Entschließung

der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes

und der Länder vom 10. März 2026

Stellungnahme zum Digital Fitness Check

Vorschläge zu Modifikationen der DSGVO

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beteiligt sich aus einer praktischen Perspektive am „Digital Fitness Check" der Europäischen Kommission zum Daten- und Digitalrecht der Europäischen Union. Sie spricht sich für wohldosierte und zielgerichtete Modifikationen der Datenschutz-Grundverordnung aus, die einen noch effektiveren Grundrechtsschutz – insbesondere für besonders schutzbedürftige betroffene Personen und im Einklang mit Herausforderungen des technischen Wandels – sicherstellen würden.

1. Grundlegende Einschätzung

Die grundlegenden Regelungen der DSGVO sind in Zeiten weit reichender Digitalisierung vieler Lebensbereiche erforderlich, um eine effektive Wirksamkeit und Durchsetzung des Grundrechts auf Datenschutz aus Art. 8 GRCh zu erreichen. Dabei wirkt Datenschutz nicht nur als informationelle Selbstbestimmung, sondern flankiert als Basis für freie Meinungsäußerung und politische Partizipation auch weitere Grundrechte (Achtung des Privatlebens, Art. 7, Meinungsfreiheit, Art. 9, Versammlungsfreiheit, Art. 12 GR-Charta). Diese Grundrechtsorientierung macht die DSGVO zu einem funktionalen und zentralen Bestandteil des Datenrechts in Europa. Dies wird durch das Verhältnis zu den EU-Digitalrechtsakten deutlich, die die Geltung der Datenschutz-Grundverordnung grundsätzlich unberührt lassen.

Darüber hinaus hat sich die DSGVO als globaler Maßstab etabliert, viele Staaten der Welt haben nach ihrem Vorbild eigene ähnliche Regelungen getroffen (Brussels Effect). Dies hilft gerade auch global tätigen Unternehmen mit Sitz in der EU.

Die DSGVO ist ein Erfolg und geeignet, ihre Ziele zu erreichen. Sie kann aber aktualisiert und auf die neueren Entwicklungen in Rechtsprechung und Praxis ausgerichtet werden. Die Datenschutzaufsichtsbehörden haben umfangreiche Erfahrungen gesammelt, die für zielorientierte Modifikationen einzelner Regelungen nutzbar gemacht werden können und damit zur Durchsetzung der datenschutzrechtlichen Regeln im aktuellen technischen und normativen Kontext beitragen können.

Der normative Kontext wird durch das Digitalrecht der EU geprägt. Die Digitalrechtsakte verfolgen das legitime Ziel, den digitalen Binnenmarkt zu stärken und eine angemessene Datennutzung zu ermöglichen. Datennutzung und Datenschutz müssen dabei vereinbar sein. Deswegen bedarf es einer

rechtlichen Fortentwicklung des europäischen Rechtsrahmens bei gleichwertigem Schutz aber besserer Harmonisierung der Rechtsakte untereinander. Das Zusammenspiel der Rechtsakte mit der DSGVO ist Gegenstand von Leitlinien des EDSA, erfordert aber darüber hinaus eine grundlegende Konsolidierung, wie sie bereits 2021 durch den Europäischen Datenschutzausschuss gefordert wurde (https://www.edpb.europa.eu/system/files/2022-04/edpb_statement_on_the_digital_services_package_and_data_strategy_de_0.pdf).

Die hier vorgeschlagenen Modifikationen der DSGVO bringen insoweit lediglich punktuelle Verbesserungen, weitere Schritte sind erforderlich.

Die (inzwischen 10 Jahre alte) DSGVO muss auch den technischen und ökonomischen Entwicklungen gerecht werden und Innovation einen verlässlichen Rahmen bieten, damit Rechtssicherheit und Innovation Hand in Hand gehen. Angesichts der dynamischen technischen Entwicklungen auf dem Gebiet der KI und ihren vielfältigen Einsatzmöglichkeiten sollten hier ungeachtet der grundsätzlichen Technologieneutralität spezifische Regelungen getroffen werden, um Innovation zu ermöglichen und zugleich ein hohes Schutzniveau für den Datenschutz der Bürgerinnen und Bürger sicherzustellen.

