Luther.

Newsletter IT- & Datenschutzrecht

Ausgabe November 2026



CRA-Durchführungsgesetz: BSI wird Aufsichtsbehörde für Produkte mit digitalen Elementen

Der Bundestag hat am 15. Oktober 2026 das Durchführungsgesetz zum Cyber Resilience Act (CRA, Cyberresilienz-Verordnung) verabschiedet. Mit diesem Gesetz wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zuständige Behörde benannt. Ab Dezember 2027 erstreckt sich das CE-Kennzeichen zudem auf die Cybersicherheit von Produkten mit digitalen Elementen. Die Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle gelten bereits seit dem 11. September 2026.

Die Aufgaben des BSI

- Marktüberwachung: Das BSI kann IT-Produkte stichprobenartig oder gezielt auf ihre Cybersicherheit prüfen, Nachbesserungen verlangen und bei Verstößen Sanktionen und Bußgelder verhängen. Produkte mit digitalen Elementen, die den CRA-Anforderungen nicht genügen, darf es vom Markt nehmen.

- Notifizierende Behörde: Das BSI bestätigt die Kompetenz von Konformitätsbewertungsstellen; durch sie können Hersteller Produkte und Prozesse auf CRA-Konformität prüfen lassen.

- Zuständiges CSIRT (Computer Security Incident Response Team): Die Koordinierung der CRA-Meldungen für Deutschland liegt seit dem 11. September 2026 beim BSI.

- Beschwerdestelle: Das BSI nimmt Hinweise von Verbraucherinnen und Verbrauchern auf Verstöße gegen den CRA entgegen.

- Unterstützung: Vor allem kleine und mittlere Unternehmen sollen beim Erfüllen der CRA-Pflichten Hilfestellung erhalten.

Meldepflichten und Fristen

Zu melden sind aktiv ausgenutzte Schwachstellen sowie schwerwiegende Sicherheitsvorfälle, die Produkte mit digitalen Elementen betreffen, welche auf dem Unionsmarkt bereitgestellt werden.

Eine Schwachstelle gilt nach Art. 3 Abs. 42 CRA als aktiv ausgenutzt, wenn bekannt ist, dass ein böswilliger Akteur sie derzeit ausnutzt. Ein schwerwiegender Sicherheitsvorfall im Sinne des Art. 3 Abs. 44 CRA liegt vor, wenn die Sicherheit des Produkts erheblich beeinträchtigt wird, etwa hinsichtlich Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit; die Einstufungskriterien ergeben sich aus Art. 14 Abs. 5 CRA. Meldepflichtig sind Hersteller sowie Verwalter quelloffener Software (Open-Source-Software-Stewards), Letztere jedoch nur, soweit sie an der Entwicklung der betreffenden Produkte beteiligt sind. Das Verfahren gliedert sich wie folgt:

- Frühwarnung: binnen 24 Stunden nach Bekanntwerden.
- Meldung: binnen 72 Stunden mit allgemeinen Informationen und erster Bewertung.
- Abschlussbericht: Bei Schwachstellen ist der Abschlussbericht spätestens 14 Tage nach Bereitstellung einer Korrekturmaßnahme wie eines Patches vorzulegen, bei schwerwiegenden Vorfällen binnen eines Monats nach der 72-Stunden-Meldung.

Die Meldungen sind an das koordinierende CSIRT zu richten, das sich grundsätzlich nach dem Ort der Hauptniederlassung des Herstellers bestimmt; Einzelheiten regelt Art. 14 Abs. 7 CRA. Dieses CSIRT leitet die Angaben unverzüglich an die CSIRTs der übrigen Mitgliedstaaten weiter, in denen das Produkt bereitgestellt wird, und unterrichtet zugleich die ENISA. Unter außergewöhnlichen Umständen kann die Weiterleitung nach Art. 16 Abs. 2 CRA aufgeschoben werden; die Voraussetzungen hierfür bestimmt die Delegierte Verordnung (EU) 2026/881.

Praxisfolgen

- **Meldefähigkeit herstellen:** Die 24-Stunden-Frist beginnt mit der Kenntnisnahme. Der Meldeweg samt Zuständigkeiten sollte deshalb vorab feststehen.
- **Produktportfolio prüfen:** Ab Dezember 2027 erfasst das CE-Kennzeichen auch die Cybersicherheit von Produkten mit digitalen Elementen.
- **Patch-Prozess absichern:** Bei Schwachstellen ist der Abschlussbericht spätestens 14 Tage nach Bereitstellung einer Korrekturmaßnahme (z. B. eines Patches) fällig; Release- und Berichtsplanung gehören zusammen.

VG Düsseldorf: Werbemails brauchen nachweisbare Einwilligung — IP-Adressen genügen nicht

Wer Werbemails verschickt, muss die Einwilligung der Empfänger belegen können, wobei technische Verbindungsdaten diesen Beleg nicht ersetzen. Das Verwaltungsgericht Düsseldorf hat die Klage eines Unternehmens gegen eine Verwarnung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) abgewiesen (Urteil vom 27.07.2026, Az. 29 K 9714/24). Das Urteil ist rechtskräftig.

