die Daten praktisch dauerhaft gespeichert werden, was zu einer möglichen Aushöhlung der Speicherbegrenzung führt.

[56] Bei Weiterverarbeitungen im Zusammenhang mit Datenaltruismus ist für den erforderlichen Kompatibilitätstest, wonach der Zweck der Weiterverarbeitung mit dem Erhebungszweck „nicht unvereinbar“ sein darf, an die Privilegierung für Archiv-, Statistik- und Forschungszwecke nach Art. 5 Abs. 1 Buchst. b Halbsatz 2 DSGVO zu denken, der wohl auch die Allgemeinwohlzwecke des Daten Governance Rechtsaktes unterfallen.

[57] Speziell für den Forschungsbereich wird daher das Konstrukt einer erweiterten Einwilligung (sogenannter „broad consent“) diskutiert, für den allerdings eine normative Grundlage fehlt.

Möchten öffentliche Stellen nicht personenbezogene Daten **an altruistische Organisationen spenden oder deren Datenbestand nutzen,** wird empfohlen, aus Schutz- und Sicherheitsgründen nur mit solchen datenaltruistischen Organisationen zusammenzuarbeiten, die in das nationale öffentliche Register der anerkannten datenaltruistischen Organisationen eingetragen sind und das unionsweite Label und Logo tragen (vergleiche Art. 17 Abs. 2 UAbs. 1 Satz 2, Art. 19 Abs. 1 DGA, Rn. 101, 104).

Aber nicht nur die Einwilligung steht im Spannungsverhältnis zwischen Datenschutz-Grundverordnung und Daten-Governance-Rechtsakt. Auch die Erwartung, dass die Sammlung von Daten durch datenaltruistische Organisationen „zur Einrichtung von Datenarchiven führt" (EG 46 Satz 1 DGA), widerspricht den für personenbezogene Daten nach Art. 1 Abs. 3 Sätze 1 bis 3 DGA zu berücksichtigenden Grundsätzen der Datenminimierung und Speicherbegrenzung in Art. 5 Abs. 1 Buchst. c und e DSGVO. 100

2. Anforderungen an datenaltruistische Organisationen

Eine Spende personenbezogener Daten ist, wie gesehen, **bereits de lege lata auf der Grundlage einer Einwilligung nach der Datenschutz-Grundverordnung** möglich; gegebenenfalls sind dann aber die Bedingungen für Anbieter von Datenvermittlungsdiensten zu beachten.[58] Datenaltruistische Organisationen im Sinne des Art. 2 Nr. 16 DGA können sich aber auch **optional nach Art. 18, 17 Abs. 1 DGA bei ihrer zuständigen nationalen Behörde als „anerkannte datenaltruistische Organisation" in ein öffentliches nationales Register eintragen** lassen und sich anschließend als „in der EU anerkannte datenaltruistische Organisation" bezeichnen und ein gemeinsames Logo verwenden, Art. 17 Abs. 2 UAbs. 1 Satz 2 DGA in Verbindung mit Durchführungsverordnung (EU) 2023/1622.[59] Solche anerkannten datenaltruistischen Organisationen genießen möglicherweise in der Praxis größeres Vertrauen als nicht anerkannte Organisationen und sind gemäß **Art. 15 DGA** grundsätzlich von den Vorschriften über Datenvermittlungsdienste in Kapitel III DGA freigestellt. Dafür müssen sie allerdings auch die – nicht unerheblichen – Eintragungs-, Transparenz-, Berichts- und Schutzanforderungen der Art. 18, 20 und 21 DGA erfüllen. 101

Art. 18 DGA statuiert als **allgemeine Eintragungsanforderungen** neben der Durchführung von datenaltruistischen Tätigkeiten (Buchstabe a) das Erfordernis von Rechtspersönlichkeit gemäß nationalem Recht (Buchstabe b), eine rechtlich und strukturell unabhängige Tätigkeit ohne Erwerbszweck (Buchstaben c und d) sowie die Wahrung des auf der Grundlage von Art. 22 Abs. 1 DGA genannten Regelwerks. Die „datenaltruistischen Tätigkeiten" nach Art. 18 Buchst. a DGA umfassen dabei die Verarbeitungen der gespendeten Daten zu den in Art. 2 Nr. 16 DGA aufgeführten Zwecken sowohl durch die datenaltruistische Person selbst als auch durch Dritte. Als mögliche datenaltruistisch tätige Organisationen kommen neben **juristi-** 102

[58] Die Ausnahme des Art. 15 DGA gilt nur für anerkannte datenaltruistische Organisationen.