Die möglichen und sinnvollen Modifikationen der DSGVO dürfen dagegen nicht ihre grundlegenden Prinzipien berühren. Die zentralen Regelungen der Art. 5, 6 DSGVO sollten grundsätzlich nicht angetastet werden. Die DSGVO hat einen einheitlichen, unmittelbar geltenden Rechtsrahmen für den Schutz personenbezogener Daten in allen Mitgliedstaaten geschaffen und damit das in Art. 8 GRCh verankerte Grundrecht in ein effektiv durchsetzbares Individualrecht überführt. Ein substanzielles Abschwächen ihrer Prinzipien könnte unabsehbare Folgen für den digitalen Grundrechtsschutz haben.

Die DSK spricht sich daher für eine zielgenaue Modifikation einzelner Vorschriften der DSGVO aus. Dies steht unter dem Vorzeichen der Vereinfachung und zugleich der Wahrung eines hohen Schutzniveaus. Diese Ziele können mit wohldosierten punktuellen Änderungen effektiv erreicht werden, ohne die Grundlagen der DSGVO anzutasten.

2. Zielgenaue Änderungsvorschläge der DSGVO

Änderungen der DSGVO sollten unter Beibehaltung des hohen Schutzniveaus Entlastungen für Unternehmen, eine einfachere Umsetzung und Durchsetzung der Vorschriften und einen effektiven Schutz der Einzelnen erreichen.

Diesen Zielen dienen insbesondere folgende Vorschläge:

a. Klarstellung des Begriffs der biometrischen Daten

Die Definitionen der DSGVO sollten nur bei echtem und begründetem Klarstellungsbedarf modifiziert werden, um das oben dargestellte, valide Grundgerüst der DSGVO nicht zu destabilisieren und dadurch Rechtsunsicherheit zu produzieren.

Die Reichweite des Begriffs der biometrischen Daten im Sinne des Art. 4 Nr. 14 DSGVO ist unklar, insbesondere vor dem Hintergrund der voranschreitenden technischen Entwicklungen in diesem Bereich. Da die Definition u.a. Auswirkung auf den Anwendungsbereich des Art. 9 Abs. 1 DSGVO hat, ist eine Klarstellung erforderlich. Insbesondere wird der Begriff der „speziellen Techniken“ nur in dem Sinne kontextuell beschrieben, indem der technische Prozess zur Gewinnung/Verarbeitung biometrischer Daten dargestellt wird (siehe ErwG 51). Durch die Aufnahme konkreter Beispiele könnte

mehr Klarheit geschaffen werden und damit die Abgrenzung zwischen biometrischen und sonstigen personenbezogenen Daten erleichtert werden. Denn diese Abgrenzung war in der Vergangenheit mit Unsicherheit behaftet, z.B. im Hinblick auf die Einordnung von Lichtbildern (Ein Lichtbild ist kein biometrisches Datum, kann aber zu einem biometrischen Datum werden, wenn ein Gesichtserkennungs-Algorithmus zum Einsatz kommt).

b. Rechtssicherheit bei der Verarbeitung von besonderen Kategorien personenbezogener Daten zum Zwecke der Vertragserfüllung in bestimmten Konstellationen

Der Schutz der besonderen Kategorien personenbezogener Daten des Art. 9 Abs. 1 DSGVO ist angesichts der erheblichen Risiken für die Rechte und Freiheiten betroffener Personen, die mit der Verarbeitung einhergehen, ein hohes und nicht anzutastendes Gut der DSGVO. Um diesen Schutz insbesondere bei der Erledigung alltäglicher Geschäfte zum Erwerb medizinischer Produkte und Unterstützungen, wie z.B. Sehhilfen, oder der Eingehung und Durchführung eines Versicherungsverhältnisses, im Rahmen dessen z.B. Gesundheitsdaten verarbeitet werden, nicht zu unterlaufen, aber gleichzeitig die Teilhabe der betroffenen Person nicht einzuschränken, sollte in Art. 9 Abs. 2 DSGVO eine Regelung eingeführt werden, die ergänzend zu Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO die Verarbeitung besonderer Kategorien personenbezogener Daten für bestimmte regelmäßige Vertragsszenarien, die eine Verarbeitung von besonderen Kategorien erfordern, mit enger Zweckbindung legitimiert. Eine solche Rechtsgrundlage würde den Verantwortlichen die Verarbeitung besonderer Kategorien personenbezogener Daten erleichtern, ohne das Risiko, das mit dieser Verarbeitung einhergeht, außer Acht zu lassen.

