LOSCHELDER

Newsletter Datenschutzrecht

März 2026

Sehr geehrte Damen und Herren,

mit dem Frühling ziehen auch neue spannende Themen rund um Datenschutz und die Digitalregulierung ein.

Wir beginnen mit einem absoluten Evergreen, der in der Praxis regelmäßig zu erheblichen Herausforderungen führt: Der Auskunftsanspruch nach Art. 15 DSGVO. Eine weitere BGH-Entscheidung verleiht diesem klarere Konturen. Besonders interessant an dieser Stelle: Die EU-Kommission schlägt mit ihrem Digital Omnibus auch Änderungen am Auskunftsrecht nach Art. 15 DSGVO vor: Auskunftsansprüche sollen als missbräuchlich zurückgewiesen werden können, wenn mit ihnen datenschutzrechtswidrige Zwecke verfolgt werden, etwa den Abfindungsanspruch nach Kündigung in die Höhe zu treiben oder anderweitig dem Verantwortlichen zu schaden.

Darüber hinaus bringen wir Ihnen Hilfestellungen aus den Behörden mit, zum rechtssicheren KI-Einsatz und für die Interessensabwägung bei Rückgriff auf die Erlaubnisgrundlage der berechtigten Interessen. Bevor wir in unserem „Zu guter Letzt“ wieder den Blick auf einige brisante Bußgeldentscheidungen richten, fassen wir Ihnen zudem den aktuellen Stand der Entwicklungen im IT-Sicherheitsrecht zusammen: Hier tut sich derzeit viel, mit dem Ablaufen der Registrierungspflicht unter BSIG (NIS-2-Richtlinie), dem in Kraft treten des KRITIS-Dachgesetzes und der aktuellen Diskussion rund um das Durchführungsgesetz zum Cyber Resilience Act.

Inhalt

Nicht alles hat Personenbezug – Grenzen des Auskunftsanspruchs nach Art. 15 DSGVO

Ein Versicherungsnehmer verlangte von seiner privaten Krankenversicherung sämtliche Tarifinformationen der vergangenen zehn Jahre. Rechtliche Grundlage war der Auskunftsanspruch nach Art. 15 DSGVO. Kernfrage: Handelt es sich bei den Tarifinformationen um personenbezogene Daten? Nur dann würde sich auch der Auskunftsanspruch darauf beziehen. Der BGH bringt mit seinem Urteil einen weiteren Mosaikstein im Ringen um die korrekten Konturen des Auskunftsanspruchs – ganz unabhängig von der derzeit diskutierten Anpassung im Rahmen des Digital Omnibus.

Werden personenbezogene Daten verarbeitet, haben Betroffene einen Auskunftsanspruch nach Art. 15 Abs. 1 DSGVO, der vom Anspruch auf „Kopie" gem. Absatz 3 der Norm begleitet wird. Erfasst sind von vornherein nur personenbezogene Daten, also Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Und genau an diesem Punkt führt eine aktuelle Entscheidung des BGH im Versicherungssektor – erneut – zu einer wesentlichen Klarstellung der Konturen des Auskunftsanspruchs nach Art. 15 DSGVO.

In dem vom BGH entschiedenen Fall (BGH, Urteil vom 18.12.2025 – I ZR 115/25) forderte ein Versicherungsnehmer sämtliche Daten über Zeitpunkt und Höhe aller Beitragsanpassungen, Tarifwechsel und Tarifbeendigungen aus über zehn Jahren – ihm selbst seien die Daten verloren gegangen. Im Kern geht es damit um die Frage, ob es sich bei diesen Tarifdaten um personenbezogene Daten handelt. Wann Daten personenbezogen sind, ist immer wieder Gegenstand gerichtlicher Streitigkeiten, wie wir im Kontext von pseudonymisierten Daten in der letzten Ausgabe berichtet haben.

Das LG Leipzig hatte dem Kläger im April 2025 einen umfassenden Auskunftsanspruch bestätigt. Der BGH sieht dies nun anders: Im Gegensatz zum LG Leipzig geht der BGH nicht davon aus, dass es sich bei sämtlichen Tarifdaten um personenbezogene Daten handelt.

Alles personenbezogene Daten?

