

Deutsche Sozialversicherung
Europavertretung
Rue d'Arlon 50
1000 Brüssel
Belgien

Tel: +32 2 282 05-50
info@dsv-europa.de
www.dsv-europa.de
Transparenzregister-Nr.:
917393784-81



Deutsche Sozialversicherung
Europavertretung | DSV

Stellungnahme der Deutschen Sozialversicherung vom 23. Februar 2026

Vorschläge der Europäischen Kommission zu
Omnibusvorschriften für den Digitalbereich

I. Vorbemerkung

Die Deutsche Sozialversicherung (DSV) begrüßt die Initiative der Europäischen Kommission, mit einem Digital-Omnibus die Vielzahl bestehender Rechtsakte im Digitalbereich zu vereinfachen und zu harmonisieren. Die Sozialversicherungsträger stehen mit eigener IT-Infrastruktur, datenintensiven Verwaltungsprozessen und der perspektivischen Nutzung von Systemen künstlicher Intelligenz (KI) vor der Aufgabe, die Anforderungen der einschlägigen Gesetzgebung frühzeitig und nachhaltig in ihre Governance- und Compliance-Strukturen zu integrieren. Eine klare, kohärente und nutzerfreundliche Regulierung ist daher entscheidend, um digitale Innovationen rechtssicher einzusetzen und gleichzeitig die hohen Standards des Datenschutzes und der sozialen Sicherheit in Europa zu gewährleisten.

Vor diesem Hintergrund erkennt die DSV an, dass die Verordnungsvorschläge wichtige Schritte zur Vereinheitlichung digitaler Regelwerke vorsehen – etwa eine Verschiebung der Fristen für Hochrisiko-KI, einheitliche Vorgaben für Datenschutzfolgeabschätzungen, die Modernisierung der Cookie-Regeln oder die geplante Bündelung von Meldestrukturen. Solche Maßnahmen können die Umsetzung vereinfachen und die Rechtssicherheit erhöhen.

Zugleich weist die DSV jedoch auf den besonderen Schutz hin, der Sozialdaten zukommen muss. Einige der vorgeschlagenen Änderungen im Datenschutzrecht betreffen zentrale Begriffsdefinitionen und könnten auch den Sozialdatenschutz berühren. Für die Sozialversicherung ist es entscheidend, dass die hohen Schutzstandards für Sozialdaten gewahrt bleiben und neue Regelungen nicht zu Rechtsunsicherheiten oder einer Absenkung des etablierten Schutzniveaus führen.

II. Stellungnahme

1 _ Künstliche Intelligenz

Die DSV unterstützt die Zielsetzung des europäischen KI-Rechtsrahmens, Innovation zu ermöglichen und gleichzeitig Grundrechte und europäische Werte zu schützen. Für die Träger der Sozialversicherung ist dabei Rechtssicherheit im Umgang mit der Verordnung (EU) 2024/1689 (KI-Verordnung) sowie Planungssicherheit von zentraler Bedeutung, da Hochrisiko-KI-Systeme insbesondere bei Leistungsentscheidungen und Reha-Steuerung zum Einsatz kommen können. Angesichts der verspäteten Bereitstellung der erforderlichen Normen begrüßt die DSV deshalb das Vorhaben,



den Zeitpunkt des Inkrafttretens der Vorschriften für Hochrisiko-KI nach hinten zu verlegen und an die Verfügbarkeit von Unterstützungsinstrumenten, einschließlich der notwendigen Normen, zu knüpfen. Eine Verlängerung der Umsetzungsfrist darf jedoch zu keiner zwischenzeitlichen Verlagerung des Einsatz- und Verarbeitungsrisikos führen. Dies bedeutet, dass eine Verlängerung der Übergangsfristen nur unter der Bedingung erfolgen kann, dass verbindliche Mindestanforderungen an die Transparenz, die Nachvollziehbarkeit und technisch-organisatorische Maßnahmen sowie risikobasierte Folgenabschätzung für den Einsatz solcher Systeme bereits vorab greifen.

Darüber hinaus begrüßt die DSV die vorgeschlagene Anpassung von Artikel 6 Absatz 4 der KI-Verordnung. Danach entfällt die Registrierungspflicht nach Artikel 49 Absatz 2 für Anbieter von in Anhang III aufgeführten KI-Systemen, wenn diese auf Grundlage einer dokumentierten Bewertung zu dem Ergebnis kommen, dass das System nicht hochriskant ist.