[59] Durchführungsverordnung (EU) 2023/1622 der Kommission vom 9. August 2023 über die Ausgestaltung gemeinsamer Logos für die in der Union anerkannten Anbieter von Datenvermittlungsdiensten und datenaltruistischen Organisationen, ABl. EU L 200 vom 10. August 2023, S. 1.

schen Personen der Privatwirtschaft auch **Innungen, Handwerks-, Berufs- sowie Industrie- und Handelskammern** in Betracht, da diese als Körperschaften des öffentlichen Rechts – im Gegensatz zu Behörden – Rechtspersönlichkeit haben.

103 **Hinweis: Behörden** als Teil der unmittelbaren Staatsverwaltung sind **unselbständige Verwaltungseinheiten** in der Trägerschaft von Bund oder Land. Die mittelbare Staatsverwaltung erfolgt dagegen durch **juristische Personen des öffentlichen Rechts** als ausgegliederte Verwaltungsträger **mit eigener Rechtspersönlichkeit**, beispielsweise Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie Beliehene.

Die Möglichkeit von öffentlichen Stellen, **als datenaltruistische Organisation tätig** zu sein, bestimmt sich daher nach dem Rechtsträger.

104 Der **Eintragungsprozess** ist in **Art. 19 DGA** geregelt. Die Eintragung in das nationale öffentliche Register der anerkannten datenaltruistischen Organisationen des jeweiligen Mitgliedstaats erfolgt gemäß Art. 19 Abs. 1 DGA **auf Antrag**, gegebenenfalls am Sitz der Hauptniederlassung (Art. 19 Abs. 2 DGA) beziehungsweise der Niederlassung des gesetzlichen Vertreters (Art. 19 Abs. 3 DGA). Der Eintragungsantrag muss die in **Art. 19 Abs. 4 DGA** aufgeführten **Angaben** enthalten, deren Änderung fristgemäß mitzuteilen ist (Art. 19 Abs. 7 DGA). Führt die Bewertung des Eintragungsantrags durch die zuständige Behörde zu dem **Ergebnis**, dass die datenaltruistische Organisation die Anforderungen des Art. 18 DGA erfüllt, trägt die Behörde diese innerhalb von zwölf Wochen nach Antragseingang in das öffentliche nationale **Register** ein, **Art. 19 Abs. 5 UAbs. 1 Satz 1 in Verbindung mit Art. 17 Abs. 1 DGA**. Die Eintragung **gilt gemäß Art. 19 Abs. 5 UAbs. 1 Satz 2 DGA in allen Mitgliedstaaten**. Nach Mitteilung durch die zuständige Behörde nimmt die Kommission diese Eintragung in das **öffentliche Unionsregister** auf, **Art. 19 Abs. 5 UAbs. 2 Satz 2 in Verbindung mit Art. 17 Abs. 2 UAbs. 1 DGA**.

105 Die Vorgaben für datenaltruistische Organisationen sind dabei mit Blick auf die Überprüfungspflicht des Art. 19 Abs. 5 UAbs. 1 Satz 1 DGA im Vergleich zu den Anforderungen an (sonstige) Datenvermittlungsdienste strenger ausgestaltet. Hintergrund könnte sein, dass eine unentgeltliche Datenspende umso mehr Vertrauen darin erfordert, dass die Daten auch tatsächlich zu den gewünschten Zwecken von allgemeinem Interesse genutzt werden.

106 Derartig anerkannte datenaltruistische Organisationen treffen nach **Art. 20 DGA** umfangreiche **Transparenzanforderungen und Berichtspflichten** etwa in Bezug auf die Datenverarbeitung, welche durch die datenaltruistische Organisation selbst oder durch Dritte erfolgen kann, die Zweckverfolgung und die Einnahmequellen. EG 46 UAbs. 1 DGA nennt weitere Anforderungen wie eine sichere Verarbeitungsumgebung und die Einrichtung von Ethikräten, deren Durchsetzbarkeit mangels Regelung im verfügenden Teil des Daten-Governance-Rechtsaktes jedoch fraglich erscheint.