Der Begriff der personenbezogenen Daten ist grundsätzlich weit auszulegen. Alle Informationen, die aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft sind, werden von dem Begriff erfasst.

Daher sind beispielsweise Schreiben des Versicherungsnehmers an den Versicherer regelmäßig als personenbezogene Daten einzuordnen. Komplizierter wird es schon bei Schreiben des Versicherers an den Versicherungsnehmer. Interne Vermerke hatte der BGH bereits vor einiger Zeit als rein rechtlich und nicht personenbezogen qualifiziert (vgl. BGH, Urteil vom 05.03.2024 – VI ZR 330/21).

Streit in der obergerichtlichen Rechtsprechung

Ob Angaben zu Beitragsanpassungen und Tarifwechseln oder Tarifbeendigungen personenbezogene Daten sind, war in der obergerichtlichen Rechtsprechung umstritten.

Einige Oberlandesgerichte urteilten, dass es sich um personenbezogene Daten handelt. Argumentiert wurde folgendermaßen:

- Aus den Daten ergebe sich, mit welchem Inhalt und zu welchen Konditionen ein Tarif bestehe.
- Beitragsanpassungen seien individuell auf den einzelnen Versicherungsnehmer zugeschnitten und damit personenbezogene Daten.
- Zum Teil wurden auch Schreiben über allgemeine Prämienzahlungen als personenbezogene Daten eingestuft, weil sie Auswirkungen auf das individuelle Versicherungsverhältnis haben.

Die Individualisierung der Daten sowie deren Bedeutung für das jeweilige Versicherungsverhältnis begründete demnach bereits den Personenbezug.

Andere Oberlandesgerichte kamen zur gegenteiligen Einschätzung.

- Sie verneinten einen Personenbezug mit der Begründung, dass die Daten keine Rückschlüsse auf die Identität der betroffenen Person zuließen und damit nicht als personenbezogene Daten einzustufen sind.
- Tariferhöhungen seien nur das Ergebnis einer anhand bestimmter Parameter vorgenommenen Preisberechnung und geben gerade nicht Aufschluss über den individualisierten Versicherungsschutz oder ähnliches.

Dieser letzten Ansicht hat sich der BGH nun angeschlossen. Entscheidend sei, ob die Informationen eine Identifizierung der betroffenen Person ermöglichen. Angaben zu dem Versicherungstarif seien zunächst „neutrale“ Daten, die erst durch zusätzliche Informationen einen Personenbezug erhalten. Es sei gerade nicht ausreichend, dass Informationen lediglich Auswirkungen auf das individuelle Versicherungsverhältnis haben.

Ob die fraglichen Daten eine Identifizierung des Klägers ermöglichen, sei durch das LG Leipzig nicht festgestellt worden und müsse nun erneut geprüft werden. Ob der Kläger letztlich Auskunft über die begehrten Tarifinformationen bekommt, hängt davon ab, ob diese bereits alleine eine Identifizierung seiner Person ermöglichen. Auf eine Vorlage zum EuGH hat der BGH verzichtet, die Auslegung des Unionsrechts sei bereits geklärt und zweifelsfrei zu beantworten.

Auskunftsanspruch auch zu datenschutzfremden Zwecken

Das Versicherungsunternehmen vertrat zudem die Ansicht, dass der Auskunftsanspruch nach Art. 15 DSGVO nicht zu datenschutzfremden Zwecken eingesetzt werden dürfe. Da der Kläger mit den begehrten Daten einen Rückforderungsprozess vorbereiten wollte und kein datenschutzrechtliches Interesse verfolge, könne er den Auskunftsanspruch nicht geltend machen.

Dieser Argumentation hat der BGH widersprochen. Das Bestehen des Anspruchs sei nicht abhängig von der Motivation des Klägers. Ziel der Geltendmachung muss nicht die Überprüfung der Rechtmäßigkeit der Datenverarbeitung sein, sondern kann auch anderen Zwecken dienen.

Bei offenkundig unbegründeten oder exzessiven Anträgen kann der Verantwortliche die Auskunft jedoch verweigern oder zur Bearbeitung ein Entgelt verlangen (Art. 12 Abs. 5 Satz 2 DSGVO). Der Anspruch erfährt so eine Begrenzung.