Auch die Ausweitung der Compliance-Instrumente durch mehr regulatorische Reallabore („regulatory sandboxes“), einschließlich einer EU-weiten Sandbox ab 2028, bewertet die DSV positiv. Sie bieten Chancen für frühe Tests von Governance-, Risiko- und Datenschutzanforderungen sowie für Pilotprojekte im Bereich Rehabilitation und Prävention. Reallabore sind damit ein nutzenbringendes Instrument für die zu operationalisierende Umsetzung von KI-Compliance, zum Beispiel das Testen von Human-in-the-Loop, Dokumentation und DSFA/GRFA-Verzahnung. Eine frühzeitige Einbindung der Sozialversicherung ist wünschenswert.

Vor dem Hintergrund der besonderen Schutzbedürftigkeit von Sozialdaten weist die DSV darauf hin, dass die vorgeschlagenen Erleichterungen und abgestuften Pflichten im KI-Rechtsrahmen für kleine und mittlere Unternehmen (KMU) und Start-ups nicht zu einer Schwächung von Transparenz, Nachvollziehbarkeit und Rechenschaftspflichten führen dürfen. Dies gilt insbesondere dann, wenn KI-Systeme von Dritten im Auftrag oder im Umfeld von Sozialversicherungsträgern eingesetzt werden. In Bereichen mit hoher Grundrechtsrelevanz – etwa im Sozial- und Gesundheitswesen – ist es daher aus Sicht der DSV erforderlich, Ausnahmeregelungen für KMU entsprechend einzugrenzen und klarzustellen, dass datenschutzrechtliche Mindeststandards, Risikobewertungen sowie eine hinreichende Dokumentation der Datenverarbeitungsprozesse uneingeschränkt gewährleistet bleiben müssen.

Außerdem hält die DSV eine klare Abgrenzung zwischen gemeinwohlorientiertem KI-Einsatz im öffentlichen Sektor und kommerziellen Profiling-Praktiken mit Blick auf Zweckbindung, Transparenz, Entscheidungsrelevanz und Möglichkeit des

Widerspruchs bzw. der Korrektur für notwendig. Gerade bei explorativen Verfahren des maschinellen Lernens sollten technisch unvermeidbare Zwischenschritte – etwa die Erzeugung von Scores oder Wahrscheinlichkeiten auf der Ebene einzelner Entitäten – nicht vorschnell als Profiling gewertet werden, um Rechtssicherheit zu schaffen und Innovation nicht zu behindern.

2 _ Daten-Governance, Datenzugang und Datenschutz

Die Sozialversicherungsträger stellen nicht nur Sozialdaten für die Forschung bereit, sondern benötigen auch selbst einen verlässlichen Datenzugang, um eine durchgängige Versorgung sicherzustellen. Die durch den Digital-Omnibus angestrebte Vereinfachung und Harmonisierung der Vorschriften zu Daten-Governance, Datenzugang und Datenschutz kann grundsätzlich dazu beitragen, den verantwortungsvollen Einsatz von Daten für Forschung, Prävention und Versorgungssteuerung zu verbessern und die Umsetzung großer Digitalprojekte zu erleichtern. Aus Sicht der Sozialversicherungsträger besteht daher ein hohes Interesse daran, dass qualitativ hochwertige und sichere Datenräume geschaffen werden, in denen insbesondere pseudonymisierte oder anonymisierte Sozialdaten zum Nutzen der Versicherten verwendet werden können.

Gleichzeitig muss jede Öffnung oder Standardisierung von Datenzugängen und Datenräumen von robusten und effektiven Schutzmechanismen begleitet sein. Hierzu können beispielsweise strenge Zweckbindung, abgestufte Zugriffskonzepte, Pseudonymisierung bzw. Anonymisierung, Prüf- und Freigabeverfahren sowie eine klare Governance-Struktur mit definierter Verantwortlichkeit gehören.

Vor diesem Hintergrund unterstützt die DSV die Zusammenführung bestehender Vorschriften in die Verordnung (EU) 2023/2854 (Data Act) beziehungsweise die Verordnung (EU) 2016/679 (DSGVO), um die Rechtssicherheit und Umsetzbarkeit zu erhöhen.

Außerdem begrüßt die DSV das Vorhaben, mit Leitlinien zu Mustervertragsklauseln für den Datenzugang und die Datennutzung sowie Standardvertragsklauseln für Cloud-Computing-Verträge die Umsetzung des Data Act zu unterstützen (Artikel 19 Data Act). Solche Mustervertragsklauseln sind für die Sozialversicherung wichtig mit Blick auf Kooperationen mit Forschungseinrichtungen und Kliniken, insbesondere im Bereich von Reha-Daten.

Auch mit Blick auf die Datenschutzfolgeabschätzungen (Artikel 35 DSGVO) begrüßt die DSV die vorgeschlagenen Änderungen, wonach der Europäische

Datenschutzausschuss einheitliche Listen der Verarbeitungsvorgänge erstellt, für die eine Datenschutzfolgeabschätzung erforderlich ist beziehungsweise nicht erforderlich ist, und darüber hinaus eine gemeinsame Methodik sowie ein einheitliches Template für deren Durchführung erarbeitet.