Der Fall

Geklagt hatte ein Unternehmen aus NRW, das Internetportale betreibt und Reisedienstleistungen sowie Online-Marketing anbietet. Ein Mann hatte sich bei der LDI NRW beschwert, weil er auf seine private E-Mail-Adresse Werbung des Unternehmens erhalten hatte; seine Adresse habe er dem Unternehmen aber nie überlassen. Im Jahr 2020 wandte das Unternehmen ein, er habe auf der Website des Unternehmens einer Zusendung zugestimmt, die Bestätigungsmail des Double-Opt-in-Verfahrens (DOI) könne es jedoch nicht vorlegen, weil es sie aus Datenschutzgründen nicht aufbewahre. Nach einer erneuten Beschwerde über eine Werbemail verwarnte die Behörde das Unternehmen mit Bescheid vom 24.10.2024 wegen Verarbeitung personenbezogener Daten ohne nachgewiesene Einwilligung (Art. 58 Abs. 2 Buchst. b DSGVO).

Warum die vorgelegten Daten nicht genügen

Wer sich auf eine Einwilligung beruft, muss nach Art. 7 Abs. 1 DSGVO belegen können, dass die betroffene Person eingewilligt hat. Das Unternehmen präsentierte dafür die E-Mail-Adresse, eine IP-Adresse nebst Zeitstempel sowie die IP-Adresse aus dem Bestätigungsschritt nebst Zeitstempel. Die Angaben sind jedoch nach Ansicht des Gerichts zum Nachweis der erteilten Einwilligung ungeeignet:

- **Eine IP-Adresse steht für ein Gerät, nicht für eine Person:** Zwar lässt sich über sie der Anschlussinhaber ermitteln. Wer zum protokollierten Zeitpunkt tatsächlich daran saß, bleibt offen, weil die IP-Adresse keinem bestimmten Nutzer zugeordnet ist.
- **Die DOI-IP-Adresse belegt nur einen zweiten Transport:** Sie zeigt lediglich, dass erneut Daten von dieser Adresse an ein Gerät des Unternehmens gingen. Welchen Inhalt das Paket hatte und ob darin eine Einwilligung lag, ist ihr nicht zu entnehmen.
- **Die Bestätigungsmail fehlt:** Nach dem eigenen Vortrag des Unternehmens (2022) wurden die DOI-Mails per Bcc an ein eigenes Postfach geleitet und dort aufbewahrt, um sie bei Rückfragen ausdrucken zu können. Hätte es sein Verfahren beachtet, hätte es die Mail vorlegen können; das Gericht schloss daraus, dass es keine gibt.

Kann der Verantwortliche den Nachweis nicht führen, gilt die Einwilligung als nicht wirksam erteilt — mit denselben Rechts-

folgen wie bei einer tatsächlich fehlenden Einwilligung. Die Verwarnung hielt das Gericht zudem für das mildeste Abhilfeinstrument nach Art. 58 Abs. 2 DSGVO, das keine unmittelbaren finanziellen Nachteile mit sich bringt. Die Landesdatenschutzbeauftragte Bettina Gayk sieht darin eine Warnung an unseriöse Anbieter: „Wer glaubt, mit nicht aussagekräftigen Belegen eine Einwilligung behaupten zu können, wird spätestens vor Gericht die Quittung dafür bekommen."

Praxisfolgen

- **Bestätigung dokumentieren – und das eigene Verfahren einhalten:** Das Gericht vermisste einen Ausdruck der Bestätigungsmail. Nach dem Hinweis der LDI gehört zu einem wirksamen Double-Opt-in-Verfahren die vollständige Dokumentation durch Speicherung und Möglichkeit zum Ausdrucken. Eine beschriebene Routine hilft nur, wenn sie eingehalten wird: Die vom Unternehmen selbst geschilderte Bcc-Sicherung hätte die Bestätigungsmail hervorgebracht.

- **Personenbezug und Inhalt belegen:** Der Nachweis muss erkennen lassen, dass gerade die betroffene Person den Vorgang ausgelöst und was sie erklärt hat. Verbindungsdaten mit Zeitstempel reichen dafür allein nicht.

BAG: Auskunftsrecht nach Art. 15 DSGVO umfasst keine Kopien ganzer Dokumente

Wer Auskunft nach Art. 15 DSGVO verlangt, hat grundsätzlich Anspruch auf die personenbezogenen Daten, nicht aber auf das Dokument, in dem sie stehen. Das Bundesarbeitsgericht hat mit Urteil vom 16. April 2026 (Az.: 8 AZR 169/25) die Revision einer in leitender Funktion beschäftigten Arbeitnehmerin zurückgewiesen, die von ihrem Arbeitgeber Kopien zweier Compliance-Abschlussberichte über ihr eigenes Führungsverhalten verlangt hatte.