Neue Vorschläge der EU-Kommission

Aus Praxissicht zu begrüßen sind angesichts dessen auch die von der EU-Kommission vorgeschlagenen Klarstellungen, wann von einem missbräuchlichen Antrag auszugehen ist: Im Rahmen des Digital Omnibus mit Änderungsvorschlägen an der DSGVO hat die EU-Kommission vorgeschlagen, die Regelung in Art. 12 Abs. 5 zu konkretisieren (COM(2025) 937 final): Ein Verweigerungsrecht soll auch

dann bestehen, „*wenn die betroffene Person die ihr durch diese Verordnung verliehenen Rechte zu anderen Zwecken als dem Schutz ihrer Daten missbraucht*“. Das soll nach Erwägungsgrund 35 des Änderungsvorschlags etwa dann der Fall sein, wenn

- die betroffene Person mit dem Auskunftsantrag eigentlich eine Entschädigungszahlung bezweckt (in der Praxis häufig anzutreffen im Rahmen von arbeitsrechtlichen Streitigkeiten),

- eine betroffene Person übermäßig von ihrem Auskunftsrecht Gebrauch macht mit der alleinigen Absicht, dem Verantwortlichen einen Schaden zuzufügen,

- oder wenn eine Einzelperson ein Verlangen stellt und gleichzeitig anbietet, dieses gegen eine bestimmte Form der Vorteilgewährung seitens des Verantwortlichen zurückzuziehen.

Diese Konkretisierungen werden in der Praxis helfen, missbräuchliche Auskunftsansprüche einzudämmen, wenn sie das EU-Verordnungsgebungsverfahren so passieren sollten. Datenschutzrechtlich überzeugend bleiben dabei indes Auskunftsansprüche dann berechtigt, wenn sie (auch) andere Zwecke verfolgen, solange diese legitim sind.

Unzulässiger Einsatz von Tracking Tools durch Meta

Das OLG München hat am 18.12.2025 gleich mit zwei Entscheidungen zum in der Praxis weit verbreiteten Einsatz von Tracking Tools durch Meta geurteilt. Das Gericht spricht in beiden Fällen den Klägern einen Schadensersatz von einigen hundert Euro zu und erklärt den Einsatz der „Meta Business Tools" in den entschiedenen Fällen für unzulässig. Weitere Entscheidungen folgen; etwa hat das OLG Dresden mit vergleichbarer Argumentation am 03.02.2026 in mehreren Parallelverfahren und das OLG Jena am 02.03.2026 in einem weiteren Verfahren vierstellige Schadensersatzansprüche zugesprochen.

Das Geschäftsmodell von Meta beruht auf personalisierter Werbung. Um diese zu ermöglichen, setzt Meta sogenannte Business Tools ein, die Daten zu den Nutzern der Plattformen speichern und sammeln. Auch viele Webseitenbetreiber machen sich dies im Online-Marketing zunutze und profitieren in ihrer Werbung gemeinsam mit Meta von einer gezielten, personalisierten Ansprache. Verwendet werden dafür auch sensible Daten wie beispielsweise Angaben zur politischen Haltung, biometrische sowie gesundheitsbezogene Daten. Die Informationen stammen von der Nutzung der Plattformen von Meta selbst und zudem von Drittseiten, sog. Offsite-Daten.

Gegen dieses Vorgehen stehen mehrere Gerichtsverfahren an, von denen einige schon durch Landgerichte entschieden wurden. Das OLG München hat mit seinen Entscheidungen (OLG München, Urteil vom 18.12.2025 – 14 U 2300/25 e und 14 U 1314/25 e) nun erste obergerichtlichen Urteile gefällt. In beiden Fällen klagten Privatpersonen, die sich gegen die Datenverarbeitung durch Meta wehrten. Weitere Entscheidungen folgen; etwa haben das OLG Dresden und das OLG Jena jüngst mit entsprechender Argumentation Schadensersatzansprüche in vierstelliger Höhe zugesprochen (OLG Dresden, Urteil vom 03.02.2026 – 4 U 292/25, 4 U 293/25, 4 U 296/25; OLG Jena, Urteil vom 02.03.2026 – 3 U 31/25).

