NEWS BOX DATENSCHUTZ

INHALTSVERZEICHNIS

SONDERAUSGABE

13. HAMBURGER DATENSCHUTZTAGE

Dr. Michael Foth, Geschäftsführer IBS data protection services and consulting GmbH

EDITORIAL

Liebe Freunde und Freundinnen des Datenschutzes!

Digitale Technologien prägen zunehmend, wie wir arbeiten, kommunizieren und leben. Gleichzeitig wachsen die Anforderungen an Datenschutz und Datensicherheit, sowohl in technischer als auch in rechtlicher Hinsicht. Umso wichtiger ist es, Datenschutz als ganzheitliches, praxisnahes Konzept zu verstehen und verantwortungsvoll im Alltag zu verankern – ganz im Sinne unseres Konferenzmottos. Unter dem Motto „Sicher navigieren im Datenmeer: Zwischen Innovation und Regulierung den richtigen Kurs setzen" bieten die 13. Hamburger Datenschutztage vom 10. bis 12. Juni 2026 im Lindner Hotel am Michel in Hamburg eine zentrale Plattform für den praxisorientierten Austausch über aktuelle Entwicklungen, Herausforderungen und Chancen rund um Datenschutz, Informationssicherheit und digitale Innovationen.
Auch in diesem Jahr dürfen Sie sich auf ausgewiesene Expertinnen und Experten freuen, die sowohl aktuelle rechtliche Entwicklungen – etwa europäische und internationale Gesetzgebungsprozesse sowie Regulierungsinitiativen wie Data Act, AI Act, Digital Services Act oder DORA – als auch die zunehmend komplexen Anforderungen an Organisationen, Unternehmen und öffentliche Stellen fundiert einordnen. Im Mittelpunkt stehen unter anderem globale Trends im Datenschutzrecht, praktische Umsetzung von Betroffenenrechten, Anonymisierung und Data Governance, künstliche Intelligenz und ihre Regulierung, Cybersecurity, Cyber Resilience Act und internationale Datentransfers, Marketing, Tracking & Cookies sowie Abmahnrisiken, Praxisbeispiele, Best Practices und Lessons Learned für den Unternehmensalltag und vieles mehr.
Die Veranstaltung legt besonderen Wert darauf, nicht nur rechtliche Fragestellungen zu behandeln, sondern auch praxisnahe Lösungen vorzustellen. Im Dialog mit Expertinnen und Experten aus unterschiedlichen Disziplinen haben Sie die Gelegenheit, neue Impulse zu gewinnen, Lösungsansätze zu diskutieren und gemeinsam Strategien für eine datenschutzkonforme und zugleich innovative Zukunft zu entwickeln.
Nutzen Sie die Gelegenheit, Ihr Netzwerk zu erweitern, sich intensiv über aktuelle Herausforderungen und künftige Trends auszutauschen und aktiv zur Gestaltung des Datenschutzes im digitalen Wandel beizutragen.
Wir freuen uns sehr, Sie zu den 13. Hamburger Datenschutztagen begrüßen zu dürfen!

Mit herzlichen Grüßen
Ihr Michael Foth

Foto: praewpailyn, Adobe Stock

DORA, NIS-2, CRA: Warum 2026 das Jahr der IKT-Resilienz wird

2026 entscheidet sich, wer regulatorische Anforderungen strategisch steuert – und wer von ihnen getrieben wird. Viele Unternehmen behandeln Regulatorik noch in Silos: Datenschutz hier, IT-Security dort, Lieferantenmanagement separat. Dieser Ansatz funktioniert mit dem Digital Operational Resilience Act (DORA), der NIS-2-Richtlinie und dem Cyber Resilience Act (CRA) nicht mehr: Resilienz wird prüf- und nachweispflichtig – durchgängig über Systeme, Prozesse und Dienstleister hinweg.

Resilienz ist mehr als „Security" – sie ist Führungsaufgabe

Regulatorisch zählt weniger, ob „irgendwo" Security-Maßnahmen existieren. Entscheidend ist ein belastbares Steuerungsmodell: klare Verantwortlichkeiten, definierte Kontrollen, kontinuierliches Monitoring und ein Management-Reporting, das Risiken transparent macht. Wer lediglich Policies sammelt, riskiert im Audit erhebliche Feststellungen, weil Evidenz, Wirksamkeit und Nachvollziehbarkeit fehlen.

Der blinde Fleck: IKT-Drittrisiken und Dienstleistersteuerung

In der Praxis entstehen viele Risiken an Schnittstellen: Cloud-Services, Managed Services, Support-Zugriffe, Subdienstleister oder Software-Updates. Die neue Regulatorik verlangt hier Transparenz und eine belastbare Steuerung.

Zentrale Fragen sind:

- Welche Services sind geschäftskritisch?
- Welche Abhängigkeiten bestehen tatsächlich?
- Welche belastbaren Nachweise liefern Dienstleister – und wo bestehen Lücken?
- Wie sind Incident-, Exit- oder Provider-Wechsel-Szenarien geregelt?

Vom „Kontrollkatalog" zur wirksamen Umsetzungs-Roadmap

Damit Resilienz nicht zum Bürokratieprojekt wird, braucht es eine klare Umsetzungslogik: Scope präzise definieren, Controls risikobasiert priorisieren, Doppelarbeiten vermeiden (z. B. durch ein integriertes Kontrollsystem für Security und Compliance), und die Nachweisführung so gestalten, dass sie im operativen Alltag mitläuft.
Wie Sie die EU-Vorgaben in ein tragfähiges Resilienz-Betriebsmodell übersetzen – inklusive Rollen, Kontrollen, Evidenzkonzept und Roadmap – erfahren Sie bei Dr. Marlen Hofmann auf den Hamburger Datenschutztagen 2026.