Der Fall in Kürze

Die Klägerin bekleidete bei der Beklagten eine Position mit Leitungsaufgaben. Im April 2023 unterrichtete die Ombudsfrau des Unternehmens die Compliance-Abteilung davon, dass drei Personen den Führungsstil der Klägerin mit den Worten einschüchternd, herabwürdigend, respektlos und unehrlich beschrieben haben. Eine von der Beklagten beauftragte Rechtsanwaltskanzlei prüfte daraufhin den Vorwurf. Von den Abschlussberichten in den Fassungen vom 31. Januar 2024 und vom 6. Februar 2024 verlangte die Klägerin Kopien, um zu prüfen, welche Aussagen über sie gemacht und gespeichert worden waren. Während das Arbeitsgericht den Anträgen noch entsprochen hatte, lehnte das Landesarbeitsgericht München die Herausgabe von Kopien ab und gestattete lediglich die Einsicht in die Fassung vom 6. Februar 2024.

Die Entscheidung

Nach Ansicht des Bundesarbeitsgerichts folgt aus Art. 15 Abs. 3 Satz 1 DSGVO kein gesonderter Anspruch auf Herausgabe eines Dokuments; die Vorschrift betrifft vielmehr die Modalität der Auskunftserteilung und verlangt eine originalgetreue, verständliche Wiedergabe aller verarbeiteten Daten. Der Leitsatz lautet:

„Das einheitliche Auskunftsrecht nach Art. 15 Abs. 1 i. V. m. Abs. 3 Satz 1 DSGVO […] bezieht sich grundsätzlich nur auf die in einem Dokument enthaltenen personenbezogenen Daten und nicht auf das gesamte Dokument." (BAG, Az. 8 AZR 169/25)

- **Personenbezogene Daten:** Hierunter fallen alle Informationen über eine bestimmte oder bestimmbare Person, einschließlich bewertender Äußerungen und subjektiver Einschätzungen. Der Bericht handelt vom Führungsverhalten der Klägerin und enthält deshalb zwangsläufig Informationen über sie.

- **Rechtliche Ausführungen:** Eine rechtliche Bewertung ist keine Information über die betroffene Person, sondern allenfalls darüber, wie der Verantwortliche die Rechtslage einschätzt. Eine Kopie des gesamten Berichts kann die Klägerin nicht verlangen, auch nicht teilgeschwärzt.

- **Ausnahme:** Auszüge oder ganze Dokumente sind nur geschuldet, wenn ihre Überlassung unerlässlich ist, damit die betroffene Person ihre Rechte wirksam ausüben kann, etwa weil die Daten ohne Kontext nicht verständlich sind. Dafür sah das Bundesarbeitsgericht keine Anhaltspunkte: Für Berichtigung, Löschung und Einschränkung nach Art. 16, 17, 18 DSGVO braucht die Klägerin die rechtlichen Bewertungen nicht; gegen eine ihrer Ansicht nach unzutreffende Rechtsauffassung kann sie ggf. prozessual vorgehen.

- **Personalakte:** § 26 Abs. 2 SprAuG und § 83 Abs. 1 BetrVG umfassen ein Einsichtsrecht, ein Anspruch auf Ko-

pien besteht nur in angemessenem Umfang. Wer die Personalunterlagen als Ganzes kopieren will, sprengt diesen Rahmen.

Praxisfolgen

Für Unternehmen als Verantwortliche zieht die Entscheidung die Grenze zwischen Datenkopie und Aktenherausgabe:

- **Antwortumfang:** Zu liefern ist grundsätzlich eine Kopie der personenbezogenen Daten, nicht das Schriftstück. Bei Untersuchungsberichten müssen rechtliche Ausführungen nicht mitgeliefert werden, soweit sie eine bloße Rechtsanalyse enthalten.

- **Kontext prüfen:** Verlangt eine betroffene Person das ganze Dokument, ist zu prüfen, ob die Daten ohne den Rahmen unverständlich blieben. Eine Kopie von Auszügen oder des ganzen Dokuments ist geschuldet, wenn sie für die wirksame Rechteausübung unerlässlich ist; Rechte Dritter sind zu berücksichtigen.

BGH: Unterlassungsanspruch wegen Datenübermittlung an Drittanbieter

Der Bundesgerichtshof hat mit Urteil vom 21. Juli 2026 (VI ZR 144/23) entschieden, dass ein Anspruch auf Unterlassung der weiteren Übermittlung personenbezogener Daten nicht allein deshalb ausgeschlossen ist, weil das Unionsrecht die Rechtsfolgen von Verstößen gegen die DSGVO abschließend regelt. Das Berufungsurteil des Oberlandesgerichts Frankfurt am Main (16 U 22/22) wurde insofern aufgehoben und die Sache zur erneuten Entscheidung zurückverwiesen. Ob der geltend gemachte Unterlassungsanspruch tatsächlich besteht, ist damit weiterhin offen.