Um personenbezogene Daten zu sammeln, die auf Seiten von Drittanbietern entstehen, bietet Meta sogenannte Business Tools an. Besucht ein Meta-Nutzer einen Online-Shop, in dem Meta-Business-Tools implementiert sind, erfasst Meta Informationen über angesehene Produkte, Kaufabsichten oder Suchverläufe – auch wenn der Nutzer zu diesem Zeitpunkt nicht in seinen Meta-Account eingeloggt ist. Zwar kann ein Nutzer durch Datenschutzeinstellungen von

Meta verhindern, dass die gesammelten Daten für personalisierte Werbung genutzt werden. Er kann jedoch nicht verhindern, dass die Daten überhaupt gesammelt werden.

Keine Rechtfertigung für die Datenverarbeitung

Das OLG München führt in den Urteilen aus, dass für die Verarbeitung der durch die Business Tools gewonnenen Daten in den beiden entschiedenen Fällen keine Rechtfertigung im Sinne der DSGVO besteht (Art. 6 Abs. 1 DSGVO). Die Klägerinnen hätten in die Datenverarbeitung weder eingewilligt, noch sei sie für die Erfüllung des Nutzungsvertrags zwischen Meta und den Nutzern zwingend erforderlich. Auch könne aufgrund der zurückhaltenden Ausführungen von Meta bezüglich des genauen Zwecks der Datenerhebung nicht angenommen werden, dass die Verarbeitung auf einem berechtigten Interesse im Sinne der DSGVO beruhe.

Die Urteile setzen dabei an die Weiterverarbeitung der Daten nach ihrer Erhebung auf den Drittseiten an. Für diese ist es üblich, im Wege der sog. „Cookie-Banner" Einwilligungen einzuholen, auch nach ePrivacy-Recht (§ 25 TDDDG). Diese Einwilligungen aber würde, unabhängig von ihrer Wirksamkeit, nur die Erhebung auf den Drittseiten betreffen, nicht aber ihre Kumulation bei Meta. Denn durch das Zusammenführen diverser Daten bei Meta entstehe ein umfassendes Persönlichkeitsprofil und damit ein darüberhinausgehender Informationsgewinn, zu dem jedenfalls in den entschiedenen Fällen keine Einwilligung erteilt worden sei.

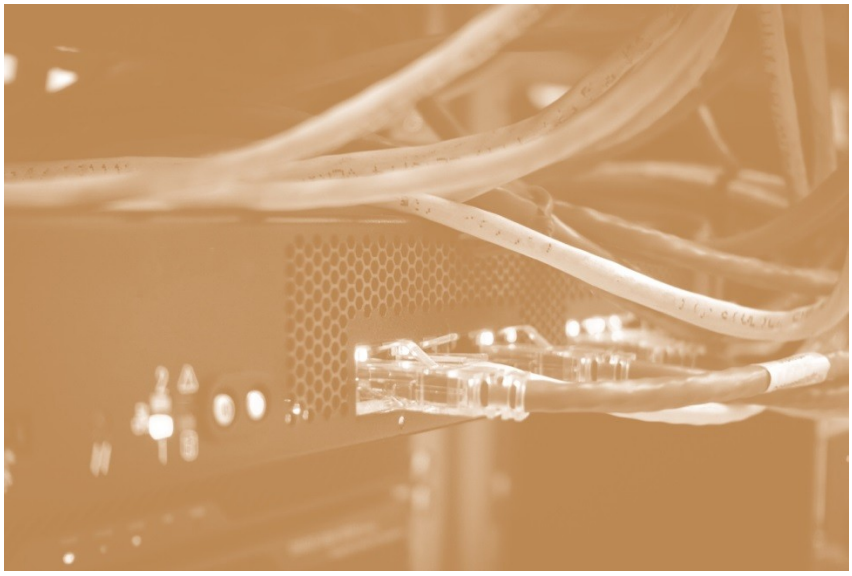
Hintergrund und Auswirkungen auf Websitebetreiber

Auslöser dieser Verfahren ist das EuGH-Urteil C-252/21 aus dem Jahr 2023. Der EuGH hatte in dieser Entscheidung die Zulässigkeit der Datenverarbeitung durch Meta nach der DSGVO geprüft und war zu dem Ergebnis gekommen, dass die Voraussetzungen für eine wirksame Rechtsgrundlage eng gefasst seien. In der Folge gingen zahlreiche Klagen bei Landgerichten ein, von denen einige bereits entschieden wurden und Betroffenen ein Anspruch auf Schadensersatz zugesprochen wurde.