Fachvortrag

Europäische IT-Regulatorik in der Praxis: DORA & Co. verständlich aufbereiten und umsetzen

Referentin: Dr. Marlen Hofmann
Termin: 11.6.2026 – 10:05 Uhr
Weitere Informationen unter: www.datakontext.com/DS-Tage

Foto: photo_grab, Adobe Stock

Copilot & Meeting-Aufzeichnungen: Die drei größten DS-GVO-Stolperfallen im KI-Alltag

Künstliche Intelligenz (KI) schleicht sich selten als strategisches Großprojekt ins Unternehmen. Sie kommt über Funktionen wie Copilot, automatische Zusammenfassungen, Transkripte und Aufzeichnungen. Genau hier entstehen die typischen Datenschutzfehler: intransparente Datenflüsse, riskante Default-Einstellungen und eine Datenschutz-Folgenabschätzung (DSFA), die erst startet, wenn es bereits kritisch wird.

Datenflüsse: Wissen Sie wirklich, wo Ihre Daten landen?

Die zentrale Praxisfrage lautet nicht „Darf KI das?“, sondern: Welche personenbezogenen Daten werden wann verarbeitet – und wohin übermittelt? Bei Meeting-Funktionen betrifft das unmittelbar personenbezogene Daten, vertrauliche Inhalte, ggf. besondere Kategorien sowie interne Geheimhaltungsinteressen.
Ohne Transparenz über Speicherorte, Zugriffskreise, Aufbewahrungsfristen und Exportmöglichkeiten bleibt jede Compliance-Bewertung unvollständig. Wer hier nicht genau hinschaut, argumentiert gegenüber Aufsichtsbehörden und Betroffenen im Blindflug.

Konfigurationen entscheiden über Rechtmäßigkeit

Viele Risiken entstehen nicht durch die Technologie selbst, sondern durch ihre Einstellungen: Aufzeichnung standardmäßig aktiviert, Transkripte automatisch gespeichert, Freigaben zu weit gefasst, Speicherfristen zu lang.
Wer Defaults nicht aktiv steuert, kann die Rechtmäßigkeit der Verarbeitung später kaum belastbar begründen – weder gegenüber Betroffenen noch im Rahmen einer Prüfung.

DSFA als Steuerungsinstrument – nicht als Pflichtübung

Gerade bei KI-Features entfaltet die Datenschutz-Folgenabschätzung ihre Wirkung nur dann, wenn sie frühzeitig erfolgt. Identifizieren Sie systematisch Risikotreiber – etwa Profiling-Effekte, Sekundärnutzung, Drittzugriffe, Trainings- und Prompting-Risiken. Leiten Sie daraus konkrete Maßnahmen ab: klare Rollen, technische und organisatorische Kontrollen, transparente Informationen sowie eine strukturierte Dienstleistereinbindung.
Verstehen Sie die DSFA nicht als Abschlussdokument, sondern als kontinuierlichen Steuerungsprozess im laufenden Betrieb.
Wer Copilot- und Meeting-Funktionen kontrolliert und rechtskonform nutzbar machen will – statt sie vorschnell zu verbieten –, erhält bei den Hamburger Datenschutztagen 2026 konkrete Praxisleitfäden für Datenfluss-Transparenz, Konfig-Checks und eine wirksame DSFA-Umsetzung von Sascha Kremer.

Fachvortrag

Wer braucht die KI-Verordnung, wenn die DS-GVO schon alles blockiert? Praxisfälle zu MS Copilot & Aufzeichnungen

Referent: Sascha Kremer
Termin: 11.6.2026 – 11:15 Uhr
Weitere Informationen unter: www.datakontext.com/DS-Tage

Foto: Generative AI, Adobe Stock

Cookie-Banner 2026: Warum „Consent“ längst ein Technik-Projekt ist

Cookie-Compliance entscheidet sich nicht im Bannertext, sondern im Zusammenspiel von Recht, User Experience (UX) und Technik. Die meisten Cookie-Banner scheitern nicht an der guten Absicht, sondern an der Umsetzung: Zwecke sind unscharf formuliert, Anbieter unvollständig erfasst, der Tag-Manager feuert zu früh – und am Ende passt der Bannertext nicht zur technischen Realität. Genau das prüfen Aufsichtsbehörden inzwischen routinemäßig.

Was Aufsichten als No-Go bewerten

Typische Problemfelder sind:

- keine echte Wahlmöglichkeit (Design oder Klickführung drängen zur Zustimmung);
- zu weit gefasste oder unklare Zweckbeschreibungen;
- fehlende oder unzureichende Nachweise, wann und wofür eine Einwilligung erteilt wurde;
- Standard-Templates, die nicht zur tatsächlichen Tracking-Architektur passen.

Wer diese Punkte nicht sauber adressiert, riskiert Beanstandungen, Beschwerden und Reputationsschäden.

Layer-Logik: Welche Informationen müssen sofort sichtbar sein?

Rechtliche Anforderungen werden in konkrete UX-Entscheidungen übersetzt: Welche Informationen gehören auf die erste Ebene und welche in die Detailansicht? Was muss „auf einen Blick“ verständlich sein – und wie stellen Sie sicher, dass diese Struktur konsistent bleibt, wenn sich Vendoren, Tags oder Tools ändern?

Die technische Realität entscheidet: CMP, Tag-Manager, Analytics

Consent ist nur belastbar, wenn die Technik konsequent folgt: konkrete Trigger-Logik, Blockieren vor Einwilligung, eindeutige Vendor-Zuordnung und dokumentierte Konfigurationen.

Wer Rechtstext, UX und Systemarchitektur nicht zusammen denkt, produziert lediglich „Papier-Consent“ – und der hält weder Prüfungen noch Beschwerden stand.

Wer sein Cookie- und Tracking-Setup so ausrichten möchte, dass Einwilligung, Nutzerführung und technische Umsetzung ineinandergreifen, erhält von Dr. Nina Herbort auf den Hamburger Datenschutztagen 2026 eine fundierte Einordnung – praxisnah und mit Blick auf typische Prüfungslogiken.