Der Fall

Die Beklagte betreibt einen Online-Shop. In ihre Seiten sind Funktionen von Drittanbietern so eingebettet, dass die Programmdaten nicht auf dem Server der Beklagten liegen, sondern der Browser des Nutzers auf Seiten der Diensteanbieter gelenkt wird (sog. Cloud-Lösung). Beim Seitenaufruf wird dem Drittserver die aktuelle IP-Adresse des Nutzers mitgeteilt. Nach eigener Darstellung hat der Kläger 2020 in dem Shop bestellt und verlangt nun, die Weitergabe zu unterlassen, solange keine vorherige Einwilligung nach Art. 4 Nr. 11 DSGVO vorliegt. Das Landgericht Wiesbaden hat die Klage abgewiesen: Der Antrag sei mangels Bestimmtheit unzulässig, die Klage zudem unbegründet. Das OLG Frankfurt am Main hat die Berufung zurückgewiesen, weil die DSGVO die Folgen von Datenschutzverstößen abschließend und voll harmonisiert regele und daneben für nationales Recht kein Platz sei.

Was der BGH entschieden hat

Die Zulässigkeit hat das Berufungsgericht nach Auffassung des Senats zu Recht bejaht. Der Senat hält jedenfalls den zuletzt gestellten Hauptantrag für hinreichend bestimmt, weil er der Beklagten untersagen soll, ihre Shop-Seiten so zu gestalten, dass bei deren Aufruf durch den Kläger ohne dessen Einwilligung Daten an die im Antrag bezeichneten Dienste übermittelt werden. Daraus ergebe sich unzweideutig, welches Verhalten verboten werden soll. Ob schon der ursprüngliche, auf „personenbezogene oder -beziehbare Daten“ gerichtete Antrag bestimmt war, lässt der Senat offen.

In der Sache trägt die Begründung des OLG nicht. Der Senat verweist auf das zeitlich nachfolgende Urteil des Gerichtshofs der Europäischen Union vom 4. September 2025 (C-655/23). Danach sieht die DSGVO für eine betroffene Person, die, wie der Kläger, keine Löschung beantragt, keinen gerichtlichen Rechtsbehelf vor, mit dem sie präventiv die künftige Unterlassung einer erneuten unrechtmäßigen Verarbeitung durch den Verantwortlichen erwirken kann. Die Mitgliedstaaten sind aber nicht gehindert, einen solchen Rechtsbehelf in ihren Rechtsordnungen vorzusehen. Er kann die praktische Wirksamkeit der DSGVO-Bestimmungen verstärken und das angestrebte hohe Schutzniveau verbessern.

Nach der Rechtsprechung aus der Zeit vor der DSGVO kommen bei einer durch rechtswidrige Datenverarbeitung verursachten Verletzung des Rechts auf informationelle Selbstbestimmung grundsätzlich Ansprüche aus § 1004 Abs. 1, § 823 Abs. 1 BGB in entsprechender Anwendung in Betracht. Diese Grundlagen seien auch bei einer nach der DSGVO rechtswidrigen Verarbeitung in Betracht zu ziehen. Ob dem Begehren entgegensteht, dass die DSGVO eigene Rechte, insbesondere das Recht auf Löschung nach Art. 17 DSGVO, bereithält und es deshalb an einem Bedürfnis für nationalen Rechtsschutz fehlt, ließ der Senat offen. Auf der festgestellten Grundlage lasse sich jedenfalls nicht annehmen, dass der Kläger sein Ziel über diese Rechte erreichen kann.

Praxisfolgen

Für Unternehmen, die Drittanbieter-Dienste einbinden, ändert sich die Verteidigungslinie:

- **Abschließende DSGVO-Regelung trägt nicht mehr:** Wer einer Unterlassungsklage allein entgegenhält, das Unionsrecht regele die Folgen von Datenschutzverstößen abschließend, dringt damit nach dieser Entscheidung nicht durch.

- **Nationale Anspruchsgrundlagen berücksichtigen:** Der Senat sieht § 1004 Abs. 1 BGB analog i.V.m. § 823 Abs. 1 BGB, zusammen mit Art. 1 Abs. 1 und Art. 2 Abs. 1 GG, sowie – bei Verstoß gegen eine als Schutzgesetz einzuordnende Datenschutzvorschrift – § 1004 Abs. 1 BGB analog i.V.m. § 823 Abs. 2 BGB als in Betracht zu ziehende Anspruchsgrundlagen.

Irische Datenschutzbehörde: 403 Millionen Euro Bußgeld gegen Google wegen Standortdaten

Die irische Datenschutzbehörde Data Protection Commission (DPC) hat am 21. September 2026 ein Bußgeld über 403 Millionen Euro gegen Google Ireland Limited bekanntgegeben. Anlass war die Verarbeitung von Standortdaten in den drei Funktionen „Web & App Activity“, „Location History“ und „Location Accuracy“ zwischen dem 25. Mai 2018 und dem 4. Februar 2020. Zugleich verpflichtete die Behörde Google, seine Verarbeitung binnen sechs Monaten mit der DSGVO in Einklang zu bringen. Eine vollständige Fassung der Entscheidung wird die DPC nach eigenen Angaben noch nachliefern.



Untersuchung von Amts wegen

Das Verfahren eröffnete die DPC im Februar 2020 aus eigener Initiative (own-volition inquiry). Auslöser waren Beschwerden mehrerer europäischer Verbraucherschutzorganisationen, darunter BEUC. Die Zuständigkeit folgt aus dem Europasitz von Google Ireland in Dublin: Die DPC handelt als federführende Aufsichtsbehörde.

