Bundesrat **Drucksache 639/23 (Beschluss)**

02.02.24

Beschluss
des Bundesrates

Entschließung des Bundesrates zum 2024 vorgesehenen Bericht der Europäischen Kommission über die Bewertung und Überprüfung gemäß Artikel 97 der 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)

Der Bundesrat hat in seiner 1041. Sitzung am 2. Februar 2024 die aus der Anlage ersichtliche Entschließung gefasst.

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0720-2946

Anlage

Entschließung des Bundesrates zum 2024 vorgesehenen Bericht der Europäischen Kommission über die Bewertung und Überprüfung gemäß Artikel 97 der 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)

Seit 25. Mai 2018 gilt mit der Datenschutz-Grundverordnung (DSGVO) ein europaweit einheitliches Datenschutzrecht. Nach Artikel 97 DSGVO hat die Europäische Kommission (im Folgenden Kommission) bis 25. Mai 2020 und danach alle vier Jahre einen Bericht über die Bewertung und Überprüfung der DSGVO vorzulegen. Im Rahmen dieser Evaluierung der DSGVO berücksichtigt sie unter anderem Standpunkte und Feststellungen des Europäischen Parlaments und des Rates, aber auch anderer einschlägiger Stellen oder Quellen (Artikel 97 Absatz 4 DSGVO).

Am 24. Juni 2020 hat die Kommission ihren ersten Bericht über die Bewertung und Überprüfung der DSGVO vorgelegt (COM(2020) 264 final).

Bereits im Rahmen dieser ersten Evaluierung hat der Bundesrat die Erfahrungen und Anliegen der Länder im Wege einer Entschließung (BR-Drucksache 570/19 (Beschluss)) dargelegt.

Eine erneute Überprüfung der DSGVO ist für das Jahr 2024 vorgesehen.

Der Bundesrat bittet die Bundesregierung und die Kommission in den weiteren Beratungen um die Berücksichtigung folgender Anliegen im Zuge der beabsichtigten Evaluierung:

1. Grundsätzliches

1.1 Der Bundesrat begrüßt die Absicht des Rates, im Zuge der Bewertung und Überprüfung der DSGVO gemäß deren Artikel 97 Absatz 4 eine Stellungnahme abzugeben und damit die Erfahrungen der Mitgliedstaaten frühzeitig in den Prozess einzubringen. In Anbetracht des Fortschritts der Beratungen im Rat richtet sich die vorliegende Stellungnahme des Bundesrates jedoch nicht nur an die Bundesregierung, sondern vor allem auch unmittelbar an die Kommission.

1.2 Der Bundesrat spricht sich nachdrücklich dafür aus, dass die Kommission diese Evaluierung – wie auch bereits im Jahr 2020 – auf weitere Fragestellungen als nur die in Artikel 97 Absatz 2 DSGVO genannten Kapitel V und VII der DSGVO erstreckt.

1.3 Der Bundesrat ist der Ansicht, dass sich die DSGVO nach nunmehr über fünf Jahren seit ihrem Inkrafttreten bewährt hat und zur europaweiten Harmonisierung datenschutzrechtlicher Standards nicht nur im Binnenmarkt, sondern durch ihre Ausstrahlungswirkung auch international zur Verbesserung des Schutzes der Grundrechte der von Datenverarbeitungen betroffenen Personen und zur Stärkung der Sensibilität und des Bewusstseins beim Umgang mit personenbezogenen Daten sowohl im öffentlichen als auch privaten Bereich maßgeblich beigetragen hat.

1.4 Der Bundesrat stellt jedoch fest, dass sich das Datenschutzrecht in Anbetracht aktueller wie künftiger technologischer, wirtschaftlicher, rechtlicher und zivilgesellschaftlicher Entwicklungen vielen Herausforderungen gegenüber sieht – genannt seien hier beispielhaft zum einen das Aufkommen von Systemen künstlicher Intelligenz (im Folgenden KI), zum anderen der zunehmend aus Forschung, Wirtschaft, Gesellschaft und öffentlichem Bereich kommunizierte Wunsch, vorhandene – auch personenbezogene – Daten im Sinne eines datenökonomischen Ansatzes zu unterschiedlichsten innovationsfördernden, datenaltruistischen oder anderen legitimen Zwecken zu nutzen und damit letztlich auch den in der DSGVO nach deren Artikel 1 Absatz 1 und Absatz 3 bereits angelegten Grundsatz des freien Verkehrs personenbezogener Daten zu verfolgen.