c. Ausgleichende Modifikation des Auskunftsrechts

Das Auskunftsrecht gem. Art. 15 DSGVO ist ein elementarer Bestandteil des Grundrechts auf Schutz personenbezogener Daten gem. Art. 8 Abs. 2 S. 2 EuGRCh. Vor diesem Hintergrund sollte es nicht insgesamt verengt werden, indem der Anwendungsbereich eingegrenzt wird. Diese Verengung wurde bereits durch den Europäischen Datenschutzausschuss im Rahmen der Stellungnahme zum Digital Omnibus hinsichtlich der beabsichtigten Änderungen des Art. 12 Abs. 5 DSGVO kritisiert. Trotzdem sollte das Auskunftsrecht nicht dazu führen, dass Rechte und Freiheiten Dritter in unverhältnismäßiger Weise beeinträchtigt werden. Dies ist jedoch keine Frage der Voraussetzung des Auskunftsrechts, sondern eine der Reichweite.

Dieser Vorbehalt des Art. 15 Abs. 4 wird in der aktuellen Fassung der Vorschrift nur im Hinblick auf Art. 15 Abs. 3 DSGVO geregelt, sollte jedoch für das gesamte Auskunftsrecht gelten und so den Verantwortlichen die Möglichkeit geben, die Auskunft auch zur Herkunft oder der Empfänger in begründeten Einzelfällen einzuschränken.

So kann ein wirksamer Ausgleich zwischen dem Recht der betroffenen Person und dem Schutz anderer Personen und Institutionen erreicht werden.

d. Bürokratieabbau durch Abschaffung der Pflicht zur Mitteilung der Kontaktdaten von Datenschutzbeauftragten an die Aufsichtsbehörden

Eine Entlastung der Wirtschaft und der Aufsichtsbehörden sowie ein spürbarer Bürokratieabbau lassen sich bereits durch eine minimalinvasive Anpassung des Art. 37 Abs. 7 DSGVO erreichen, indem die Pflicht zur Mitteilung der Kontaktdaten von benannten Datenschutzbeauftragten an die Aufsichtsbehörde gestrichen wird. Es hat sich in der Praxis gezeigt, dass die Veröffentlichung der Kontaktdaten der Datenschutzbeauftragten und die Auskunftspflicht der Verantwortlichen im Bedarfsfall für die Zwecke der Aufsicht ausreichend sind. Eine zusätzliche Mitteilung der Kontaktdaten gegenüber der Aufsichtsbehörde ist demgegenüber nicht erforderlich und das Bedürfnis einer entsprechenden gesetzlich verankerten Pflicht mithin nicht gegeben.

e. Effektivierung der Funktion der Aufsichtsbehörden

Die Datenschutzaufsichtsbehörden haben die Funktion, die Anwendung der DSGVO zu überwachen, um die Grundrechte und Grundfreiheiten der betroffenen Personen bei der Verarbeitung zu schützen und dadurch auch den freien Datenverkehr zu erleichtern. Zur Erfüllung dieser Funktion haben die Datenschutzaufsichtsbehörden gem. Art. 57 DSGVO verschiedene Aufgaben, die neben der Überwachung, Kontrolle und Bearbeitung von Beschwerden auch die Beratung und Information als proaktive Elemente der Datenschutzaufsicht sowie die Kooperation untereinander und mit anderen betreffen. Letztere hat aufgrund der Pflicht zur einheitlichen Anwendung und vor dem Hintergrund der durch die Digitalstrategie der EU hinzutretenden Kooperationserfordernisse mit weiteren Aufsichtsbehörden an Bedeutung gewonnen.