Vier Verstöße

Die Behörde stellt Verstöße in vier Punkten fest:

- **Rechtmäßigkeit und Fairness:** Die Verarbeitung von Standortdaten in „Web & App Activity“ und „Location History“ verstieß gegen diese beiden Grundsätze.

- **Rechenschaftspflicht:** Bei „Location Accuracy“ konnte Google nicht belegen, dass es Rechtmäßigkeit, Fairness und Transparenz einhält. Den fehlenden Nachweis führt die Behörde als eigenen Verstoß an.

- **Transparenz:** Die Informationspflichten verletzte Google bei allen drei Funktionen.

- **Speicherdauer:** Standortdaten aus „Web & App Activity“ und „Location History“ wurden länger aufbewahrt als erforderlich.

Warum Standortdaten ins Gewicht fallen

Die DPC betont die Aussagekraft von Standortdaten. So könnten Standortdaten viel über das Leben einer Person preisgeben. Nutzer hätten möglicherweise nicht bemerkt, dass ihr Standort etwa genutzt wurde, um sie mit Werbung zu beeinflussen oder ihre Interessen abzuleiten, und könnten so die Kontrolle über ihre Daten verlieren. Die zu lange Speicherung habe diesen Kontrollverlust zudem verstärkt.

Google macht geltend, dass die beanstandeten Vorgänge einer früheren Praxis zuzuordnen seien. Seit 2019 seien die Abläufe grundlegend umgestellt worden. An der Bewertung der Jahre 2018 bis 2020 ändert das nichts.

Praxisfolgen

Die von der DPC veröffentlichten Feststellungen unterstreichen allgemein sinnvolle Herangehensweisen für Unterneh-

men, um DSGVO-Compliance sicherzustellen, insbesondere (aber nicht nur) wenn sie Standortdaten erheben:

- **Transparenz:** Hinsichtlich der Gestaltung von Einstellungen und Datenschutzhinweisen sollten Verantwortliche prüfen, ob für Nutzer hinreichend erkennbar ist, welche Daten zu welchem Zweck verarbeitet werden.

- **Dokumentation:** Verantwortliche sollten belegen können, dass ihre Verarbeitung rechtmäßig, fair und transparent ist; schon den fehlenden Nachweis wertete die DPC als eigenen Verstoß.

- **Löschfristen:** Verantwortliche sollten ihre Löschfristen auf Angemessenheit prüfen.

EDPB: Leitlinien zum Web Scraping für KI-Training

Der Europäische Datenschutzausschuss (EDPB) hat am 07. Juli 2026 die Leitlinien 03/2026 zum Web Scraping im Kontext generativer KI als Version 1.0 für die öffentliche Konsultation verabschiedet. Sie richten sich an private Unternehmen, die Trainingsdaten selbst oder über einen Dienstleister aus dem Netz ziehen oder einen bereits gescrapten Datensatz übernehmen. Die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO bleibt bestehen, auch wenn der Verantwortliche kaum überblickt, welche personenbezogenen Daten sein Datensatz enthält.

Was die Leitlinien erfassen

Web Scraping meint den automatisierten Abruf und das Speichern von Informationen aus öffentlich zugänglichen Webdiensten, wie öffentliche Register, Open-Data-Portale, Nachrichtenseiten, soziale Medien, Foren und Blogs. Erfasst ist die Erhebung personenbezogener Daten aus unternehmensexternen Quellen zum Training oder Fine-Tuning generativer Modelle, gleich ob selbst gescrapt, an einen Dienstleister vergeben oder als fertiger Datensatz übernommen. Ausgeklammert bleiben reine Datenhändler, die Datensätze nur vorhalten, die Verarbeitung eigener Bestandsdaten und öffentliche Stellen; datenschutzrechtlich irrelevant sind diese Fälle damit nicht.

Zweckbindung, Transparenz, Datenminimierung, Richtigkeit

Die Leitlinien arbeiten die Pflichten an den Grundsätzen ab:

- **Zweckbindung:** Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht für unvereinbare Zwecke weiterverarbeitet werden.

- **Transparenz:** Je nach Ausgestaltung kann die Einzelinformation nach Art. 14 Abs. 5 lit. b DSGVO entfallen, wenn sie unmöglich oder unverhältnismäßig aufwendig ist. Darauf soll sich außerhalb von Forschungs-, Archiv- oder Statistikzwecken nicht routinemäßig gestützt werden. Die Angaben nach Art. 14 Abs. 1 und 2 DSGVO sind dann öffentlich zugänglich zu machen, mit präziser Quellenangabe. Als gute Praxis gelten Domainnamen und URLs in durchsuchbarer Form sowie der Erhebungszeitraum.