Für die notwendige Fortentwicklung des digitalen Binnenmarkts, insbesondere im Hinblick auf die Entwicklung eines umfassenden Rechtsrahmens für wissenschaftliche, ökonomische oder gesellschaftliche Anliegen zur Nutzung von Daten bis hin zur Entwicklung und Nutzung von KI-Technologien, muss die DSGVO ein stabiles und entwicklungsoffenes Fundament darstellen.

Um die Zukunftsfähigkeit der DSGVO auch weiterhin zu gewährleisten, bedarf es nach Auffassung des Bundesrates insbesondere folgender Anpassungen.

2. Erinnerung an die Stellungnahme des Bundesrates im Rahmen der Evaluierung 2020

2.1 Der Bundesrat erinnert zunächst an seine Stellungnahme im Rahmen der Evaluierung der DSGVO im Jahre 2020 (BR-Drucksache 570/19 (Beschluss)). Viele der dort vorgebrachten Anliegen beanspruchen auch heute noch Gültigkeit und werden im Rahmen der folgenden Nummern in Bezug genommen.

2.2 Dazu zählt insbesondere eine nach wie vor teils unklare und teils nicht in ausreichendem Maße auf die Bedürfnisse von kleinen und mittleren Unternehmen sowie von überwiegend ehrenamtlich tätigen Vereinen und sonstigen ehrenamtlich Tätigen eingehende Rechtslage.

3. Verhältnis der DSGVO zu anderen Unionsrechtsakten

Der Bundesrat bittet die Kommission, im Zusammenspiel der DSGVO mit anderen Unionsrechtsakten Kohärenz zu gewährleisten. Das Zusammenspiel der DSGVO mit einer Vielzahl jüngerer Unionsrechtsakte (vergleiche etwa Data Act, Data Governance Act, KI-Verordnung, Digital Services Act, Digital Markets Act, European Health Data Space) gestaltet sich nicht reibungsfrei und belastet deren Anwendung in der Praxis mit unnötigen Rechtsunsicherheiten. Die Vorgaben der DSGVO zu Datenschutz und Datensicherheit dürfen durch die genannten Rechtsakte nicht ausgehöhlt werden, aber auch nicht fälschlich als unverrückbare Universalstandards betrachtet werden.

3.1 So besteht beispielsweise Konfliktpotenzial zwischen dem Datenschutzrecht und dem Wesen von KI-Systemen, da deren Funktionsweise gerade auf der umfassenden Verarbeitung auch von personenbezogenen Daten beruht. In den

Rechtsakten enthaltene Klauseln, wonach die Regelungen der DSGVO unberührt blieben, helfen daher über im Einzelfall bestehende Widersprüche zwischen den Zielsetzungen der neuen Regelungen zur Nutzung von KI oder zur Etablierung einer europäischen Datenökonomie und den allgemeinen Vorgaben der DSGVO nicht hinweg. Eigentlich sollten die jeweiligen Rechtsakte von Anfang an eng miteinander abgestimmt sein; jedenfalls sollten sie in noch laufenden Rechtssetzungsprozessen entsprechend harmonisiert beziehungsweise vor ihrer Geltung etwaige Unklarheiten für die Rechtsanwender zumindest durch Anwendungshinweise ausgeräumt werden.

3.2 Bedeutung und Stärke der DSGVO liegen, wie schon die Worte „Grund"-Verordnung – oder noch deutlicher „General" Data Protection Regulation – zum Ausdruck bringen, gerade in ihren Grundsätzen, nicht einem unantastbaren Geltungsanspruch im Detail. Angesichts zahlreicher neuer Bedingungen der Verarbeitung personenbezogener Daten, für die die Rechtsakte der europäischen Digitalstrategie nunmehr zunehmend konkrete Rahmenbedingungen setzen, gibt die zweite Evaluation der DSGVO darüber hinaus Anlass dazu zu analysieren, ob die DSGVO durch weitere Rechtsakte fortentwickelt werden sollte, um den Schutz personenbezogener Daten in der digitalen Transformation durch risikogerechte bereichsspezifische Regelungen effektiver, rechtssicherer und praxisgerechter auszugestalten.