107 Zum **Schutz der Rechte und Interessen betroffener Personen und Dateninhaber** im Hinblick auf ihre Daten enthält **Art. 21 DGA** zusätzliche **besondere Anforderungen**, namentlich eine **Informationspflicht** zu Zielen und gegebenenfalls Zweck und Standort der Verarbeitung (Art. 21 Abs. 1 DGA und Art. 21 Abs. 6 DGA für die Verarbeitung durch Dritte), eine **Zweckbindungspflicht** (Art. 21 Abs. 2 DGA), eine **Pflicht zur Bereitstellung von Werkzeugen zur Einholung und zum Widerruf von Einwilligungen und Erlaubnissen** (Art. 21 Abs. 3 DGA), eine **Pflicht zur Sicherstellung eines angemessenen Sicherheitsniveaus** für

die Speicherung und Verarbeitung nicht personenbezogener Daten (Art. 21 Abs. 4 DGA) sowie eine **Unterrichtungspflicht bei unbefugter Verarbeitung** der geteilten nicht personenbezogenen Daten (Art. 21 Abs. 5 DGA).

Hinweis: Bei Verarbeitung personenbezogener Daten gelten zusätzlich die umfangreicheren Informations- und Meldepflichten der Datenschutz-Grundverordnung. 108

Um den Datenaltruismus operativ zu erleichtern, soll die Kommission ein „**Regelwerk**" mit Details zu unter anderem Betroffeneninformation und technischen Sicherheitsmaßnahmen als delegierten Rechtsakt erlassen, **Art. 22 DGA**. Ein solches liegt bislang nicht vor. 109

Als weitere Erleichterung der Erhebung von Daten auf der Grundlage des Datenaltruismus sieht **Art. 25 Abs. 1 und 2 DGA** vor, dass die Kommission für das Einholen von Einwilligungen und Erlaubnissen ein modulares **europäisches Einwilligungsformular für Datenaltruismus** schafft. Dieses Formular soll nach **Art. 25 Abs. 3 DGA für personenbezogene Daten auch die Anforderungen der Datenschutz-Grundverordnung** erfüllen und die Widerrufsmöglichkeit integrieren. Mit Blick auf diesen intendierten weiten Anwendungsbereich erscheint es nicht ausgeschlossen, dass dieses Formular nach Erlass auch in anderen Fällen als von der Kommission genehmigte Einwilligungserklärung zum Einsatz kommen wird. 110

3. Zuständige Behörden und Überwachung der Einhaltung

Jeder Mitgliedstaat benennt gemäß **Art. 23 Abs. 1 DGA** unter Wahrung der Anforderungen des **Art. 26 DGA eine oder mehrere „zuständige Behörden"**, die für das öffentliche nationale Register der anerkannten datenaltruistischen Organisationen zuständig sind, und teilt der Kommission bis zum 24. September 2023 deren Namen mit, Art. 23 Abs. 2 DGA. In Deutschland ist eine solche nationale Benennung bislang nicht erfolgt. 111

Nach **Art. 23 Abs. 3 DGA** nimmt die für die Eintragung von datenaltruistischen Organisationen zuständige Behörde ihre Aufgaben in Bezug auf die Verarbeitung personenbezogener Daten **in Zusammenarbeit mit der einschlägigen Datenschutz-Aufsichtsbehörde** sowie mit den einschlägigen sektoralen Behörden desselben Mitgliedstaats wahr. Eine dem Art. 13 Abs. 3 DGA vergleichbare ausdrückliche Regelung, wonach die Befugnisse der Datenschutz-Aufsichtsbehörden unberührt bleiben, fehlt zwar für den Bereich des Datenaltruismus, ergibt sich allerdings mit Blick auf **Art. 1 Abs. 3 Satz 2 DGA**, wonach der Daten-Governance-Rechtsakt unbeschadet der Datenschutz-Grundverordnung (und explizit) „einschließlich im Hinblick auf die Befugnisse der Aufsichtsbehörden" gelten soll. 112