Fachvortrag

Update Tracking-Technologien – Was gibt’s Neues zu Cookies & Co.?

Referentin: Dr. Nina Herbort

Termin: 11.6.2026 – 12:00 Uhr

Weitere Informationen unter: www.datakontext.com/DS-Tage

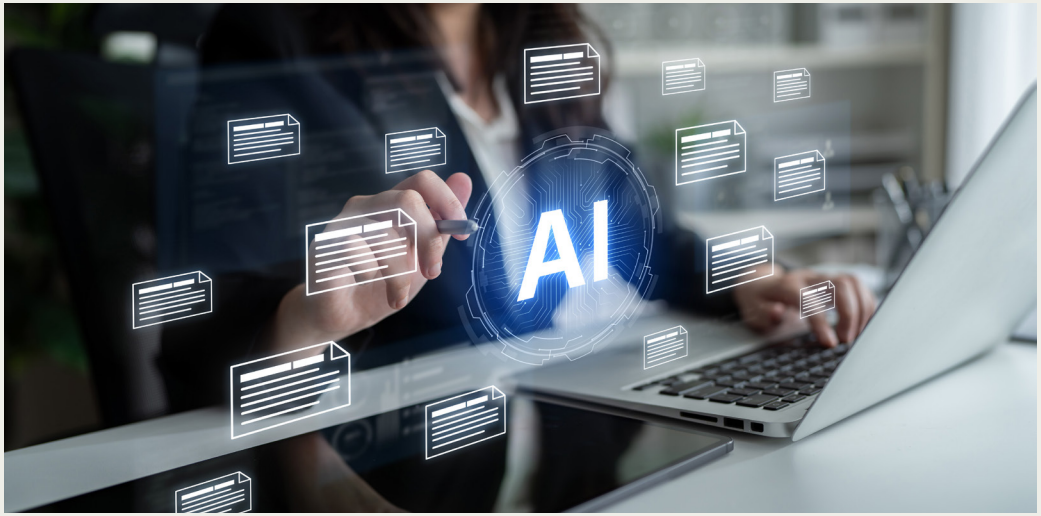

Foto: nfiniteFlow, Adobe Stock

DSK-Orientierungshilfe zu RAG: Leitplanken für den datenschutzkonformen KI-Einsatz

Im Oktober 2025 hat die Datenschutzkonferenz (DSK) die dritte Orientierungshilfe ⭳ zu KI-Systemen seit 2024 veröffentlicht. Bereits erschienen sind Orientierungshilfen zum Einsatz ⭳ sowie zur Entwicklung von KI-Systemen ⭳. Diese dritte Orientierungshilfe wendet sich an Unternehmen und Behörden, die KI-Systeme mit sogenannter Retrieval Augmented Generation (RAG) bereits einsetzen oder einsetzen möchten. Auf 18 Seiten bietet die Orientierungshilfe ⭳ rechtliche und technische Hinweise, wie die Potenziale solcher KI-Systeme genutzt und zugleich die Risiken für die Betroffenen verringert werden können.

RAG ist eine KI-Technologie, bei der große Sprachmodelle durch gezielten Zugriff auf unternehmens- oder behördeneigene Wissensquellen ergänzt werden, um kontextspezifische Antworten zu liefern. Typische Anwendungsbeispiele sind unternehmensinterne Chatbots, die auf aktuelle Geschäftsdaten zugreifen und wissenschaftliche Assistenzsysteme, die Forschungsdatenbanken nutzen. RAG-Systeme sollen die Genauigkeit, Nachvollziehbarkeit und Verlässlichkeit der KI-Ausgaben erhöhen, während die für große Sprachmodelle typischen Halluzinationen und unrichtigen Ausgaben vermindert werden sollen.
Meike Kamp, Berliner Beauftragte für Datenschutz und Informationsfreiheit sowie 2025 DSK-Vorsitzende: „RAG-Systeme können Unternehmen und Behörden dabei unterstützen, die Vorteile moderner KI zu nutzen und zugleich die damit einhergehenden Risiken für die Rechte und Freiheiten von betroffenen Personen zu vermindern. Entscheidend ist jedoch, dass ihr Einsatz von Anfang an datenschutzkonform gestaltet wird. Verantwortliche müssen Transparenz, Zweckbindung und die Wahrung der Betroffenenrechte jederzeit gewährleisten."
RAG-Systeme können eigenständig entwickelt, betrieben und kontrolliert werden und damit Datenschutz-by-Design abbilden. Zudem können sie den Einsatz kleinerer und auch lokal betriebener Modelle ermöglichen, was beispielsweise einen Betrieb des Systems ohne Übermittlung personenbezogener Daten an Dritte wie etwa Hyperscaler ermöglicht. Damit kann die RAG-Methode einen wichtigen Beitrag zur digitalen Souveränität leisten.

RAG-Systeme bringen gleichwohl auch datenschutzrechtliche Risiken mit sich, die Verantwortliche im Blick haben müssen. Sie beseitigen beispielsweise nicht die datenschutzrechtlichen Probleme eines rechtswidrig trainierten Large Language Modells (LLM). Je nach Ausgestaltung können sie aber Teil einer Antwort auf solche unrechtmäßig trainierten Systeme sein. Auch bleibt es herausfordernd, Transparenz, Zweckbindung und die Umsetzung von Betroffenenrechten im gesamten System sicherzustellen. Verantwortliche Stellen, die solche RAG-Systeme einsetzen wollen, müssen die datenschutzrechtlichen Bewertungen der einzelnen Verarbeitungen jeweils individuell vornehmen und ihre technisch-organisatorischen Maßnahmen immer auf dem aktuellen Stand halten.
So wertvoll die Orientierungshilfe als Leitlinie ist, bleibt die eigentliche Herausforderung ihre Umsetzung im Unternehmensalltag. Datenschutzrisiken entstehen dabei meist nicht auf konzeptioneller Ebene, sondern im praktischen Umgang mit KI-Systemen – etwa, wenn sensible Daten unbedacht in Prompts eingegeben werden, ungeeignete Tools genutzt werden oder rechtliche Rahmenbedingungen nicht sauber berücksichtigt sind.
Wie sich solche Risiken in der Praxis erkennen und vermeiden lassen und worauf es beim rechtssicheren Einsatz von KI im Unternehmen tatsächlich ankommt, zeigt Dr. Karsten Kinast auf den Hamburger Datenschutztagen. Anhand konkreter Praxisbeispiele und eines „KI-Crash-Tests“ werden typische Fehlerquellen analysiert und praxistaugliche Lösungsansätze für den sicheren Einsatz von KI im Unternehmensalltag vorgestellt.