- **Datenminimierung:** Der EDPB empfiehlt vorab präzise Erhebungskriterien, eine Bestandsaufnahme, Filter für nicht benötigte Kategorien und den Ausschluss von Websites, die sich mit robots.txt, ai.txt oder CAPTCHA sperren; nach der Erhebung syntaxbasierte Filter, Anonymisierung oder Pseudonymisierung. Die Menge allein ist dagegen kein Verstoß: “the principle of data minimisation does not prohibit training an AI model or AI system with large volumes of data” (*EDPB, Guidelines 03/2026, Version 1.0*)

- **Richtigkeit:** Soweit möglich empfiehlt der EDPB, verlässliche Quellen zu wählen, einen Zeitstempel der Erhebung zu erfassen und eine Validierung vor dem KI-Training durchzuführen.

Rechtsgrundlage: Berechtigtes Interesse und Art. 9 DSGVO

Private Akteure stützen sich nach den Leitlinien häufig auf das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO. Dessen drei Voraussetzungen müssen kumulativ erfüllt sein: berechtigtes Interesse, Erforderlichkeit und eine Abwägung, bei der die Interessen oder Grundrechte der betroffenen Person nicht überwiegen. In die Abwägung lassen sich technische und organisatorische Maßnahmen einstellen, wie standardmäßiger Ausschluss bestimmter Datenkategorien oder Quellen, Beschränkung auf frei zugängliche Daten, mehr Transparenz, frühestmögliches Löschen oder Anonymisieren sowie Vorkehrungen gegen Memorierung, Wiedergabe und Angriffe auf das Modell.

Eine Einwilligung dürfte in der Regel ausscheiden, weil bei indirekter Massenerhebung kein direkter Kontakt zu den Betroffenen besteht; eine fehlende robots.txt ist keine Einwilligung: “the absence or non-applicability of a robots.txt file on a web site does not amount to consent within the meaning of the GDPR” (*EDPB, Guidelines 03/2026, Version 1.0*).

Für besondere Kategorien personenbezogener Daten gilt das Verarbeitungsverbot. Wer sie gezielt erheben will, braucht neben einer Rechtsgrundlage nach Art. 6 DSGVO eine Ausnahme nach Art. 9 Abs. 2 DSGVO. Für die beiläufige und restliche Erfassung trotz Gegenmaßnahmen kann nach Auffassung des EDPB die Suchmaschinen-Rechtsprechung des EuGH (C-136/17) relevant sein – aber nur unter vergleichbaren Umständen und nicht als generelle Ausnahme. Das Verbot gilt dann nur im Rahmen der Verantwortlichkeiten, Befugnisse und Möglichkeiten des Verantwortlichen; der EDPB verlangt dafür mindestens Filter vor der Erhebung, sofortiges Löschen danach und Schutz gegen die Extraktion solcher Daten aus dem Modell.

Praxisfolgen

- **Quellen kartieren:** Erfassen und dokumentieren Sie, welche Quellen Sie und Ihre Dienstleister tatsächlich heranziehen — die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO entfällt nicht, weil die Datenmengen unübersichtlich sind.

- **Rollen klären:** Ob Datensammler und Modellentwickler getrennt oder gemeinsam verantwortlich oder Auftragsverarbeiter sind, bemisst sich nach den tatsächlichen Umständen, nicht nach der formalen Bezeichnung im Vertrag.

- **Sperren respektieren:** Der EDPB empfiehlt, Websites auszunehmen, die sich mit robots.txt, ai.txt oder CAPTCHA gegen das Auslesen sperren.

- **Transparenz schaffen:** Fehlt die Möglichkeit der Einzelinformation, müssen die Angaben nach Art. 14 Abs. 1 und 2 DSGVO öffentlich zugänglich sein, darunter Zweck, Rechtsgrundlage, Datenkategorien, eine präzise Angabe der Quellen und Kontaktdaten.

- **Art. 9 DSGVO prüfen:** Wer besondere Kategorien gezielt erhebt, braucht zusätzlich eine Ausnahme nach Art. 9 Abs. 2 DSGVO. Für die ungewollte Miterfassung erwartet der EDPB Filter vor der Erhebung, sofortiges Löschen und Ausgabefilter am Modell – und dass Sie deren Wirksamkeit nachweisen können.

EDPB: Leitlinie zur Anonymisierung

Am 7. Juli 2026 hat der Europäische Datenschutzausschuss (EDPB) die Leitlinien 02/2026 zur Anonymisierung in Version 1.0 verabschiedet und in die öffentliche Konsultation gegeben. Sie lösen die Stellungnahme 05/2014 der Artikel-29-Datenschutzgruppe ab und tragen der EuGH-Rechtsprechung, neuen EU-Datenräumen und den Fortschritten bei KI Rechnung. Im Kern geht es um die Frage, an der viele Datenprojekte hängen: Wann sind Daten so weit entkleidet, dass die DSGVO nicht mehr greift? Anonyme Daten fallen nicht in den Anwendungsbereich der DSGVO *(Art. 2 Abs. 1 DSGVO, Erwägungsgrund 26*) — ein Freiheitsgewinn, der nur trägt, wenn die Anonymisierung hält.