Ebenso wird der vorgeschlagene Modernisierungsvorschlag zu den Cookie-Regeln positiv bewertet (Artikel 88a und 88b DSGVO). So soll es Nutzerinnen und Nutzern möglich werden, ihre Einwilligung mit einem Klick zu erteilen und ihre Cookie-Einstellungen zentral in den Präferenzen des Browsers oder des Betriebssystems zu speichern. Dies trägt dazu bei, Rechtsklarheit in Bezug auf den rechtmäßigen Zugang zu und die Verarbeitung von Daten zu schaffen, den administrativen Aufwand bei Unternehmen und Betroffenen zu mindern und letztlich die Nutzerfreundlichkeit digitaler Angebote – zum Beispiel webbasierte Plattformen im Bereich Rehabilitation oder Nachsorge – zu verbessern.

Hinsichtlich des vorgesehenen Umgangs mit Datenschutzvorfällen (Artikel 33 DSGVO) unterstützt die DSV die Einführung einer zentralen Meldestelle bei der European Union Agency for Cybersecurity (ENISA). In Deutschland gibt es seit langem den Bedarf an einer Vereinheitlichung der Meldestrukturen, dem zuletzt durch die aktuell im Gesetzgebungsprozess befindliche Streichung des § 83a SGB X – also die zusätzliche Meldung von Datenschutzvorfällen mit Sozialdaten an das Bundesamt für Soziale Sicherung (BAS) – Rechnung getragen wurde. Die geplante Meldestelle soll dem Gesetzesvorschlag nach ebenso für andere meldepflichtige Vorfälle nach verschiedenen Rechtsakten gelten, unter anderem in den Bereichen Cybersicherheit und elektronische Identifikation. Dies kann dazu beitragen, den Aufwand für öffentliche Einrichtungen zu reduzieren, Doppelmeldungen zu vermeiden und einen klaren, einheitlichen Meldeprozess sicherzustellen. Aus Sicht der DSV ist die ENISA dafür auch die passende Behörde. Gleichzeitig ist zu berücksichtigen, dass Fragen der Datenschutzaufsicht in Deutschland dem Föderalismusprinzip unterliegen und daher nur begrenzt durch EU-Gesetzgebung vereinheitlicht werden können. Vor diesem Hintergrund bedarf es einer Klarstellung, wie die zentrale Meldestelle mit den zuständigen nationalen Aufsichtsbehörden zusammenarbeiten soll.

Auch die vorgeschlagene Verlängerung der Meldefrist nach der DSGVO ist zu begrüßen, denn oft reichen die aktuell gegebenen 72 Stunden nicht aus, um den Sachverhalt zu rekonstruieren und eine valide Basis für die Risikoeinschätzung zu haben. Dabei sollte noch konkretisiert werden, ob Wochenende und Feiertage davon ausgenommen sind. Aus Sicht der DSV sollte zudem geprüft werden, inwieweit die vorgeschlagene Verlängerung der Meldefristen mit den einschlägigen Meldepflichten aus anderen EU-Rechtsakten – insbesondere der Richtlinie (EU) 2022/2555 (NIS-2-

Richtlinie) und der Richtlinie (EU) 2022/2557 (CER-Richtlinie) – kohärent ausgestaltet werden kann. Eine stärker abgestimmte Fristenlogik würde die Praxis entlasten und die angestrebte Vereinfachung durch die zentrale Meldestelle sinnvoll ergänzen.

Mit Blick auf weitere vorgeschlagene Änderungen der DSGVO weist die DSV darauf hin, dass jegliche Anpassungen der DSGVO konform zu Artikel 8 der Charta der Grundrechte der EU erfolgen müssen. Die auftretenden Fragen – etwa in Bezug auf die Definition personenbezogener Daten (Artikel 4 und Artikel 41a DSGVO), die Rechtsgrundlagen für die Verarbeitung mit KI (Artikel 9 und Artikel 6 DSGVO) sowie den Umfang von Betroffenenrechten (Artikel 33 und Artikel 34 DSGVO) – müssen in möglichst enger Zusammenarbeit mit dem Europäischen Datenschutzausschuss geklärt werden.

So mahnt die DSV etwa mit Blick auf die Verarbeitung besonderer Kategorien personenbezogener Daten mit KI (Artikel 9 DSGVO) zur Vorsicht. Der vorgeschlagene neue Artikel 9 Absatz 2 Buchstabe k DSGVO sieht einen Erlaubnistatbestand vor, der die Verarbeitung besonders schutzwürdiger Daten mit KI regeln soll. Diese Erlaubnis wäre jedoch an die verwendete Technologie geknüpft und nicht – wie bislang – an den Zweck der Verarbeitung. Dies hätte zur Folge, dass die Verarbeitung sensibler Gesundheitsdaten mit herkömmlichen Technologien, etwa Datenbanken, verboten wäre, während sie unter Einsatz von KI erlaubt wäre. Damit würde das bislang technikneutrale Konzept der DSGVO verlassen, obwohl KI-gestützte Verarbeitungen auch heute schon zu rechtmäßigen Zwecken möglich sind. Den Regelungsentwurf zu Artikel 9 Absatz 2 Buchstabe k DSGVO lehnt die DSV deshalb in der vorliegenden Form ab.