Quelle: Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Parallel-Vortrag

KI ohne Datencrash: Produktiver arbeiten – sicher mit Informationen umgehen
Referent: Dr. Karsten Kinast, LL.M.
Termin: 10.6.2026 – 9:30 Uhr bis 17:00 Uhr
Weitere Informationen unter: www.datakontext.com/DS-Tage

Foto: Happy Hues, Adobe Stock

Wettbewerbszentrale veröffentlicht Leitfaden zur KI-Kennzeichnung

Künstliche Intelligenz (KI) durchdringt den Alltag vieler Menschen. Werbetreibende haben mit KI ein effizientes Tool an die Hand bekommen, um schnell und unkompliziert Werbeinhalte zu erzeugen.

Aber welche Regeln gelten, wenn Unternehmen mit KI erzeugte Bilder oder Texte in Werbeanzeigen verwenden? Vor dem vollständigen Inkrafttreten der KI-Verordnung der EU am 2. August 2026 veröffentlicht die Wettbewerbszentrale einen kostenfreien Leitfaden für Unternehmen, der erläutert, worauf es bei der Verwendung KI-generierter Inhalte ankommt. Das PDF finden Sie hier.

Neue Kennzeichnungspflicht für KI-generierte Inhalte

Insbesondere KI-generierte (Werbe-)Bilder, die scheinbar echt wirken, werfen rechtliche Fragen auf. Die KI-Verordnung (KI-VO) verlangt künftig, dass diese als KI-generiert markiert werden, wenn das Bild „echten" Personen oder Objekten „ähnelt". Dann handelt es sich nach der Verordnung um ein sogenanntes „Deepfake".
Wann Medien Personen oder Objekten „ähneln", ist noch unklar. Angesichts der Zielsetzung der Verordnung empfiehlt die Wettbewerbszentrale derzeit sicherheitshalber: Auch KI-Erzeugnisse, die Menschen abstrakt ähneln, ohne eine bestimmte Person nachzubilden, sollten im Zweifel gekennzeichnet werden. Entscheidend ist letztlich, ob ein Bild fälschlich für echt gehalten wird.
Von den angesprochenen Zielgruppen und der Betrachtungssituation hängt ab, welche Inhalte echt wirken könnten. Hierzu werden sich mit der Zeit aus der Rechtsprechungspraxis weitere Anhaltspunkte ergeben.

Leitfaden bietet Orientierung

Doch bis dahin werden KI-Systeme immer häufiger auch professionell genutzt. Die aus der KI-VO folgenden Pflichten führen dabei teilweise zu Verunsicherung.
Der Leitfaden der Wettbewerbszentrale bietet daher eine erste Orientierungshilfe: Anhand von Beispielen erläutert die Zentrale die neue Kennzeichnungspflicht für Deepfakes, aber auch benachbarte Themen wie irreführendes „AI-Washing" und Chatbot-Kennzeichnung.
Allerdings steigen mit dem zunehmenden Einsatz von KI im Marketing auch die rechtlichen Risiken. Fehlende oder unzureichende Kennzeichnungen, irreführende Darstellungen oder unklare Transparenzpflichten können schnell zu wettbewerbsrechtlichen Auseinandersetzungen führen – und damit auch zu Abmahnungen durch Mitbewerber oder entsprechende Verbände.
Welche typischen Angriffspunkte sich im digitalen Marketing ergeben und wie Unternehmen auf Abmahnungen rechtssicher reagieren können, zeigt Rechtsanwalt Antonio Reschke auf den Hamburger Datenschutztagen. Anhand konkreter Praxisfälle erläutert er, wie Abmahnstrategien funktionieren und welche Maßnahmen Unternehmen und öffentliche Einrichtungen ergreifen können, um rechtliche Risiken im digitalen Umfeld frühzeitig zu erkennen und zu vermeiden.

Quelle: Wettbewerbszentrale e.V.

Parallel-Vortrag

Abmahnungen im digitalen Marketing – Konkrete Praxisstrategien für Unternehmen und staatliche Einrichtungen

Referent: RA Antonio Reschke
Termin: 11.6.2026 – 15:10 Uhr
Weitere Informationen unter: www.datakontext.com/DS-Tage