Die zuständigen Behörden **überwachen und beaufsichtigen** – unter Umständen auf Antrag einer natürlichen oder juristischen Person[60] – auch die Einhaltung der in Kapitel IV DGA festgelegten Anforderungen, **Art. 24 Abs. 1 DGA**. Stellt die zuständige Behörde einen **Verstoß** 113

[60] Missverständlich wiederum (vergleiche Fn. 49) die deutsche Sprachfassung, die im Zusammenhang mit dem Antrag in Art. 24 Abs. 1 Satz 2 DGA von der Überwachung und Beaufsichtigung der „Einhaltung der Rechtsvorschriften durch diese datenaltruistischen Organisationen" spricht und einen weitreichenden Aufsichtsbereich suggeriert. Aus der englischen Sprachfassung geht auch hier eindeutig hervor, dass Überwachungs- und Beaufsichtigungsgegenstand jeweils die Anforderungen des Kapitels IV DGA sind: „The competent authorities for

gegen Kapitel IV DGA fest, kann sie gemäß **Art. 24 Abs. 3 und 4 DGA** – nach Abfrage einer Stellungnahme – die **Beendigung** des Verstoßes verlangen und ergreift angemessene und verhältnismäßige Maßnahmen, um die Einhaltung des Kapitels IV DGA sicherzustellen. **Besteht der Verstoß fort**, verliert die betreffende anerkannte datenaltruistische Organisation ihr Recht, die Bezeichnung „in der EU anerkannte datenaltruistische Organisation" zu führen, und wird aus dem einschlägigen öffentlichen nationalen Register gestrichen; diese Entscheidung wird öffentlich zugänglich gemacht, **Art. 24 Abs. 5 DGA**. Weitergehende Sanktionsmöglichkeiten sind nicht vorgesehen, da datenaltruistische Organisationen auch ohne Registrierung tätig sein dürfen.

4. Zusammenfassung

114 Auch beim Datenaltruismus überlässt der Verordnungsgeber die Erleichterung der Datenspende nach Art. 16 DGA weitgehend den Mitgliedstaaten. Hinzu kommt, dass die Zurverfügungstellung von personenbezogenen Daten für Allgemeinwohlzwecke gegenüber der Datenschutz-Grundverordnung nicht nur nicht erleichtert wird, sondern anerkannten datenaltruistischen Organisationen noch zahlreiche zusätzliche Pflichten auferlegt werden. Ob mit der Registrierung ein wesentlicher Mehrwert in Form einer Vertrauensförderung einhergeht, der diese Nachteile aufwiegt, wird die Praxis zeigen. Rein tatsächlich ist eine Spende (nicht) personenbezogener Daten auch auf der Grundlage einer Einwilligung nach der Datenschutz-Grundverordnung beziehungsweise einer Gestattung und ganz ohne registrierte datenaltruistische Organisationen möglich. Bestenfalls erleichtert aber das neue europäische Einwilligungsformular für Datenaltruismus gerade im Bereich der Forschung den flexiblen und einwilligungsbasierten Austausch von Daten.

the registration of data altruism organisations shall monitor and supervise compliance of recognised data altruism organisations with the requirements laid down in this Chapter. The competent authority for the registration of data altruism organisations may also monitor and supervise the compliance of such recognised data altruism organisations, on the basis of a request by a natural or legal person."

VI. Ergänzende Regelungen

Ergänzt werden die vorgenannten Regelungen durch allgemeine Vorgaben zu Verfahrensvorschriften und Sanktionen, die Einführung des Europäischen Dateninnovationsrats als neuem Expertengremium sowie durch Vorgaben zum – praktisch bedeutsamen – Transfer nicht personenbezogener Daten in Drittstaaten. 115

