20.11.2025

„Digitaler Omnibus: EU-Kommission schlägt überarbeitete Digitalverordnungen vor"

Prof. Dr. Dennis-Kenji Kipker

Research Director, cyberintelligence.institute, Frankfurt am Main, und Professor für IT-Sicherheitsrecht, Hochschule Bremen

Kernpunkte der Überarbeitung

„Der ‚Digitale Omnibus' strebt eine Zusammenführung und Vereinheitlichung verschiedener Digitalgesetze an. Insbesondere sollen Open Data Directive, Free-Flow-of-non-personal-Data-Verordnung, Data Governance Act und Data Act in einem überarbeiteten Data Act gebündelt werden. Ziel ist es, redundante Regelungen zu reduzieren, Compliance-Aufwand zu verringern und insbesondere für kleine und mittlere Unternehmen die Umsetzung digitaler Vorschriften zu erleichtern."

„Dabei wird allerdings die Rechtsgrundlage für die Verarbeitung personenbezogener Daten ausgeweitet. Der Entwurf sieht vor, dass das sogenannte ‚berechtigte Interesse' gemäß Artikel 6 Datenschutz-Grundverordnung (DSGVO) künftig auch für Online-Tracking, Cookies und das Training von Modellen künstlicher Intelligenz (KI) mit personenbezogenen Daten ausreicht. Dies markiert eine Abweichung von der bisherigen Praxis, die in vielen Fällen die ausdrückliche Einwilligung der Betroffenen voraussetzt."

„Außerdem wird die Definition sensibler personenbezogener Daten nach Artikel 9 DSGVO enger gefasst. Nur noch direkt offen gelegte Informationen zu Gesundheit oder sexueller Orientierung unterliegen dem erhöhten Schutz. Daten, aus denen sensible Informationen indirekt abgeleitet werden können, fallen künftig nicht mehr unter das strenge Verarbeitungsverbot. Das bedeutet eine Verschiebung des Schutzniveaus."

Bewertung bestehender Digitalverordnungen

„Die bestehenden Digitalgesetze der Europäischen Union (EU) zeichnen sich durch ein hohes Schutzniveau für personenbezogene Daten und eine klare Betonung von Grundrechten aus. Gleichzeitig sind sie in ihrer Gesamtheit komplex und teilweise uneinheitlich strukturiert. So existieren Überschneidungen zwischen DSGVO, E-Privacy-Richtlinie, Data Governance Act und weiteren Regelwerken. Das erschwert die Rechtsanwendung und kann zu Unsicherheiten bei Unternehmen und Betroffenen führen. Die Zuständigkeiten sind zwar formal geregelt, jedoch in der Praxis oft schwer nachvollziehbar, insbesondere bei grenzüberschreitender Datenverarbeitung und bezüglich Künstlicher Intelligenz."

Chancen und Risiken der Überarbeitung

„Der Digitale Omnibusentwurf hat das Potenzial, die bestehenden Regelwerke in Bezug auf Struktur und Übersichtlichkeit zu verbessern. Durch die Zusammenführung mehrerer Gesetzesakte und die Harmonisierung einzelner Begriffe könnten Redundanzen verringert und die Umsetzungspflichten für Unternehmen transparenter werden. Gleichzeitig besteht das Risiko, dass die angestrebte Vereinfachung zulasten des Datenschutzes und der Grundrechte geht. Die geplanten Lockerungen könnten die klare Schutzlogik der DSGVO untergraben, etwa beim berechtigten Interesse und bei der Definition sensibler Daten. Somit ist die Verbesserung der Übersichtlichkeit nicht automatisch gleichbedeutend mit einer Stärkung des Schutzes für Betroffene."

Risiko für Datenschutz

„Kritiker, die im Entwurf des digitalen Omnibusgesetzes einen Schlag gegen den Datenschutz sehen, argumentieren zu Recht, dass die vorgeschlagenen Änderungen zu einer spürbaren Absenkung des etablierten Schutzniveaus führen könnten. Insbesondere die Ausweitung des ‚berechtigten Interesses' als Rechtsgrundlage für Tracking, Profilbildung und das Training von KI-Modellen birgt das Risiko, zentrale Prinzipien der DSGVO auszuhöhlen: Die DSGVO basiert auf Transparenz, Zweckbindung, Datenminimierung sowie bei sensiblen Daten einem ausdrücklichen Verarbeitungsverbot mit engen Ausnahmen. Die geplanten Lockerungen würden diesen Rahmen erheblich verschieben, indem sie zu einer faktischen Entgrenzung der Datenverarbeitung führen. In Kombination mit der vorgesehenen Reduzierung von Auskunftsrechten gefährden sie somit die informationelle Selbstbestimmung grundlegend."

„Besonders kritisch zu bewerten ist auch die geplante Neudefinition sensibler personenbezogener Daten nach Artikel 9 DSGVO. Der Entwurf beschränkt den besonderen Schutz künftig auf Informationen, die sensible Merkmale unmittelbar offenlegen. Daten, aus denen sich etwa Gesundheitszustand, politische Überzeugungen oder sexuelle Orientierung nur mittelbar erschließen lassen, sollen nicht länger dem erhöhten Schutzniveau unterliegen. Moderne, datengetriebene Modelle ermöglichen die Ableitung sensibler Informationen aus Verhaltensdaten mit hoher Treffsicherheit und ohne großen Aufwand. Angesichts dessen wären Profiling und zielgerichtete Auswertungen persönlicher Gewohnheiten und Präferenzen ohne die strengen Anforderungen des Artikel 9 noch einfacher möglich. Dies birgt das Risiko neuer Formen der Diskriminierung und beeinträchtigt die Privatsphäre in bislang unbekanntem Ausmaß."