Anonymität gilt je nach Betrachter

Ob Informationen personenbezogen sind, lässt sich nicht allein am Datensatz ablesen. Dieselben Angaben können für einen Empfänger anonym und für einen anderen personenbezogen sein, wenn nur dieser sie einer Person zuordnen kann. Die Leitlinien empfehlen deshalb, die Anonymität aus der Sicht jeder betreffenden Stelle zu beurteilen. Der Bezug zu einer Person kann sich aus dem Inhalt, dem Zweck oder der Wirkung der Information ergeben; er muss nicht ohne Weiteres erkennbar sein und kann sich erst durch weitere Verarbeitung zeigen. Verarbeitet eine Stelle im Auftrag eines Verantwortlichen, gilt für sie dessen Perspektive. Ein unabhängiges Forschungsinstitut dagegen, das von einem Krankenhaus Auszüge aus Patientenakten erhält und diese eigenverantwortlich auswertet und nie an das Krankenhaus zurückgibt, wird nach eigener Sicht beurteilt.

Drei Kriterien, zwei Prüfwege

Für die technische Prüfung nennt der EDPB drei Kriterien. Sind alle drei erfüllt, können die Daten als anonym gelten. Ist eines verletzt, sind die Daten damit nicht automatisch personenbezogen – dann ist weiter zu prüfen.

- **Keine Isolierung einzelner Datensätze (No Record Isolation):** Die Daten enthalten keine einmalige Kombination von Merkmalen, die sich auf eine einzelne Person bezieht, wie etwa Geschlecht, Geburtsdatum und Postleitzahl, die zusammen nur auf einen Patienten passen.

- **Keine Verknüpfung (No Linkage):** Kein Datensatz lässt sich mit einem Datensatz aus einer anderen Quelle verbinden, der sicher oder sehr wahrscheinlich dieselbe Person betrifft. Das lässt sich nur mit Blick auf andere verfügbare Datenbestände prüfen.

- **Keine Rückschlüsse (No Inference):** Aus den Daten lässt sich nichts Bestimmtes und Erhebliches über eine einzelne Person ableiten. Insbesondere nichts, was ihre Rechte und Interessen berühren kann und sich nicht schon aus allgemeinem Wissen ergibt.

Ist ein Kriterium verletzt, kommt es auf die Folge an: Lässt sich eine Person über ihren einmaligen Datensatz tatsächlich herausgreifen oder macht eine Verknüpfung sie identifizierbar, sind die Daten personenbezogen. Andernfalls können sie trotzdem anonym sein.

Angewandt werden die Kriterien auf zwei Wegen. Der **kontextbezogene Ansatz** fragt, welche Mittel die jeweils betreffenden Stellen nach allgemeinem Ermessen wahrscheinlich nutzen. Er ist genauer, aber aufwendig, und wer eine Stelle übersieht, hält Daten womöglich zu Unrecht für anonym. Der **vereinfachte Ansatz** blendet diese Unterschiede aus. Er ist kein eigener rechtlicher Maßstab, sondern bewusst vorsichtiger: Daten können dabei als personenbezogen behandelt werden, obwohl sie anonym wären. Beide lassen sich verbinden, etwa mit dem vereinfachten Ansatz beginnen und kontextbezogen weiterprüfen, wenn er Identifizierungsmöglichkeiten zeigt.

Wer re-identifizieren kann

Maßgeblich ist nicht technische Unmöglichkeit, sondern ob die Identifizierung mit Mitteln gelingt, die nach allgemeinem Ermessen wahrscheinlich genutzt werden. Dieser Begriff ist weit: Er erfasst auch Mittel, die nur über einen Dritten zugänglich sind, und den Fall, dass eine Stelle sie über einen Dienstleister einkauft. Je nach Umständen können dazu unter anderem gehören: der Verantwortliche, Empfänger der Daten, unredliche Beschäftigte, Partner, Freunde, Kollegen und Nachbarn, investigative Journalisten, inländische Strafverfolgungsbehörden und Nachrichtendienste, ausländische Nachrichtendienste, unethische Unternehmen sowie Cyberkriminelle. Auf fehlende Motivation der Beteiligten lässt sich nicht bauen: Sie ist schwer objektiv zu belegen und kann sich ändern. Die Wahrscheinlichkeit einer Identifizierung muss nicht null sein, sie muss in der Praxis unerheblich bleiben: „the likelihood of the individual being successfully distinguished from others within the given context does not need to be zero; instead, that likelihood should be insignificant in reality“ (*EDPB, Guidelines 02/2026, Rn. 22*).

Praxisfolgen

- **Relevante Perspektiven zuerst festlegen:** Vor jeder technischen Bewertung muss feststehen, für wen die Daten anonym sein sollen — für die eigene Nutzung, für Empfänger oder für jeden, der Zugang erhält. Daraus ergibt sich, welche Fähigkeiten einzubeziehen sind.

- **Vereinfachten Ansatz als Puffer erwägen:** Wer die kontextbezogene Prüfung scheut, kann den vereinfachten Ansatz wählen; er kann über den rechtlichen Maßstab hinausgehen, gibt dafür größere Sicherheit und lässt sich mit der kontextbezogenen Bewertung verbinden.