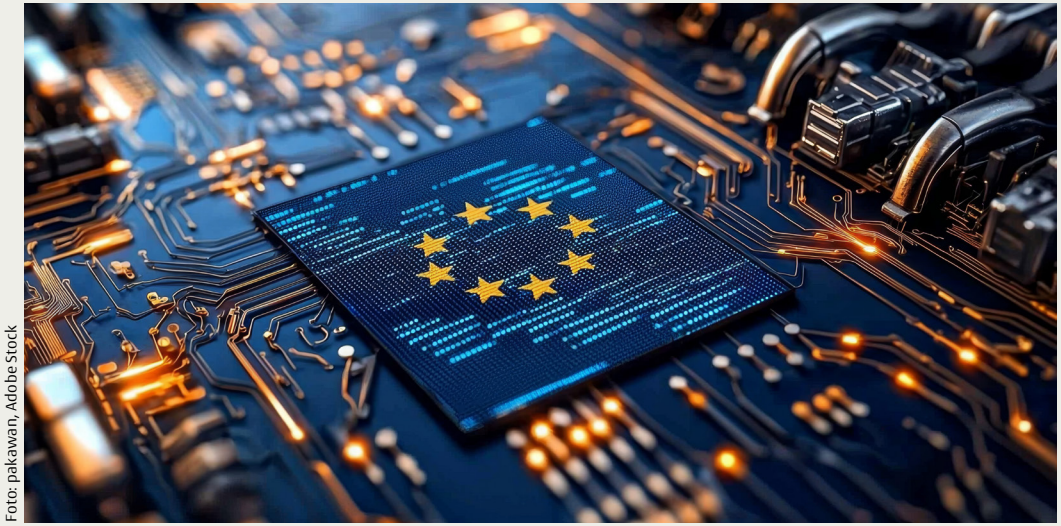

Foto: pakawan, Adobe Stock

Kommission stärkt Resilienz und Kapazitäten der EU im Bereich der Cybersicherheit

Europa ist täglich Cyberangriffen und hybriden Angriffen auf wesentliche Dienste und demokratische Institutionen ausgesetzt, die von erfahrenen staatlichen und kriminellen Gruppen verübt werden.

Angesichts dieser wachsenden Bedrohungen hat die Europäische Kommission am 20. Januar 2026 ein neues Cybersicherheitspaket vorgeschlagen, um die Resilienz und die Kapazitäten der EU im Bereich der Cybersicherheit weiter zu stärken.
Das Paket umfasst einen Vorschlag für eine überarbeitete Cybersicherheitsverordnung, mit der die Sicherheit der EU-Lieferketten im Bereich der Informations- und Kommunikationstechnik (IKT) verbessert wird. So soll durch ein einfacheres Zertifizierungsverfahren sichergestellt werden, dass Produkte, die die EU-Bürgerinnen und -Bürger erreichen, von vornherein cybersicher sind. Der Vorschlag erleichtert auch die Einhaltung der bestehenden EU-Cybersicherheitsvorschriften und stärkt die Rolle der Agentur der Europäischen Union für Cybersicherheit (ENISA) im Hinblick auf die Unterstützung der Mitgliedstaaten und der EU beim Umgang mit Cybersicherheitsbedrohungen.

Stärkung der Sicherheit der IKT-Lieferketten in der EU

Die neue Cybersicherheitsverordnung soll die Risiken in der IKT-Lieferkette der EU verringern, die von Lieferanten aus Drittländern ausgehen, bei denen Bedenken hinsichtlich der Cybersicherheit bestehen. Damit wird ein vertrauenswürdiger Rahmen für die Sicherheit der IKT-Lieferkette festgelegt, der auf einem harmonisierten, verhältnismäßigen und risikobasierten Ansatz beruht. Dies wird es der EU und den Mitgliedstaaten ermöglichen, Risiken in den 18 kritischen Sektoren der EU gemeinsam zu ermitteln und zu mindern, wobei auch die wirtschaftlichen Auswirkungen und das Marktangebot berücksichtigt werden.
Die jüngsten Cybersicherheitsvorfälle haben die großen Risiken deutlich gemacht, die von Schwachstellen in den für das Funktionieren kritischer Dienste und Infrastrukturen unerlässlichen IKT-Lieferketten ausgehen.
In der heutigen geopolitischen Landschaft geht es bei der Sicherheit der Lieferketten nicht mehr nur um die Sicherheit technischer Produkte oder Dienste, sondern auch um Risiken im Zusammenhang mit Lieferanten, insbesondere um Abhängigkeiten und Einflussnahme aus dem Ausland.
Die neue Cybersicherheitsverordnung wird die obligatorische Minderung der von Hochrisikoanbietern aus Drittländern ausgehenden Risiken für die europäischen Mobilfunknetze ermöglichen und auf den Arbeiten aufbauen, die bereits im Rahmen des Instrumentariums für die 5G-Sicherheit durchgeführt wurden.

Vereinfachung und Erweiterung des europäischen Rahmens für die Cybersicherheitszertifizierung

Mit der überarbeiteten Cybersicherheitsverordnung wird sichergestellt, dass Produkte und Dienste, die die Verbraucherinnen und Verbraucher in der EU erreichen, effizienter auf ihre Sicherheit geprüft werden. Dies wird durch einen erneuerten europäischen Rahmen für die Cybersicherheitszertifizierung (European Cybersecurity Certification Framework, ECCF) erfolgen. Der ECCF wird für mehr Klarheit und einfachere Verfahren sorgen, sodass Zertifizierungssysteme standardmäßig innerhalb von 12 Monaten entwickelt werden können.

Außerdem wird eine flexiblere und transparentere Governance eingeführt, um die Interessenträger durch Information und Konsultation der Öffentlichkeit besser einzubeziehen.

Zertifizierungssysteme, die von der ENISA verwaltet werden, werden zu einem praktischen, freiwilligen Instrument für Unternehmen, mit dessen Hilfe sie die Einhaltung der EU-Rechtsvorschriften nachweisen und so den Aufwand und die Kosten verringern können. Neben IKT-Produkten, -Diensten und -Prozessen sowie verwalteten Sicherheitsdiensten werden Unternehmen und Organisationen in der Lage sein, ihre Cyberabwehr zertifizieren zu lassen, um dem Marktbedarf gerecht zu werden. Letztlich wird der erneuerte ECCF einen Wettbewerbsvorteil für EU-Unternehmen darstellen. Für Bürgerinnen und Bürger, Unternehmen und Behörden in der EU wird er ein hohes Maß an Sicherheit und Vertrauen in komplexe IKT-Lieferketten gewährleisten.