4. Datenschutzrechtliche Anforderungen als Belastung von kleinen und mittleren Unternehmen

Der Schutz personenbezogener Daten und die Gewährleistung ihrer rechtskonformen und sicheren Verarbeitung ist für Unternehmen unabhängig von ihrer Größe meist Grundlage von Wertschöpfung, aber auch von Vertrauen und Reputation bei Kundeninnen und Kunden sowie Beschäftigten. Trotzdem steht der praktische Aufwand für die Erfüllung dieser Anforderungen in Kernbereichen der DSGVO wie dem Grundsatz der Rechenschaftspflicht oder Informationspflichten vielfach im Missverhältnis zum erkennbaren Mehrwert für Betroffene und wird daher immer wieder als unverhältnismäßige bürokratische Belastung wahrgenommen:

4.1 Dokumentations- und Rechenschaftspflicht nach Artikel 5 Absatz 2 DSGVO

Der Bundesrat stellt fest, dass die Verantwortlichen für eine rechtssichere Dokumentation die technischen Funktionsweisen der Systeme ihrer Auftragsverarbeiter nicht nur kennen, sondern durchdringen müssen. Soweit es sich bei den Kunden und späteren Verantwortlichen um kleine und mittlere Unternehmen, überwiegend ehrenamtlich tätige Vereine und sonstige ehrenamtlich Tätige und auf Seiten der Auftragsverarbeiter um teils große Cloud-Diensteanbieter mit erheblicher Marktmacht handelt, wird die Kommission gebeten, Wege zu prüfen, die Anforderungen an eine rechtssichere Dokumentation im Sinne des Artikels 5 Absatz 2 DSGVO – zumindest in den genannten Fällen – auf ein angemessenes Maß zu reduzieren. Denn in den genannten Fällen dürften zu strenge Anforderungen an die Rechenschaftspflicht regelmäßig zu einer Überforderung der Verantwortlichen führen. Beispielsweise mit der Möglichkeit, auf eine Online-Dokumentation des Auftragsverarbeiters beziehungsweise Cloud-Diensteanbieters und umgekehrt auf die Verfahrensdokumentation der Verantwortlichen beziehungsweise Kunden zur Beschreibung von Geschäftsgegenstand, Arten und Kategorien von Daten zu verweisen, könnten die Dokumentations- und Rechenschaftspflichten bereits erheblich vereinfacht werden.

4.2 Transparenz- und Informationspflichten nach den Artikeln 12 fortfolgende DSGVO

Der Bundesrat erinnert an Nummer 2.2 der bereits erwähnten Stellungnahme im Rahmen der Evaluierung der DSGVO 2020 (BR-Drucksache 570/19 (Beschluss)). Er ist der Ansicht, dass die in der DSGVO vorgesehenen Informationspflichten insbesondere für kleine und mittlere Unternehmen sowie überwiegend ehrenamtlich tätige Vereine und sonstige ehrenamtlich Tätige, deren Kerntätigkeit gerade nicht in der Verarbeitung von personenbezogenen Daten besteht, eine Herausforderung darstellen können. Im Hinblick auf Erwägungsgrund 13, der den Auftrag gibt, bei der Anwendung der DSGVO die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen, wird die Kommission gebeten zu prüfen, ob und wie die Informationspflicht bei risikoarmen Verarbeitungsprozessen – etwa durch Erleichterungen im Hinblick auf den Umfang und die Art und Weise der Informationserteilung –

vereinfacht werden kann und wie Erleichterungen für den Business-to-Business-Bereich im Rahmen der Artikel 12 ff. DSGVO geschaffen werden können.