Die Beschwerdebearbeitung ist ein wichtiger Bestandteil dieser Aufgaben der Datenschutzaufsichtsbehörden, da darin deren Auftrag zum Ausdruck kommt, den betroffenen Personen zu ihrem Datenschutzgrundrecht zu verhelfen. Die Datenschutzaufsichtsbehörden in der gesamten EU sehen sich jedoch einer massiv steigenden Zahl von Beschwerden betroffener Personen gegenüber.

Aufgrund der engen Voraussetzungen gem. Art. 57 DSGVO sind die Datenschutzaufsichtsbehörden verpflichtet, sich mit Beschwerden betroffener Personen zu befassen und dabei den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen. Diese Bearbeitung muss mit gebotener Sorgfalt erfolgen. Mehr Flexibilität würde es den Datenschutzaufsichtsbehörden dagegen ermöglichen, die begrenzten Ressourcen interessengerecht einzusetzen.

Vor diesem Hintergrund schlägt die DSK vor, den Datenschutzaufsichtsbehörden mehr Spielraum hinsichtlich des Ob und des Wie der Bearbeitung zu geben und die betroffenen Personen mehr in die Pflicht zu nehmen, wenn insbesondere Beschwerden keine grundsätzliche Bedeutung haben und Betroffenen eigene Mittel zur Wahrnehmung ihrer Interessen zur Verfügung stehen.

Zudem sollte bei einer Verschärfung des Missbrauchstatbestands des Art. 12 Abs. 5 DSGVO der Art. 57 Abs. 4 DSGVO im Gleichlauf angepasst werden, wie es bereits in der Stellungnahme des Europäischen Datenschutzausschusses zum Digital Omnibus empfohlen wird.

3. Verantwortlichkeit von Herstellern und Anbietern

Die DSK hält es für erforderlich, die Überprüfung der Digitalrechtsakte und ihres Zusammenspiels mit der DSGVO zu nutzen, um das Konzept der datenschutzrechtlichen Verantwortlichkeit fortzuentwickeln und an das anderer Digitalrechtsakte wie den Cyber Resilience Act (CRA) oder die KI-Verordnung anzugleichen. Dies würde zu einer erheblichen Entlastung der Anwender, insbesondere

kleinerer und mittlerer Unternehmen (KMU), und einer substanziellen Vereinfachung für sie führen, wenn sie personenbezogene Daten verarbeiten.

Die DSGVO stellt bereits heute mit Data Protection by Design and by Default (Art. 25 DSGVO) Grundsätze auf, die sich in der Sache an Hersteller, Importeure und Anbieter richten, nimmt aber nicht diese, sondern ausschließlich die Anwender von Hard- und Software datenschutzrechtlich in die Pflicht. Anders als CRA und KI-Verordnung konzentriert die DSGVO damit die Erfüllung datenschutzrechtlicher Anforderungen am Ende und nicht am Beginn der Entwicklungs- und Wertschöpfungskette. Sie belastet damit insbesondere KMU in nicht unerheblichem Umfang mit Fragestellungen und Anforderungen, deren sachgerechte Bewältigung effektiver auf vorgelagerten Ebenen der Anbieter und Hersteller (bzw. Entwickler) erreichbar wäre.

Die Einbeziehung der Anbieter bzw. Hersteller von Hard- und Software in das etablierte System datenschutzrechtlicher Pflichten würde daher die Verantwortung dorthin verlagern, wo die Entscheidungen über grundsätzliche Weichenstellungen in Systemen getroffen werden. Gleichzeitig würden die Anwender von IT-Produkten, die keinen Einfluss auf das Produktdesign haben, die Haftungsrisiken nicht alleine tragen.