Einfachere Einhaltung der Cybersicherheitsvorschriften

Das Paket enthält Maßnahmen zur Vereinfachung der Einhaltung der EU-Cybersicherheitsvorschriften und Risikomanagementanforderungen für in der EU tätige Unternehmen, die die in der Digital-Omnibus-Verordnung vorgeschlagene zentrale Anlaufstelle zur Meldung von Vorfällen ergänzen. Mit gezielten Änderungen der NIS-2-Richtlinie soll die Rechtsklarheit erhöht werden. Dies wird 28.700 Unternehmen, darunter 6.200 Kleinst- und Kleinunternehmen, die Einhaltung der Vorschriften erleichtern. Außerdem wird eine neue Kategorie kleiner Midcap-Unternehmen eingeführt, um die Befolgungskosten für 22.500 Unternehmen zu senken. Die Änderungen werden die Zuständigkeiten vereinfachen, die Erhebung von Daten über Ransomware-Angriffe straffen und die Beaufsichtigung grenzüberschreitend tätiger Einrichtungen dank der verstärkten Koordinierungsrolle der ENISA erleichtern.

Ermächtigung der ENISA zur Stärkung der Resilienz Europas im Bereich der Cybersicherheit

Seit der Annahme des ersten Rechtsakts zur Cybersicherheit im Jahr 2019 ist die ENISA zu einem Eckpfeiler des Cybersicherheitsökosystems der EU geworden. Gestützt auf die heute vorgelegte überarbeitete Cybersicherheitsverordnung kann die ENISA der EU und ihren Mitgliedstaaten künftig besser dabei helfen, die gemeinsamen Bedrohungen zu erfassen. Sie ermöglicht es ihnen auch, sich auf Cybervorfälle vorzubereiten und darauf zu reagieren.

Die Agentur wird Unternehmen und Interessenträger, die in der EU tätig sind, weiter unterstützen, indem sie frühzeitig vor Cyberbedrohungen und -vorfällen warnt. In Zusammenarbeit mit Europol und den Computer-Notfallteams wird sie Unternehmen helfen, auf Ransomware-Angriffe zu reagieren und sich von ihnen zu erholen. Darüber hinaus wird die ENISA ein Unionskonzept entwickeln, um den Interessenträgern bessere Dienste für das Schwachstellenmanagement zur Verfügung zu stellen. Sie wird die zentrale Anlaufstelle zur Meldung von Sicherheitsvorfällen betreiben, die mit der Digital-Omnibus-Verordnung vorgeschlagen wird.

Die ENISA wird nach wie vor eine Schlüsselrolle beim weiteren Aufbau einer qualifizierten Arbeitskräftebasis im Bereich der Cybersicherheit in Europa spielen. Dazu wird sie die Akademie für Cybersicherheitskompetenzen als Pilotinitiative fortführen und EU-weite Systeme zur Bescheinigung von Cybersicherheitskompetenzen einrichten.

Nächste Schritte

Die neue Cybersicherheitsverordnung wird unmittelbar nach der Annahme durch das Europäische Parlament und den Rat der EU in Kraft treten. Die begleitenden Änderungen der NIS-2-Richtlinie werden ebenfalls zur Annahme vorgelegt. Nach deren Annahme haben die Mitgliedstaaten ein Jahr Zeit, um die Richtlinie in nationales Recht umzusetzen und der Kommission ihre Umsetzungsvorschriften zu übermitteln.

Die geplanten Maßnahmen zeigen, dass Cybersicherheit zunehmend zu einer zentralen regulatorischen und organisatorischen Herausforderung für Unternehmen wird. Neben technischen Schutzmaßnahmen rücken dabei insbesondere Fragen der Resilienz, der Governance und des Krisenmanagements in den Fokus. Organisationen müssen nicht nur ihre IT-Infrastruktur absichern, sondern auch klare Verantwortlichkeiten, Meldewege und Entscheidungsprozesse etablieren, um im Fall eines Cybervorfalls handlungsfähig zu bleiben und regulatorische Anforderungen zu erfüllen.

Wie sich diese Anforderungen in der Praxis umsetzen lassen und welche Strukturen Unternehmen für ein wirksames Krisen- und Resilienzmanagement benötigen, zeigt Marc Neumann im Pre-Seminar „Cybersecurity & Datenschutz – Resilienz und Krisenmanagement unter NIS-2, DORA, KRITIS“ auf den Hamburger Datenschutztagen. Das Seminar vermittelt praxisnah, wie Organisationen Cybervorfälle strukturiert bewerten, Meldepflichten erfüllen und ihre Handlungsfähigkeit in den ersten Stunden eines Incidents sicherstellen können.

Quelle: Europäische Kommission

Pre-Seminar

Cybersecurity & Datenschutz – Resilienz und Krisenmanagement unter NIS-2, DORA, KRITIS

Referent: Marc Neumann
Termin: 10.6.2026 – 9:30 Uhr bis 17:00 Uhr
Weitere Informationen unter: www.datakontext.com/DS-Tage

Foto: Crazyluke, Adobe Stock

Digitaler Omnibus: EDSA und EDSB unterstützen Vereinfachung sowie Wettbewerbsfähigkeit und äußern gleichzeitig zentrale Bedenken

Seit ihrem Inkrafttreten 2018 war die Datenschutz-Grundverordnung (DS-GVO) unberührt. Das ändert sich jetzt. Am 19. November 2025 legte die EU-Kommission mit dem sogenannten Digitalen Omnibus ein umfassendes Reformpaket vor, das erstmals zentrale Regelungen der DS-GVO anpasst. Betroffen sind unter anderem die Datenschutz-Grundverordnung, die NIS-2-Richtlinie, das Datengesetz sowie die Datenschutzrichtlinie für elektronische Kommunikation.