4.3 Evaluation und Förderung von Best-Practice-Projekten

Flankierend zur Prüfung normativer Nachbesserungen im Interesse der Entlastung von kleinen und mittleren Unternehmen sollte die Kommission die Wirksamkeit der bereits von ihr genauso wie etwa von den Datenschutzaufsichtsbehörden auf den Weg gebrachten Anwendungshilfen für kleine Unternehmen systematisch überprüfen. Der Bundesrat bittet, dabei auch aufzuzeigen, wie die Wahrnehmung und Zielerreichung solcher Hilfestellungen für diese den Wohlstand und die wirtschaftliche Leistungsfähigkeit Europas sichernden Unternehmen verbessert werden kann, und weitere Förderansätze aufzuzeigen, die auch die rechtssichere Handhabung datenschutzrechtlicher Regelungen im Ehrenamt unterstützen.

5. Recht auf Auskunft nach Artikel 15 DSGVO

Nach Auffassung des Bundesrates sind Inhalt und Reichweite des Artikels 15 Absatz 1 und Absatz 3 DSGVO in der praktischen Umsetzung der Verantwortlichen – trotz neuerer Rechtsprechung des Europäischen Gerichtshofs (Urteil vom 4. Mai 2023 – C- 487/21) – nach wie vor in weiten Teilen unklar. Um eine ausufernde Bürokratisierung im Rahmen der Auskunftserteilung (zum Beispiel durch umfassende Sichtungen und gegebenenfalls Schwärzungen) einerseits sowie ein Unterlaufen von nationalen Auskunfts- und Informationszugangsregelungen andererseits zu verhindern, wird die Kommission gebeten, die in diesem Regelungsbereich verbleibenden Rechtsunsicherheiten auch durch ergänzende Bestimmungen zu beseitigen, die Rechtsmissbrauch und unvertretbaren Einschränkungen anderer Grundrechtspositionen wie dem Schutz von Geschäftsgeheimnissen entgegenwirken.

6. Anforderungen an automatisierte Entscheidungen nach Artikel 22 DSGVO

Automatisierte Entscheidungen einschließlich Profiling und Scoring nehmen an Bedeutung zu. In Artikel 22 DSGVO werden Anforderungen an die Zulässigkeit von solchen automatisierten Entscheidungen im Einzelfall getroffen. Materielle Anforderungen an die Richtigkeit der Datengrundlage,

einschließlich der Vermeidung von Verzerrungen („Bias“) oder an die mathematische Ermittlung der Ergebnisse werden nicht gestellt. Soweit automatisierte Entscheidungen zulässig sind, sollten sie auf wissenschaftlichen Standards beruhen und zu diskriminierungsfreien Ergebnissen führen. Der Entwurf der KI-Verordnung lässt zwar Ansätze für entsprechende Regelungen erkennen, jedoch werden hiervon voraussichtlich nicht alle der unter Artikel 22 DSGVO fallenden Sachverhalte erfasst. Die Kommission wird daher gebeten zu prüfen, ob Qualitätsanforderungen für automatisierte Entscheidungen etabliert und insbesondere ein wirksamer Schutz vor Diskriminierung eingerichtet werden könnten.

7. Gemeinsame Verantwortlichkeit nach Artikel 26 DSGVO

Wie bereits in Nummer 2.4 der Stellungnahme im Rahmen der Evaluierung der DSGVO 2020 (BR-Drucksache 570/19 (Beschluss)) aufgezeigt, bestehen nach wie vor Rechtsunsicherheiten zur Frage, wann eine gemeinsame Festlegung der Zwecke und der Mittel zur Verarbeitung im Sinne des Artikels 26 DSGVO stattfindet und welcher Beitrag ausreicht, um eine gemeinsame Verantwortung anzunehmen. Insbesondere auch die Rechtsprechung des Europäischen Gerichtshofs (Urteil vom 5. Juni 2018 – C-210/16) zur Frage der gemeinsamen Verantwortlichkeit von Betreibern und Nutzern von Social-Media-Plattformen hat nach den Erkenntnissen des Bundesrates in der Praxis nicht zu Rechtssicherheit, sondern -unsicherheit geführt. Der Bundesrat bittet die Kommission daher erneut, in ihrem Bericht einen Vergleich der tatsächlichen Anwendung durch die Aufsichtsbehörden vorzunehmen und zu prüfen, wie eine Präzisierung erreicht werden kann.

8. Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 DSGVO

Wie der Bundesrat bereits in Nummer 2.6 seines Beschlusses vom 8. November 2019 dargelegt hat (BR-Drucksache 570/19 (Beschluss)), verbleibt für die von der Pflicht zur Führung eines Verarbeitungsverzeichnisses eine Ausnahme vorsehende Regelung des Artikels 30 Absatz 5 DSGVO aufgrund der dort vorgesehenen Gegenausnahmen kaum ein nennenswerter Anwendungsbereich. Die Regelung bringt daher insbesondere für kleine und mittlere Unternehmen keine Entlastung. Da sich etwa bereits Datenverarbeitungen zur Personalverwaltung (zum Beispiel bei Arbeitsunfähigkeitsbescheinigungen als Gesundheitsdatum) und Lohnabrechnung (zum Beispiel Kirchensteuer-

pflichtigkeit erlaubt Rückschlüsse auf Religionszugehörigkeit) mit den Ausnahmetatbeständen des Artikels 30 Absatz 5 DSGVO nicht vereinbaren lassen, sind auch bei Unternehmen mit weniger als 250 Mitarbeitern in den meisten Fällen alle Verarbeitungen in einem Verzeichnis aufzuführen. Bereits im Rahmen ihres Berichts aus dem Jahr 2020 hatte die Kommission eine Prüfung in Aussicht gestellt, diesbezüglich eine gezielte Änderung vorzuschlagen. Im Hinblick auf den bereits genannten Erwägungsgrund 13 wird die Kommission daher gebeten, zu prüfen, wie sich diesbezüglich tatsächliche Erleichterungen im Rahmen eines risikobasierten Ansatzes erreichen lassen.

9. Fragen der Anonymisierung

9.1 Der Bundesrat ist der Ansicht, dass die Maßnahme der Anonymisierung personenbezogener Daten einen wesentlichen Baustein darstellt, um die entsprechenden Daten zu vielfältigen Zwecken nutzbar zu machen, soweit ein Personenbezug hierfür gerade nicht erforderlich ist. Aus diesem Grund wird das Mittel der Anonymisierung in bereichsspezifischen Unionsrechtsakten vermehrt vorgesehen.

Aus Sicht des Bundesrates ist jedoch weiterhin nicht geklärt, welche Anforderungen aus datenschutzrechtlicher Sicht an eine in Erwägungsgrund 26 lediglich genannte Anonymisierung zu richten sind und wie diese praxistauglich umgesetzt werden können.

9.2 Mit Blick auf die auch für die Datenstrategie der Europäischen Union immer wichtiger werdenden Möglichkeiten der Anonymisierung verfolgte zuletzt etwa das Europäische Gericht mit Urteil vom 26. April 2023 (T-557/20) den Ansatz, dass keine „absolute“ Anonymisierung erforderlich sei, um den Anwendungsbereich der DSGVO zu verlassen. Das Gericht folgt vielmehr einer risikobasierten Betrachtung und wendet einen „relativen“ Ansatz an. Die Kommission wird daher gebeten zu prüfen, ob sich in diesem Kontext zum Zwecke der Rechtssicherheit unter Berücksichtigung einer zu erwartenden Klärung der durch die Entscheidung des Europäischen Gerichts aufgeworfenen Fragen durch den Europäischen Gerichtshof normative Klarstellungen anbieten.

9.3 Rechtsunsicherheit besteht zudem bislang noch im Hinblick auf die Frage, ob der Vorgang der Anonymisierung selbst eine Datenverarbeitung nach Artikel 4 Nummer 2 DSGVO darstellt, welche ihrerseits somit das Vorliegen einer Rechtsgrundlage im Sinne des Artikels 6 beziehungsweise 9 DSGVO voraussetzt.