Eine derartige Ergänzung der DSGVO kann deshalb einen substantiellen Beitrag dazu leisten, die Anwendung der DSGVO insbesondere für KMU zu vereinfachen und mit den übrigen Digitalrechtsakten zu harmonisieren, indem die Hersteller in ähnlicher Weise frühzeitig in die Pflicht genommen werden, grundlegende Regulierungsziele des Unionsrechts mit zu verwirklichen, wenn sie ihre Produkte und Dienste im Geltungsbereich der DSGVO anbieten. Die Ergänzung erhöht zudem die Rechtssicherheit für Anwender, denen durch die künftig von Herstellern und Anbietern bereitzustellenden Konformitätserklärungen die Erfüllung ihrer Rechenschaftspflicht erleichtert wird.

Die DSK schlägt daher vor, die bisher im CRA enthaltenen Verpflichtungen von Herstellern, in der Konzeption, Entwicklung und Herstellung von IT-Produkten im Hinblick auf die Gewährleistung der IT-Schutzziele und die Datenminimierung wirksame Prozesse zu etablieren, fortzuentwickeln und im Rahmen der DSGVO auszubauen. Um ein kohärentes Konzept für die Herstellerhaftung zu erreichen, sollten über diese Sicherheitsbelange hinaus alle Anforderungen der Datenschutzgrundsätze (Art. 5 Abs. 1 DSGVO) umfassend auch für Hersteller und Anbieter gelten. Die Anwender würden dadurch nachhaltig unterstützt, ihrer Rechenschaftspflicht nachkommen zu können. In diesem Sinne sollten die Hersteller in möglichst standardisierter Form Informationen insbesondere für das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) und für die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) bereitstellen, welche die Verantwortlichen nur noch für ihre jeweilige Verarbeitungssituation anpassen müssten.

In einer weiteren Stufe kann zudem ein an datenschutzrechtliche Zertifizierungen angelehntes Modell auch für Produktzertifizierungen entwickelt werden.

Ergänzend sollten die bisher alleine an den Verantwortlichen gerichteten Verpflichtungen zu den datenschutzfreundlichen Voreinstellungen (Art. 25 DSGVO) auch auf Auftragsverarbeiter erstreckt werden, um neben Herstellern auch deren Rolle bei der Gewährleistung des Datenschutzes durch Technikgestaltung hervorzuheben und Verantwortliche möglichst umfassend von Aufgaben zu entlasten, die an anderer Stelle effektiver geklärt werden können.

4. Kinder- und Jugendschutz

Kinder sind besonders schutzbedürftig – auch im digitalen Raum. Bereits am Tag der Kinderrechte, dem 20. November 2025, hat die DSK einen Zehn-Punkte-Plan zur Verbesserung des gesetzlichen Datenschutzes von Kindern verabschiedet. Darin fordert die DSK unter anderem ein Verbot von personalisierter Werbung und kindgerechte Voreinstellungen in Sozialen Netzwerken.

Vielen Kindern, aber auch Erziehungsberechtigten, ist nicht bewusst, dass aus ihren Angaben und ihrem Verhalten neue Daten entstehen, die ihr Selbstbild, ihre sozialen Beziehungen und ihr Weltverständnis prägen können. Die Datenschutz-Grundverordnung (DSGVO) trägt der besonderen Schutz- und Fürsorgepflicht gegenüber Kindern bereits in vielen Punkten Rechnung – aber nicht in allen. Deshalb hat die DSK zehn Vorschläge erarbeitet, um die DSGVO gezielt um Regelungen zum Schutz von Kindern zu ergänzen. Es geht vor allem um Datenverarbeitungen, in denen die besondere Schutzbedürftigkeit von Kindern in der Praxis nicht immer ausreichend beachtet wird.

Die DSK schlägt zehn konkrete Änderungen der DSGVO vor:

1.Vereinbarkeit eines neuen Verarbeitungszwecks: Wenn die Daten eines Kindes für einen neuen Zweck verwendet werden sollen, soll bei der Prüfung der Schutz von Kinderrechten ebenso stark gewichtet werden wie bei der Ersterhebung der Daten.