Vereinfachung ja, aber mit Fragezeichen

Der Europäische Datenschutzausschuss (EDSA) und der Europäische Datenschutzbeauftragte (EDSB) haben eine gemeinsame Stellungnahme zum Vorschlag für eine Verordnung über digitale Omnibusse verabschiedet. EDSA und EDSB begrüßen das Ziel der Vereinfachung und Stärkung der Wettbewerbsfähigkeit europäischer Unternehmen ausdrücklich. Zugleich äußern sie in ihrer gemeinsamen Stellungnahme zentrale Bedenken. Sie konzentrieren sich dabei auf die Aspekte der DS-GVO, der EU-DSVO, der Datenschutzrichtlinie für elektronische Kommunikation und des Besitzstands im Bereich der Datenverarbeitung. Insbesondere bewerten sie, ob der Vorschlag

1) zu einer echten Vereinfachung führt und die Einhaltung erleichtert,
2) mehr Rechtssicherheit schafft und
3) die Grundrechte des Einzelnen beeinträchtigt.

Änderungen, die Anlass zu erheblichen Bedenken geben

Einige vorgeschlagene Änderungen geben Anlass zu erheblichen Bedenken, da sie das Schutzniveau für Einzelpersonen beeinträchtigen, Rechtsunsicherheit schaffen und die Anwendung des Datenschutzrechts erschweren können.

Der EDSA und der EDSB fordern die beiden gesetzgebenden Organe nachdrücklich auf, die vorgeschlagenen Änderungen an der Definition personenbezogener Daten nicht anzunehmen, da sie weit über eine gezielte oder technische Änderung der DS-GVO hinausgehen. Darüber hinaus spiegeln sie nicht genau wider und gehen eindeutig über die Rechtsprechung des EuGH hinaus, und sie würden dazu führen, dass der Begriff der personenbezogenen Daten erheblich eingeschränkt würde. Der Europäischen Kommission sollte nicht die Befugnis übertragen werden, im Wege eines Durchführungsrechtsakts zu entscheiden, was nach der Pseudonymisierung keine personenbezogenen Daten mehr sind, da sich dies unmittelbar auf den Anwendungsbereich des EU-Datenschutzrechts auswirkt.

Schritte in die richtige Richtung

Der EDSA und der EDSB befürworten die Anhebung des Risikoschwellenwerts, der dazu führt, dass eine Datenschutzverletzung der zuständigen Datenschutzbehörde gemeldet werden muss, sowie die Verlängerung der Frist für die Übermittlung einer solchen Meldung. Dies würde den Verwaltungsaufwand für Organisationen erheblich verringern, ohne den Schutz personenbezogener Daten zu beeinträchtigen. Darüber hinaus sind die vorgeschlagenen gemeinsamen Vorlagen und Listen für Datenschutzverletzungen und Datenschutz-Folgenabschätzungen positiv.

Der EDSA und der EDSB begrüßen auch die vorgeschlagene Einführung einer neuen Ausnahmeregelung für die Verarbeitung besonderer Kategorien von Daten für die biometrische Authentifizierung, wenn die Überprüfungsmittel unter der alleinigen Kontrolle der Person stehen. Schließlich unterstützen sie die Harmonisierung des Begriffs „wissenschaftliche Forschung“ und andere damit zusammenhängende Änderungen, da sie die Rechtssicherheit erhöhen und zu einer stärkeren Harmonisierung beitragen.

Änderungen, die einer Feinabstimmung bedürfen

Wie in der Stellungnahme 28/2024 des EDSA zu KI-Modellen dargelegt, kann in einigen Fällen ein berechtigtes Interesse als Rechtsgrundlage im Zusammenhang mit der Entwicklung und Einführung von KI-Modellen oder -Systemen herangezogen werden. Daher halten es der EDSA und der EDSB nicht für erforderlich, eine spezifische Bestimmung dazu in die DS-GVO aufzunehmen.
Der EDSA und der EDSB begrüßen das Ziel des Vorschlags, eine spezifische Ausnahme vom Verbot der Verarbeitung sensibler Daten unter Auflagen einzuführen, die die zufällige und verbleibende Verarbeitung solcher Daten im Zusammenhang mit der Entwicklung und dem Betrieb von KI-Systemen oder -Modellen umfasst. Sie empfehlen jedoch mehrere Verbesserungen, wie die Klärung des Anwendungsbereichs der Ausnahmeregelung und die Gewährleistung von Schutzmaßnahmen während des gesamten Lebenszyklus.
Der EDSA und der EDSB stimmen dem Ziel der Kommission zu, den für die Verarbeitung Verantwortlichen bei Rechtsmissbrauch durch betroffene Personen Rechtsklarheit zu verschaffen. Sie sind jedoch der Ansicht, dass die Ausübung des Rechts auf Zugang zu anderen Zwecken als dem Schutz personenbezogener Daten kein Element sein sollte, das definiert, was ein Missbrauch ist. In Bezug auf die neue Ausnahmeregelung für Transparenz unterstützen der EDSA und der EDSB die Vereinfachung der Informationsanforderungen und die Verringerung des Verwaltungsaufwands, insbesondere für kleine und mittlere Unternehmen (KMU), schlagen jedoch Klarstellungen vor, um Rechtssicherheit zu gewährleisten und sicherzustellen, dass Einzelpersonen bei Bedarf weiterhin relevante Informationen über ihre Daten erhalten können. Schließlich sollten die Änderungen an der Bestimmung über die automatisierte individuelle Entscheidungsfindung präzisiert werden, damit diese Änderungen aussagekräftig und rechtlich fundiert sind.