10. Rahmenbedingungen für datenschutzrechtliche Zertifizierungen und Verhaltensregeln verbessern nach den Artikeln 40 fortfolgende DSGVO

Der Bundesrat erinnert an Nummer 3.1 der Stellungnahme im Rahmen der Evaluierung der DSGVO 2020 (BR-Drucksache 570/19 (Beschluss)). Fünf Jahre nach Geltungsbeginn der DSGVO haben sich die als eine der zentralen Fortentwicklungen aufgenommenen Instrumente der Selbstregulierung durch datenschutzrechtliche Zertifizierungen und Verhaltensregeln in der datenschutzrechtlichen Praxis nach Auffassung des Bundesrates weder etabliert, noch bestehen zumindest breitere Angebote solcher Verfahren, die die Erwartung auf eine zeitnahe Marktverbreitung solcher Instrumente rechtfertigen würden. Die Evaluierung sollte daher zum Anlass genommen werden, die Rahmenbedingungen dieser für Rechtssicherheit insbesondere bei kleinen und mittleren Unternehmen genauso wie für digitale Innovationen essentiellen Rechtsinstrumente zu analysieren, Schwachstellen oder Defizite aufzuzeigen und Verbesserungsmaßnahmen – sei es durch normative Änderungen, sei es durch indirekte Anreize, Fördermaßnahmen oder Aufklärungskampagnen – aufzuzeigen.

11. Datenschutzrechtliche Erleichterungen in Reallaboren

Um Innovationsanreize zu setzen, bittet der Bundesrat die Kommission zu prüfen, ob Erleichterungen für die Verarbeitung personenbezogener Daten in Reallaboren etabliert werden können, wie beispielsweise ein Tatbestand, der die Verarbeitung personenbezogener Daten für Erprobungsszenarien in räumlich und zeitlich beschränkten Reallaboren zulässt, sofern die Durchführung behördlich begleitet wird. Es wird um Prüfung gebeten, ob darüberhinausgehende Erleichterungen im Hinblick auf Betroffenenrechte, Informations- oder Dokumentationspflichten in Reallaboren möglich sind.

12. Plädoyer für eine Regelung zur Verantwortung von Herstellern

Der Bundesrat ist in Anbetracht der Probleme, mit welchen sich Verantwortliche und Auftragsverarbeiter beispielsweise im Rahmen ihrer Rechenschaftspflicht, aber auch im Hinblick auf die Konzentration der Marktmacht bestimmter Software-Hersteller konfrontiert sehen, der Ansicht, dass ein Anknüpfen der datenschutzrechtlichen Verantwortung allein bei Verantwortlichem und Auftragsverarbeiter zu kurz greift.

Aus Sicht des Bundesrates sollten Hersteller selbst gewährleisten müssen, dass die von ihnen in Verkehr gebrachten Produkte datenschutzkonform sind, um dadurch alle Anwender, wie beispielsweise auch kleine und mittlere Unternehmen, die diese Produkte einsetzen, zu entlasten. Ein paralleler Gedanke findet sich nicht nur im geplanten Cyber-Resilience-Act zur Cybersicherheit von IT-Produkten für deren gesamten Lebenszyklus, sondern auch in der KI-Verordnung im Hinblick auf das Inverkehrbringen von KI-Systemen. Auch die DSGVO sieht mit Artikel 25 (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) eine Regelung vor, die bereits lange bevor es auch nur zur Erhebung konkreter Daten kommt, den Schutz dieser Daten durch Voreinstellungen und Gestaltung der Technik vorsieht. Die bisherige Systematik zielt jedoch nur auf den Verantwortlichen ab. Für Hersteller ergibt sich nach Erwägungsgrund 78 der DSGVO bislang lediglich eine unverbindliche Ermutigung, das Recht auf Datenschutz bei der Entwicklung und Gestaltung ihrer Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen in der Lage sind, ihren Datenschutzpflichten nachzukommen.

Im Hinblick darauf, dass entsprechende Regelungen mit Verweis auf deren spezifisch datenschutzrechtlichen Bezug weder im Rahmen der Überarbeitung der EU-Produkthaftungsrichtlinie noch der EU-Produktsicherheitsverordnung Einzug gefunden haben, bietet sich die DSGVO als geeigneter Standort für eine derartige generelle unionsrechtliche Regelung an.