Unabhängig von den vorgeschlagenen Einzeländerungen im Gesetzestext weist die DSV darauf hin, dass mit Blick auf die praktische Gewährleistung und Umsetzung von Anforderungen der DSGVO im Sozialversicherungskontext auch eine Fortentwicklung der datenschutzrechtlichen Verantwortlichkeit von besonderer Bedeutung wäre. So sollten Unternehmen, die IT-Dienstleistungen anbieten und personenbezogene Daten verarbeiten, stärker verpflichtet werden, die Grundsätze des Datenschutzes bereits bei der Konzeption ihrer Dienste zu berücksichtigen. Dies gilt insbesondere für Auftragsverarbeiter, die ihre Dienste von vornherein datenschutzkonform ausgestalten sollten.

3 _ Elektronische Identifikationsdienste

Die DSV unterstützt das Ziel, mit der europäischen digitalen Identität (EUDI) und der EUDI-Wallet die Grundlage für sichere, interoperable und grenzüberschreitende Identifikationsverfahren zu schaffen. Voraussetzung ist jedoch, dass die europäischen Lösungen kompatibel mit bestehenden Infrastrukturen sind, um Doppelstrukturen und unnötige Schnittstellenentwicklungen zu vermeiden. Dies gilt auch mit Blick auf die European Business Wallet (EBW).

Vor diesem Hintergrund ist die zügige und kohärente Umsetzung des europäischen Rahmens für eine digitale Identität (Verordnung (EU) 2024/1183 – Verordnung eIDAS-Verordnung) entscheidend. Dabei muss gewährleistet sein, dass neben der primären Identität auch ergänzende Nachweise durch einheitliche europäische Standards geregelt werden, um ihre Kompatibilität sicherzustellen. Ebenso sollte vorgesehen werden, dass Änderungen persönlicher Daten, wie Namens- oder Geschlechtsänderungen, automatisch in allen relevanten Nachweisen aktualisiert werden können, um nationale Einzelprozesse zu vermeiden und die grenzüberschreitende Interoperabilität zu stärken. Insgesamt sollten bestehende nationale Rechtsgrundlagen sowie etablierte Verfahren der Sozialversicherung berücksichtigt werden, um unverhältnismäßige administrative oder organisatorische Belastungen zu vermeiden.

Die Authentifizierung selbst sollte dabei klaren Prinzipien folgen. Die DSV begrüßt, dass die eIDAS-Verordnung in diesem Zusammenhang den Grundsatz der Datensparsamkeit vorsieht. Demnach müssen nutzende Stellen vorab festlegen, welche Identifizierungsdaten für den jeweiligen Zweck erforderlich sind, und dürfen nur diese aus dem Identifizierungsmittel auslesen und verarbeiten. Darüber hinaus sollte gewährleistet werden, dass neben dem Standardweg der elektronischen Identifizierung weitere sichere Verfahren zur Verfügung stehen, sodass Nutzerinnen und Nutzer flexibel das für sie passende Mittel wählen können.

Über uns

Die Deutsche Rentenversicherung Bund (DRV Bund), die Deutsche Gesetzliche Unfallversicherung (DGUV), der GKV-Spitzenverband, die Verbände der gesetzlichen Kranken- und Pflegekassen auf Bundesebene sowie die Sozialversicherung für Landwirtschaft, Forsten und Gartenbau (SVLFG) haben sich mit Blick auf ihre gemeinsamen europapolitischen Interessen zur „Deutschen Sozialversicherung Arbeitsgemeinschaft Europa e.V.“ zusammengeschlossen. Der Verein vertritt die Interessen seiner Mitglieder gegenüber den Organen der Europäischen Union sowie anderen europäischen Institutionen und berät die relevanten Akteure im Rahmen aktueller Gesetzgebungsvorhaben und Initiativen. Die Kranken- und Pflegeversicherung mit 75 Millionen Versicherten, die Rentenversicherung mit 57 Millionen Versicherten und die Unfallversicherung mit mehr als 70 Millionen Versicherten in 5,2 Millionen Mitgliedsunternehmen bieten als Teil eines gesetzlichen Versicherungssystems den Bürgerinnen und Bürgern in Deutschland wirksamen Schutz vor den Folgen großer Lebensrisiken.