Im Fokus der Verfahren stehen die umfassenden Datenverarbeitungspraktiken durch Meta, weniger die Drittseitenbetreiber, die Meta Business Tools implementiert haben. Auch auf diese können

sich die Verfahren indes auswirken, da bei einer unzulässigen Weiterverarbeitung womöglich auch die Erhebung selbst infiltriert wird und damit, wenn ihr notwendiger Zweck die Weiterleitung an Meta und dortige Zusammenführung zu umfassenderen Profilen ist.

Webseitenanbieter sollten die weitere Entwicklung im Auge behalten und rechtszeitig auf den Einsatz von Meta Business Tools verzichten. Bis dahin ist es in jedem Fall elementar, diese Tools nur mit Einwilligung der Webseitenbesucher zu aktivieren.



Handreichung der BfDI: KI-Systeme datenschutzkonform einsetzen

Beim Einsatz von KI-Systemen werden personenbezogene Daten verarbeitet. Für Unternehmen stellt sich die Frage, wie KI datenschutzkonform genutzt werden kann und was dafür zu beachten ist. Die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) hat eine Handreichung zum datenschutzkonformen Einsatz von KI in der Bundesverwaltung veröffentlicht, die auch für Unternehmen hilfreiche Informationen enthält.

Die von der BfDI veröffentlichte Handreichung über den datenschutzkonformen Einsatz und Training von KI-Systemen ist unmittelbar an die öffentliche Verwaltung adressiert. Sie kann jedoch auch für Unternehmen als Richtschnur zum rechtssicheren Einsatz von KI dienen.

Datenschutzrechtliche Herausforderungen von KI

Große Sprachmodelle (Large Language Models, kurz: LLM) wie ChatGPT oder Gemini werden mit kuratierten Trainingsdaten trainiert, auf deren Basis das System lernt, wie es sich verhalten muss. Aufgrund dieser Trainingsdaten wird ein neuronales Netz gebildet, mit dem das Modell operiert.

Hierbei ergeben sich verschiedene datenschutzrechtliche Herausforderungen, die in der Handreichung Berücksichtigung finden.

- **Black-Box-Charakter**: Der Output eines LLM ist aufgrund der besonderen Architektur nicht ohne Weiteres nachvollziehbar. Problematisch erscheint dies insbesondere bei der Umsetzung von Betroffenenrechten (Auskunftsanspruch, Recht auf Löschung oder Berichtigung). Da die Informationen als statistische Muster oder Wahrscheinlichkeiten in das Modell eingewoben sind, ist es schwierig, diese zu identifizieren, zu ändern oder zu entfernen.

- **Halluzinationen**: Trainingsdaten, auf denen das KI-Modell beruht, können fehlerhafte Informationen enthalten. Daraus ergibt sich eine Herausforderung für den Grundsatz der Datenrichtigkeit, der in Art. 5 Abs. 1 lit. D DSGVO verankert ist.

- **Erinnerung (Memorisierung) personenbezogener Daten**: Das Training von KI-Modellen erfolgt oftmals (auch) mit personenbezogenen Daten. Diese können unabsichtlich, aber auch durch gezielte Attacken, im Output des Modells enthalten sein. Zudem besteht die Gefahr, dass aufgrund der Zusammenführung personenbezogener Daten Rückschlüsse auf sensible Daten (wie z.B. auf politische Haltung oder Gesundheitsdaten) gezogen werden können. Die Verarbeitung von sensiblen Daten ist nur in eng begrenzten Fällen zulässig.

- **Voreingenommenheit**: Daten, mit denen das LLM trainiert wird, können einen Bias bzw. eine Voreingenommenheit aufweisen. Dies könnte im Konflikt mit dem Grundsatz von Treu und Glauben stehen (Art. 5 Abs. 1 lit. a DSGVO).

- **KI-Bereitstellung**: Bei der Bereitstellung eines KI-Modells können mehrere Dienstleister beteiligt sein. Hier ergeben sich

gegebenenfalls Fragen hinsichtlich der datenschutzrechtlichen Verantwortlichkeit oder der Auftragsverarbeitung.