Die DSGVO sollte daher dahingehend überprüft werden, ob eine Verpflichtung von Herstellern und Anbietern digitaler Produkte und Dienste im Unionsrecht getroffen werden könnte, wonach diese ihre Produkte und Dienste verpflichtend zu zertifizieren hätten oder auf sonstige Weise sicherstellen müssten, dass nur Produkte und Dienste auf den Markt gebracht

werden, die nach ihren Voreinstellungen im typischen Kreis ihrer Nutzer beziehungsweise datenschutzrechtlich Verantwortlichen den Anforderungen der DSGVO genügen. Zur Erfüllung solcher Verpflichtungen wären zum Beispiel hinreichende Einwilligungs- oder Löschprozesse vorzusehen, Datensicherheitsstandards „ab Werk“ zu aktivieren oder im Falle etwaiger Drittstaatentransfers hinreichende Garantien vorzusehen. Dies würde für den Anwender entsprechender Produkte, mithin den späteren Verantwortlichen, auch eine Erleichterung im Rahmen seiner Rechenschaftspflicht nach Artikel 5 Absatz 2 DSGVO bedeuten und den in den voranstehenden Beiträgen aufgezeigten Anwendungsschwierigkeiten gerade im Bereich der kleinen und mittleren Unternehmen entgegenwirken. Zugleich würde die Effektivität der Tätigkeit der Aufsichtsbehörden im Sinne des Artikel 51 DSGVO gestärkt, wenn sie bereits an der Ursache möglicher Rechtsbeeinträchtigungen ansetzen könnten.

Angesichts des Vorbildcharakters der Hersteller- und Anbieterverantwortung in den Vorschlägen zum Cyber-Resilience-Act und zur KI-Verordnung erscheint eine Initiative zur datenschutzrechtlichen Hersteller- und Anbieterverantwortung fünf Jahre nach Geltungsbeginn der DSGVO mittlerweile als eine der wirksamsten und systemkonformsten Impulse zur Verbesserung des Schutzes personenbezogener Daten. Die unter dem Dach des Europäischen Datenschutzausschusses durchgeführte gemeinsame Untersuchung mehrerer europäischer Datenschutzaufsichtsbehörden zum Einsatz von Cloud-Diensten im öffentlichen Sektor („2022 Coordinated Enforcement Action – Use of cloud-based services by the public sector“ vom 17. Januar 2023) wie auch weitere Untersuchungen zu spezifischen Produkten (etwa zu Microsoft 365 durch den Europäischen Datenschutzbeauftragten [„Ongoing Investigation into the use of M365 by EUIS after Schrems II“] und eine Arbeitsgruppe deutscher Aufsichtsbehörden [vgl. Bericht der Arbeitsgruppe „Microsoft-Onlinedienste“ und die dazugehörige Festlegung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24. November 2022]) belegen mehrfach, dass Verantwortliche angesichts der unzureichenden Berücksichtigung europäischer Datenschutzstandards in Produkten und Diensten global agierender Hersteller oder Anbieter vor beträchtlichen Herausforderungen stehen. Da zudem vergaberechtliche Entscheidungen in verschiedenen Mitgliedstaaten (Conseil d’État, Beschluss N° 450163 vom 12. März 2021; Vergabekammer Baden-

Württemberg, Beschluss vom 13. Juli 2022, 1 VK 23/22; OLG Karlsruhe, Beschluss vom 7. September 2022 – 15 Verg 8/22) wiederholt Rechtsunsicherheiten bei der Frage aufgezeigt hatten, durch wen und nach welchen Maßstäben die Erfüllung datenschutzrechtlicher Anforderungen durch ein bestimmtes Produkt oder einen einzelnen IT-Service nachzuweisen ist, würde eine gesetzliche Konformitätsverpflichtung von Herstellern oder Anbietern von IT-Dienstleistungen auch insoweit einen nachhaltigen Beitrag zu mehr Rechtssicherheit und datenschutzgerechter Digitalisierung leisten und den Vollzug durch die Datenschutzaufsichtsbehörden effektivieren.

13. Berücksichtigung durch die Bundesregierung

Die Bundesregierung wird gebeten, den in der Entschließung genannten Handlungsbedarf im weiteren Verlauf der Diskussion auf Unionsebene zu berücksichtigen.

14. Direktzuleitung an die Kommission

Der Bundesrat übermittelt diese Stellungnahme direkt an die Kommission.