- **Altfälle nicht neu aufrollen:** Wer einen Datensatz vor Veröffentlichung der Leitlinien nach der Stellungnahme 05/2014 als anonym bewertet hat, muss nach Auffassung des EDPB nicht neu prüfen. Eine regelmäßige Nachprüfung der Re-Identifikationsrisiken bleibt gleichwohl gute Praxis.

EU-Kommission: Erster harmonisierter Standard zur Umsetzung der KI-Verordnung

Die EU-Kommission hat am 14. Oktober 2026 den ersten harmonisierten Standard zur Umsetzung der KI-Verordnung im Amtsblatt der Europäischen Union veröffentlicht. Es handelt sich um die EN 18286:2026 – Artificial intelligence – Quality management system for EU AI Act regulatory purposes, die von CEN und CENELEC erarbeitet wurde. Der Standard übersetzt die Anforderungen an ein Qualitätsmanagementsystem (QMS) nach Art. 17 der KI-Verordnung in ein operatives QMS. Für Anbieter von Hochrisiko-KI-Systemen ist die Umsetzung des Standards von erheblichem Vorteil: Nach dem Durchführungsbeschluss (EU) 2026/2274 vom 12. Oktober 2026 wird für diejenigen, die den Standard umsetzen, die Konformität mit den davon erfassten Anforderungen des Art. 17 vermutet. Weitere harmonisierte Standards sollen folgen.

Rechtswirkung: Konformitätsvermutung nach Art. 40

Die Vermutungswirkung folgt aus Art. 40 der KI-Verordnung. Danach wird die Konformität mit den einschlägigen Anforderungen vermutet, wenn ein Hochrisiko-KI-System mit harmonisierten Normen übereinstimmt, deren Fundstellen im Amtsblatt veröffentlicht wurden. Der Standard selbst liegt bereits seit dem Sommer 2026 vor; die Vermutung greift jedoch erst seit der Veröffentlichung der Fundstelle am 14. Oktober 2026. Die Anwendung der Norm bleibt freiwillig. Die Vermutung erstreckt sich zudem nur auf die Anforderungen, die der Standard tatsächlich abdeckt. Wer einen anderen Weg wählt oder Anforderungen des Art. 17 nicht vom Standard erfasst sieht, muss die Eignung seines QMS gegebenenfalls auf andere Weise nachweisen.

Aufbau statt Ersatz

Der Standard orientiert sich am Lebenszyklus des KI-Systems und nicht an der Organisation. Er soll bestehende internationale Standards nicht ersetzen, sondern auf ihnen aufsetzen, etwa auf ISO/IEC 42001, ISO 9001 oder einem sektoralen QMS wie ISO 13485. Anbietern in regulierten Sektoren erlaubt der Standard ausdrücklich, ihre Managementsysteme zusammenzuführen, statt sie getrennt zu betreiben. Dadurch lassen sich Governance, Dokumentation und Qualitätssicherung einheitlich steuern, anstatt sie in getrennten Compliance-Projekten zu bearbeiten.

Anforderungen des Art. 17 KI-VO

Art. 17 Abs. 1 KI-VO verlangt, dass Anbieter von Hochrisiko-KI-Systemen ein QMS einrichten, das die Einhaltung der Verordnung gewährleistet. Das System ist systematisch und ordnungsgemäß in Form schriftlicher Regeln, Verfahren und Anweisungen zu dokumentieren. Dazu gehören unter anderem ein Konzept zur Regelungseinhaltung sowie Verfahren für Entwurf, Entwicklung, Qualitätskontrolle, Test und Validierung. Die EN 18286 konkretisiert diese Vorgaben insbesondere in den Bereichen Governance, Lebenszyklussteuerung, Dokumentation, Tests und Beobachtung nach dem Inverkehrbringen.

Praxisfolgen

- **Betroffenheit prüfen:** Fallen Sie als Anbieter eines Hochrisiko-KI-Systems unter die Pflichten des Art. 17 KI-VO? Die Pflicht zur Einrichtung eines QMS trifft Anbieter, nicht ohne Weiteres Betreiber.
- **Status quo prüfen:** Welche Standards werden bereits umgesetzt, und welche Lücken bestehen im Vergleich zu den Anforderungen der EN 18286?
- **Neuen Standard umsetzen:** Und gegebenenfalls mit bestehenden Systemen wie ISO/IEC 42001, ISO 9001 oder ISO 13485 verbinden.
- **Abdeckung dokumentieren:** Die Vermutungswirkung reicht nur so weit, wie der Standard die Anforderungen abdeckt. Für nicht erfasste Teile des Art. 17 sollte der Nachweis auf anderem Weg geführt werden.
- **Weitere Standards beobachten:** Folgende harmonisierte Standards können die Vermutungswirkung auf weitere Anforderungen erweitern.

Ihr Ansprechpartner



Dr. Michael Rath
Rechtsanwalt, Certified Information Privacy Professional/Europe (CIPP/E) | Partner
Fachanwalt für IT-Recht Certified ISO/IEC 27001 Lead Auditor
Köln
+49 221 9937 25795
michael.rath@luther-lawfirm.com

Stand: November 2026