2. Keine Einwilligung in Profiling und Werbezwecke: Werbung auf der Grundlage von Persönlichkeits- oder Nutzerprofilen von Kindern sollte – wie schon im Digital Services Act und in der Verordnung über die Transparenz und das Targeting politischer Werbung – generell verboten sein.

3. Keine Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO: Kinder sollen, anders als Erwachsene, grundsätzlich keine besonders schützenswerten Daten wie Angaben zu ihrer Gesundheit, Religion oder politischen Meinung freigeben können.

4. Datenverarbeitung für Präventions- und Beratungsdienste sowie ärztliche Untersuchungen und Heileingriffe: Kinder sollen Beratungs- und Gesundheitsangebote ab einem bestimmten Alter vertraulich nutzen können, ohne dass ihre Eltern automatisch informiert werden.

5. Widerspruch zur Verarbeitung von Kindesdaten: Beim Widerspruchsrecht soll der Verantwortliche im Sinne der Betroffenen berücksichtigen, dass Daten aus der Kindheit stammen.

6. Keine Einwilligung in automatisierte Entscheidungen: Kinder sollen nicht Verfahren unterworfen werden, bei denen Entscheidungen vollständig automatisiert getroffen werden.

7. Datenschutzgerechte Systemgestaltung: Gerade Soziale Netzwerke und andere datengetriebene Plattformen sollen den Schutz von Kindern bereits bei der technischen Gestaltung sicherstellen.

8. Datenschutzfreundliche Voreinstellung: Voreinstellungen zum Datenschutz, etwa in Sozialen Netzwerken, sollen auch für Kinder verständlich sein und sie konsequent vor Risiken schützen.

9. Meldung von Datenschutzverletzungen: Bei der Frage, ob eine Datenpanne der Aufsichtsbehörde zu melden ist, sollen auch die Risiken für Kinder berücksichtigt werden.

10. Datenschutzfolgenabschätzung: Bei Datenschutzfolgenabschätzung sollen die besonderen Risiken und Schutzbedürfnisse von Kindern angemessen berücksichtigt werden.

5. Sicherstellung der Rechte von Betroffenen beim Einsatz von KI

Bei der Verarbeitung personenbezogener Daten durch KI-Systeme sieht die DSK Bedarf für Reformen, die über die bisherigen Vorschläge der EU-Kommission hinausgehen. Die DSK fordert, spezifische

Rechtsgrundlagen für Entwicklung, Training und Betrieb von KI-Modellen und KI-Systemen gesetzlich festzulegen.

Zudem fordert die DSK den europäischen Gesetzgeber auf, die Rechte von betroffenen Personen beim KI-Einsatz stärker zu berücksichtigen und insbesondere die Informations- und Auskunftsrechte im Hinblick auf den Einsatz von KI zur Verarbeitung von personenbezogenen Daten zu stärken. Generell muss solchen KI-Systemen der Vorzug gegeben werden, die Betroffenenrechte gewährleisten. Für solche KI-Systeme, in denen Betroffenenrechte nur mit unverhältnismäßigem Aufwand umgesetzt werden können, sollen funktionsäquivalente bzw. kompensatorische Schutzmaßnahmen vorgesehen werden.

Die Durchsetzung individueller Rechte der betroffenen Personen aus der DSGVO erweist sich aufgrund des momentanen Standes der Technik in manchen Fällen als schwierig, wenn bei der Datenverarbeitung KI, die sich überwiegend durch probabilistische Verarbeitungen auszeichnet, eingesetzt wird. Ziel muss es aber sein, auch dann die Gewährleistung der Betroffenenrechte sicherzustellen. Anbieter und Betreiber von KI-Systemen haben sich daher insbesondere mit steigendem Risiko für die Rechte der betroffenen Personen am Stand der Wissenschaft und Technik zu orientieren und alle angemessenen Maßnahmen zu ergreifen, um die Schutzfunktion der Rechte der Betroffenen zu erfüllen.

Soweit Betroffenenrechte technisch nicht oder nur mit unverhältnismäßigem Aufwand umgesetzt werden können, sollen funktionsäquivalente bzw. kompensatorische Schutzmaßnahmen gesetzlich vorgesehen werden.