1. Verfahrensvorschriften, Art. 27 und 28 DGA, und Sanktionen, Art. 34 DGA

Art. 27 DGA statuiert – Art. 77 DSGVO nachgebildet – ein vom nationalen Gesetzgeber auszugestaltendes allgemeines **Beschwerderecht** für natürliche und juristische Personen in Bezug auf die Tätigkeit von Anbietern von Datenvermittlungsdiensten und anerkannten datenaltruistischen Organisationen, das bei den jeweils zuständigen Behörden auszuüben ist. Diese sind verpflichtet, den Sachverhalt nach pflichtgemäßem Ermessen aufzuklären und gegebenenfalls von ihren Befugnissen nach Art. 14 Abs. 3 bis 7 beziehungsweise Art. 24 Abs. 3 bis 6 DGA Gebrauch zu machen. Eine Beschwerde gegen Maßnahmen der zuständigen Behörde selbst ist auf dieser Grundlage dagegen nicht möglich. 116

Zudem steht jeder betroffenen natürlichen oder juristischen Person nach **Art. 28 DGA** das **Recht auf einen wirksamen gerichtlichen Rechtsbehelf** gegen rechtsverbindliche Entscheidungen der jeweils zuständigen Behörden gemäß Art. 14 (Datenvermittlungsdienste) und Art. 19, 24 DGA (anerkannte datenaltruistische Organisationen) sowie bei Untätigkeit der zuständigen Behörden auf eine Beschwerde hin zu. 117

Art. 34 Abs. 1 DGA schließlich verpflichtet die Mitgliedstaaten, **Vorschriften über Sanktionen** bei Verstößen von Anbietern von Datenvermittlungsdiensten und anerkannten datenaltruistischen Organisationen gegen die in Satz 1 explizit aufgeführten Vorgaben des Daten-Governance-Rechtsaktes zu erlassen und anzuwenden. Diese Sanktionen müssen nach Art. 34 Abs. 1 Satz 2 DGA **wirksam, verhältnismäßig und abschreckend** sein und sind der Kommission bis zum 24. September 2023 mitzuteilen, Art. 34 Abs. 1 Satz 4 DGA. Bei der **Verhängung von Sanktionen** sollen die Mitgliedstaaten die **Kriterien nach Art. 34 Abs. 2 Buchst. a bis e DGA** berücksichtigen. Auch insoweit steht in Deutschland eine nationale Regelung noch aus. Bei (Mit-)Betroffenheit personenbezogener Daten richtet sich die Rechtsdurchsetzung ausweislich Art. 1 Abs. 3 DGA nach den datenschutzrechtlichen Vorschriften. 118

2. Europäischer Dateninnovationsrat

119 **Art. 29 DGA** sieht die Einrichtung eines „**Europäischen Dateninnovationsrats**“ in Form einer **Expertengruppe**[61] vor, die sich unter anderem aus Vertretern der zuständigen mitgliedstaatlichen Behörden, des Europäischen Datenschutzausschusses, des Europäischen Datenschutzbeauftragten, der Kommission sowie weiterer europäischer Institutionen und Expertengremien zusammensetzt (vergleiche EG 53 DGA).

120 Der Europäische Dateninnovationsrat hat die in **Art. 30 DGA** im Einzelnen normierten **Aufgaben**, welche insbesondere die **institutionalisierte Beratung der Europäischen Kommission** bei verschiedenen Aspekten des Daten-Governance-Rechtsaktes umfassen.

3. Regelungen zum Transfer von nicht personenbezogenen Daten in und zum Zugang zu solchen Daten durch Drittstaaten

121 Gänzlich neu sind auch die Regelungen des **Art. 31 DGA**, der ein **Transferregime für nicht personenbezogene Daten** einführt, welches für die Weiterverwendung von nicht personenbezogenen vertraulichen oder durch Rechte des geistigen Eigentums geschützten Daten in einem Drittland in **Art. 5 Abs. 9 bis 14 DGA** eine **Spezialregelung** erfährt. Der Regulierungsansatz gleicht zwar nur in Einzelaspekten den Regelungen der Art. 44 ff. DSGVO betreffend die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen, zielt aber auf dieselben restriktiven Effekte ab.