Änderungen der Datenschutzrichtlinie für elektronische Kommunikation

Der EDSA und der EDSB unterstützen nachdrücklich das Ziel, eine Regulierungslösung bereitzustellen, um der Ermüdung der Einwilligung und der Verbreitung von Cookie-Bannern entgegenzuwirken. Dies betrifft beispielsweise die vorgeschlagenen Anforderungen an die Verwendung automatisierter und maschinenlesbarer Hinweise auf die Wahlmöglichkeiten von Einzelpersonen bei der Verarbeitung ihrer Daten. Der Einsatz technischer Mittel kann die Einhaltung der Vorschriften durch die für die Verarbeitung Verantwortlichen vereinfachen und Einzelpersonen dabei unterstützen, ihre Online-Entscheidungen wirksam zu gestalten.
Der EDSA und der EDSB begrüßen auch die begrenzten zusätzlichen Ausnahmen vom allgemeinen Verbot, personenbezogene Daten in den Endgeräten zu speichern oder Zugang zu ihnen zu erhalten, und fordern die beiden gesetzgebenden Organe ferner auf, Anreize für kontextbezogene Werbung anstelle von verhaltensorientierter Werbung zu schaffen, indem sie eine spezifische Ausnahme hinzufügen, die von einigen Garantien umgeben ist.
Der EDSA und der EDSB begrüßen, dass die Datenschutzbehörden mit der Aufsicht über solche Angelegenheiten betraut werden.
Gleichzeitig weisen der EDSA und der EDSB auf die rechtlichen und technischen Schwierigkeiten hin, die sich aus der Koexistenz zweier unterschiedlicher Regelungen für personenbezogene und nicht

personenbezogene Daten ergeben. Sie enthalten auch zusätzliche Empfehlungen zur Verbesserung der Rechtssicherheit, zur Minimierung des Risikos und zur Förderung verantwortungsvoller Innovationen.

Änderungen am Daten-Acquis

Der EDSA und der EDSB unterstützen die Vereinfachung des Besitzstands im Bereich der Daten durch die Integration des Daten-Governance-Gesetzes und der Vorschriften der Richtlinie über offene Daten über die Weiterverwendung von Daten und Dokumenten im Besitz öffentlicher Stellen in das Datengesetz.

In Bezug auf den Zugang, der von öffentlichen Stellen zur Weiterverwendung gewährt wird, empfehlen sie, die Klarheit des derzeitigen Rechtsrahmens zu wahren, nämlich dass er öffentliche Stellen nicht verpflichtet, die Weiterverwendung zuzulassen, und auch keine Rechtsgrundlage für die Gewährung des Zugangs bietet.

In Bezug auf öffentliche Notfälle empfehlen der EDSA und der EDSB zu bekräftigen, dass personenbezogene Daten nur in pseudonymisierter Form an öffentliche Stellen weitergegeben werden dürfen, wenn anonyme Daten nicht ausreichen, um auf den öffentlichen Notfall zu reagieren.

In Bezug auf Datenvermittlungsdienste und datenaltruistische Organisationen betonen der EDSA und der EDSB, wie wichtig ein vertrauenswürdiger und verantwortungsvoller Datenaustausch ist. Sie empfehlen die Beibehaltung spezifischer Schutzvorkehrungen, um Transparenz und Aufsicht zu fördern.

Der EDSA und der EDSB empfehlen, die Bestimmungen über die Durchsetzung weiter zu straffen (z. B. durch die Ermöglichung eines regulierungsübergreifenden Austauschs von Informationen über die Durchsetzung, auch mit Datenschutzbehörden, und durch die Klärung der Rolle der Datenschutzbehörden bei der Durchsetzung des Datengesetzes).

Der EDSA und der EDSB begrüßen die Bestätigung der Rolle des Europäischen Dateninnovationsrats (EDIB) bei der Unterstützung der kohärenten Anwendung des Datengesetzes durch den Vorschlag. In Bezug auf die Ausarbeitung von Leitlinien empfehlen sie, die Kommission zu ermächtigen, Leitlinien zu allen Themen im Zusammenhang mit dem Datengesetz herauszugeben, und die Rolle des EDIB bei der Unterstützung der Kommission in diesem Prozess zu präzisieren. Dies würde es der Kommission ermöglichen, gemeinsame Leitlinien mit dem EDSA auszuarbeiten. Zudem würde es dem EDIB die Möglichkeit bieten, die Kommission bei der Ausarbeitung solcher Leitlinien zu beraten und zu unterstützen.

Was das für die Praxis bedeutet

Das EU-Parlament und der Rat müssen dem Reformpaket noch zustimmen, und es bleibt zu hoffen, dass die Empfehlungen EDSA und EDSB berücksichtigt werden. Mit einer Umsetzung in nationales Recht ist also frühestens 2027 zu rechnen. Wie sich die datenschutzrechtliche „Großwetterlage“ 2026 für Unternehmen insgesamt einordnen lässt, welche Entwicklungen aus DS-GVO-Reform, KI-Regulierung und internationalen Datentransfers unmittelbar relevant sind und welche Handlungsempfehlungen sich daraus ableiten, fasst Dr. Jens Ambrock, Referatsleiter beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, auf den Hamburger Datenschutztagen 2026 kompakt zusammen.

Quelle: Europäische Kommission

Fachvortrag

EU-Datenschutzrecht im Fokus: DS-GVO, KI-Regulierung und internationale Leitlinie

Referent: Dr. Jens Ambrock
Termin: 12.6.2026 – 09:00 Uhr
Weitere Informationen unter: www.datakontext.com/DS-Tage

Impressum

DATAKONTEXT GmbH
Augustinusstraße 11 A
50226 Frechen

Telefon: +49 2234 98949-30
Fax: +49 2234 98949-32

kundenservice@datakontext.com
www.datakontext.com

Geschäftsführung:
Stefan Waldeisen
Dr. Karl Ulrich
Amtsgericht Köln, HRB 82299

Newsletter

Möchten Sie bei Erscheinen der aktuellen Datenschutz Newsbox informiert werden und so keine Ausgabe mehr verpassen? Dann tragen Sie sich unverbindlich und kostenlos ein unter:
www.datakontext.com/newsletter