Innovation und Datenschutz

„Vertrauen kann nur entstehen, wenn Gesetzgebung und Datenverarbeitung nachvollziehbar, transparent und grundrechtskonform bleiben. Die Behauptung erscheint hingegen verkürzt, Innovation benötige zwingend eine Absenkung von Schutzstandards. Aus wirtschaftlicher Sicht mag es nachvollziehbar erscheinen, dass innovative KI-Modelle große Mengen unterschiedlichster Daten benötigten. Auch ist verständlich, dass Unternehmen Rechtssicherheit und geringere bürokratische Hürden begrüßen. Der wirtschaftliche Innovationsdruck darf jedoch nicht zu einer Schwächung des Rechts auf informationelle Selbstbestimmung führen. Ein innovationsfreundlicher und zugleich grundrechtskonformer Weg wäre vielmehr durch eine datenschutzfreundliche Harmonisierung der Begriffe, klare technische und organisatorische Anforderungen, datensparsame KI-

Trainingsmethoden und robuste Transparenzmechanismen erreichbar, ohne die Substanz der DSGVO anzutasten."

Strategie für eine Datenunion

„Die European Data Union Strategy scheint ambitioniert: Sie will eine kohärente europäische Dateninfrastruktur und sieht den erleichterten Zugang zu hochwertigen Daten für KI-Anwendungen vor. Zugleich will sie aber die digitale Souveränität der EU stärken. Grundsätzlich ist die geplante Sicherung sensibler Datenbestände und die Förderung vertrauenswürdiger, interoperabler Datenräume *(ermöglichen sicheres Teilen und Nutzen von Daten; Anm. d. Red.)*, welche Unternehmen ermöglichen sollen, Daten innerhalb der EU kontrolliert zu nutzen, zunächst positiv zu bewerten. Ebenso erscheint die Betonung auf Pseudonymisierung, Anonymisierung und die Einrichtung sicherer Data Labs generell unterstützenswert, die datenschutzkonforme Verarbeitung ermöglichen und die Kontrolle bei den Datenhaltern belassen sollen."

„Allerdings sieht die Strategie eine massive Ausweitung der Datennutzung vor, wodurch das Prinzip der Datenminimierung potenziell unterlaufen wird. Die geplante Vereinfachung regulatorischer Vorgaben, etwa durch Anpassungen der DSGVO und automatisierte Compliance-Systeme, könnte den Schutz individueller Rechte weiter schwächen, wenn das Prinzip der Zweckbindung nicht konsequent angewendet wird."

Hintergrund zur Datenunion

„Die European Data Union Strategy verfolgt das übergeordnete Ziel, die Wettbewerbsfähigkeit der EU im Zeitalter der künstlichen Intelligenz zu stärken, indem der Zugang zu hochwertigen Daten systematisch ausgeweitet, regulatorische Hürden reduziert und die europäische Datensouveränität gesichert werden. Sie baut auf der bisherigen Datenstrategie auf und adressiert drei zentrale Herausforderungen: die bestehende Datenknappheit, die regulatorische Komplexität und die wachsende internationale Konkurrenz um Daten."

„Inhaltlich umfasst die Strategie den Ausbau interoperabler Datenräume, die Einrichtung von Data Labs für datenschutzkonformes Training von KI-Systemen, die Förderung nachhaltiger Cloud- und Recheninfrastrukturen sowie die Bereitstellung strategischer Datenbestände aus öffentlichen, wissenschaftlichen, kulturellen und sprachlichen Quellen. Ergänzend sollen die rechtlichen Rahmenbedingungen durch Konsolidierung und Vereinfachung bestehender Gesetze, One-Click-Compliance-Systeme und unterstützende Programme insbesondere für kleine und mittlere Unternehmen (KMU) modernisiert werden. International strebt die EU faire und sichere Datenflüsse, den Schutz sensibler Daten und die Stärkung ihrer Position in globalen Datenstrukturen an. Die langfristige Vision ist eine souveräne europäische Datenökonomie, in der Daten effizient, vertrauenswürdig und datenschutzkonform genutzt werden können."

Impressum

Die Science Media Center Germany gGmbH (SMC) liefert Journalisten schnellen Zugang zu Stellungnahmen und Bewertungen von Experten aus der Wissenschaft – vor allem dann, wenn neuartige, ambivalente oder umstrittene Erkenntnisse aus der Wissenschaft Schlagzeilen machen oder wissenschaftliches Wissen helfen kann, aktuelle Ereignisse einzuordnen. Die Gründung geht auf eine Initiative der Wissenschafts-Pressekonferenz e.V. zurück und wurde möglich durch eine Förderzusage der Klaus Tschira Stiftung gGmbH.

Nähere Informationen: **www.sciencemediacenter.de**

Diensteanbieter im Sinne MStV/TMG
Science Media Center Germany gGmbH
Schloss-Wolfsbrunnenweg 33
69118 Heidelberg
Amtsgericht Mannheim
HRB 335493

Redaktionssitz
Science Media Center Germany gGmbH
Rosenstr. 42–44
50678 Köln

Vertretungsberechtigter Geschäftsführer
Volker Stollorz

Verantwortlich für das redaktionelle Angebot (Webmaster) im Sinne des § 18 Abs. 2 MStV
Volker Stollorz