122 Nach **Art. 31 Abs. 1 DGA** müssen öffentliche Stellen, Datenweiterverwender sowohl in Form natürlicher als auch juristischer Personen, Anbieter von Datenvermittlungsdiensten und anerkannte datenaltruistische Organisationen alle **angemessenen technischen, rechtlichen und organisatorischen Maßnahmen** ergreifen, um die **Übertragung** von in der Europäischen Union gespeicherten **nicht personenbezogenen Daten in Drittstaaten oder den Zugang von Regierungsorganisationen** zu diesen Daten zu **verhindern**, wenn Übertragung oder Zugang im Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats stünden.

123 **Hinweise:** Welche technischen, rechtlichen und organisatorischen Maßnahmen jeweils „angemessen“ sind, sollte differenzierend adressaten- und situationsspezifisch bestimmt werden. So obliegen natürlichen Personen als Weiterverwender in der Regel weniger umfangreiche Pflichten als wirtschaftlich starken Anbietern von Datenvermittlungsdiensten.

Öffentliche Stellen sollten ein Sicherheits- und Schutzkonzept betreffend den Transfer nicht personenbezogener Daten in Drittländer entwickeln und dessen Umsetzung sorgfältig dokumentieren.

124 **Entscheidungen von Gerichten oder Verwaltungsbehörden aus Drittstaaten**, die von den oben genannten Stellen oder Personen die Übermittlung von oder den Zugang zu nicht personenbezogenen Daten verlangen, können **gemäß Art. 32 Abs. 2 DGA nur anerkannt**

[61] Beschluss der Kommission zur Festlegung horizontaler Bestimmungen über die Einsetzung und Arbeitsweise von Expertengruppen der Kommission, C(2016) 3301 final, Internet: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2016)3301&lang=de.

oder vollstreckt werden, wenn sie auf einer **geltenden völkerrechtlichen Übereinkunft** wie etwa einem Rechtshilfeabkommen (mutual legal assistance treaty – MLAT) zwischen der Europäischen Union oder einem Mitgliedstaat und dem ersuchenden Drittstaat beruhen. **Besteht keine solche völkerrechtliche Übereinkunft** und würde die Befolgung der Entscheidung eines Gerichts oder einer Verwaltungsbehörde eines Drittlandes den Adressaten in Widerspruch zum Unionsrecht oder zum nationalen Recht des betreffenden Mitgliedstaats bringen, erfolgt die **Übertragung** der Daten an die Behörde des Drittlands oder die entsprechende Zugangsgewährung nach **Art. 31 Abs. 3 DGA nur dann, wenn** unter anderem das Rechtssystem des Drittlands die Darlegung der Gründe und der Verhältnismäßigkeit der Entscheidung verlangt und Einwände von Adressaten gegen Übertragungen oder Zugänge von Gerichten im Drittstaat geprüft werden.

Sind die in Art. 31 Abs. 2 oder 3 DGA festgelegten Bedingungen nicht erfüllt, so ist aufgrund einer vertretbaren Auslegung des Ersuchens **nur** die auf das Ersuchen hin **zulässige Mindestmenge an Daten** zu übertragen, **Art. 31 Abs. 4 DGA**. **125**

Nach **Art. 31 Abs. 5 DGA** ist der **Dateninhaber** grundsätzlich vorab über das Vorliegen eines jeden solchen Ersuchens zu **informieren**. **126**

Insgesamt ist anzunehmen, dass die neuen Regelungen zum internationalen Zugang zu und zur internationalen Übertragung von nicht personenbezogenen Daten in der Praxis noch erhebliche Aufmerksamkeit auf sich ziehen werden. **127**

4. Sonstiges

Zu den im Übrigen beachtenswerten Einzelregelungen des Daten-Governance-Rechtsaktes gehören der Fokus auf die besondere **Berücksichtigung der Belange von kleinen und mittleren Unternehmen sowie Start-up-Unternehmen** (Art. 6 Abs. 4, Art. 8 Abs. 3, Art. 11 Abs. 11 Satz 3 und Art. 29 Abs. 1 Satz 1 DGA), die **Pflichten und Befugnisse der Kommission zum Erlass von delegierten und Durchführungsrechtsakten** (Art. 5 Abs. 11 UAbs. 2, Art. 5 Abs. 12, Art. 11 Abs. 9 UAbs. 2, Art. 17 Abs. 2 UAbs. 2 Satz 1, Art. 22 Abs. 1 und Art. 25 Abs. 1 Satz 1 DGA) sowie der Vorschlag in EG 56 DGA, die Anmelde- und Eintragungsverfahren für Anbieter von Datenvermittlungsdiensten und anerkannte datenaltruistische Organisationen im Rahmen des **einheitlichen digitalen Zugangstors** nach der Verordnung (EU) 2018/1724[62] anzubieten. **128**

[62] 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, ABl. EU L 295 vom 21. November 2018, S. 1.

VII. Fazit

129 Der Daten-Governance-Rechtsakt enthält zwar umfassende Regelungen zur Standardisierung des Teilens von Daten im Binnenmarkt und soll einer übergreifenden Datenteilungskultur Vorschub leisten. Diese Regelungen sind allerdings primär organisatorischer oder institutioneller Natur und entfalten **keine materiell-rechtlich verpflichtende Wirkung**. Insbesondere beim Zugang zu behördlichen Daten ist noch ein **substanzielles eigenständiges Handeln der Mitgliedstaaten notwendig**, das kaum vorgesteuert wird und somit auch zuvor schon möglich war. Der gewünschte harmonisierende Effekt der Maßnahmen wird daher eher gering ausfallen und durch die **sehr umfangreichen Pflichten der einzelnen Akteure** unter Umständen noch zusätzlich konterkariert. Hinzu kommen die **möglichen Friktionen mit der Datenschutz-Grundverordnung** in Gestalt von weitreichenden Auslegungsfragen und strukturellen Widersprüchen.

130 Für den Zugang zu Daten der öffentlichen Hand stellt ausschließlich die Schaffung der „zentralen Informationsstelle" als zentralem Anlaufpunkt eine Fortentwicklung zur bisherigen Rechtslage dar, dessen Mehrwert erst in der Praxis erprobt werden muss. Auch für Stellen, die mit Gesundheits-, Mobilitäts-, Umwelt- und landwirtschaftlichen Daten arbeiten, mögen sich die Regelungen des Daten-Governance-Rechtsaktes aufgrund der nun strukturierter geregelten Datenteil- und -spendemöglichkeiten als interessant erweisen und durch das künftige europäische Einwilligungsformular für Datenaltruismus zusätzlich erleichtert werden.

131 Für eine umfassende Bewertung **fehlt** derzeit indes die **nationale Ausgestaltung** der zahlreichen den Mitgliedstaaten obliegenden Fragen in Bezug auf zuständige Stellen, Sanktionsregelungen etc. Wann und in welcher Form ein deutsches DGA-Umsetzungsgesetz in Kraft treten wird, ist – trotz Geltungsbeginns des Daten-Governance-Rechtsaktes und damit Ablauf der Umsetzungsfrist am 24. September 2023 – völlig offen.

132 Von praktischer Bedeutung wird schließlich auch sein, wie sich das bislang nur im Entwurf vorliegende **Datengesetz** zum Daten-Governance-Rechtsakt verhält. Trotz der begrifflichen Nähe widmen sich die beiden Verordnungen unterschiedlichen Regelungsgegenständen, die jedoch (in Teilen) komplementär zueinander stehen: Während der Daten-Governance-Rechtsakt Verfahren und Strukturen schafft, um die gemeinsame Datennutzung zu vereinfachen, soll das Datengesetz klären, wer unter welchen Bedingungen aus bestimmten Daten im privaten Besitz Wert schöpfen kann. Als Teil der europäischen Datenstrategie weisen die beiden Verordnungen Gemeinsamkeiten auf, beispielsweise die Privilegierungen von KMU und Start-up-Unternehmen sowie die nahezu wortlautgleichen Vorschriften zu Drittlandzugriffen und -transfers, für deren Konkretisierung auch unter dem Datengesetz der Europäische Dateninnovationsrat zuständig sein soll. In EG 35 Satz 3 Datengesetz-Entwurf, wonach für die Übermittlung an dritte Datenempfänger auch Datenvermittlungsdienste nach dem Daten-Governance-Rechtsakt in Betracht kommen, gibt es sogar eine unmittelbare Schnittstelle.