- **Datenübermittlung in Drittländer**: LLMs werden häufig außerhalb der EU gehostet oder es erfolgen Zugriffe von Drittstaaten auf in der EU gehostete KI-Systeme mit Modellen von Anbietern aus diesen Drittstaaten. Dadurch entstehen Risiken u.a. von staatlichen Zugriffen auf die übermittelten oder gespeicherten Daten oder auch Erschwernisse bei der Durchsetzung von Betroffenenrechten, etwa Löschungsansprüchen nach der DSGVO.

Empfehlungen der Handreichung

Bei der Bewältigung dieser und weiterer Herausforderungen bietet die Handreichung des BfDI Orientierung zum rechtssicheren Einsatz von KI-Systemen.

Unter anderem wird empfohlen:

- Bei der Auswahl von Anbietern sollte berücksichtigt werden, ob diese europäische Rechenzentren nutzen.
- Dem Bias sollte durch anerkannte Methoden gezielt entgegengewirkt werden.
- Personenbezogene Daten sollten anonymisiert oder pseudonymisiert werden.
- Es sollten, wo möglich, kleinere Sprachmodelle verwendet werden, um das Risiko einer unabsichtlichen Memorisierung zu verringern.
- Es sollten regelmäßige Schwachstellenüberprüfungen durch simulierte Systemattacken durchgeführt werden.

Rechtssichere Datenverarbeitung auch bei Abwägungsentscheidungen

Die Verarbeitung von personenbezogenen Daten muss auf eine Rechtsgrundlage der DSGVO gestützt sein. In Betracht kommt dabei auch eine Interessenabwägung der Beteiligten. Diese Abwägung gestaltet sich jedoch mitunter als anspruchsvoll. Eine Veröffentlichung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit bietet eine erste Orientierung und erleichtert die erforderliche Dokumentation.

Kommt es zu der Verarbeitung personenbezogener Daten, müssen die Voraussetzungen der DSGVO erfüllt werden. Diese stellt mehrere Erlaubnistatbestände auf, unter deren Voraussetzungen eine Datenverarbeitung erfolgen kann. Neben der Einwilligung durch den Betroffenen kann die Datenverarbeitung unter anderem auch auf die Erfüllung eines Vertragsverhältnisses gestützt werden. Als letzte, aber nicht subsidiäre, Rechtsgrundlage kommt die Wahrung eines berechtigten Interesses des Datenverantwortlichen oder eines Dritten in Betracht (Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO). Die Anwendung dieser Rechtsgrundlage steht unter dem Vorbehalt, dass die Interessen oder Grundrechte bzw. Grundfreiheiten der durch die Datenverarbeitung betroffenen Person nicht überwiegen. Erforderlich ist daher eine Interessenabwägung. Die rechtssichere Durchführung ebendieser Interessenabwägung gestaltet sich jedoch

als herausfordernd und ist immer wieder Gegenstand rechtlicher Diskussionen.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat Anfang des Jahres einen Fragenkatalog veröffentlicht, der die Prüfung des Erlaubnistatbestands erleichtern soll. Auch kann er dazu dienen, die Interessenabwägung entsprechend den europäischen Vorgaben zu dokumentieren. Ausdrücklich handelt es sich dabei nicht um eine zweifelsfrei rechtssichere Prüfung. Es wird weiterhin eine qualifizierte Rechtsberatung empfohlen. Insbesondere in neuen oder komplizierten Fallkonstellationen können die durch den Fragebogen aufgeworfenen Aspekte unzureichend sein, um eine vollständige Prüfung vornehmen zu können.

Die Interessenabwägung als zentrale Stellschraube der DSGVO

Die Erlaubnisgrundlage aufgrund einer Interessenabwägung ist wertungsoffen und in ihrer Anwendung auch nach etlichen Urteilen nach wie vor mit Unsicherheiten behaftet. Die Leitlinien aus Hamburg helfen angesichts dessen bei der Anwendung und bringen insofern Rechtssicherheit: Der Fragenkatalog des Hamburgischen Datenschutzbeauftragten orientiert sich an dem etablierten dreistufigen Prüfungsverfahren (legitimer Zweck, Erforderlichkeit, Interessensabwägung) und basiert inhaltlich auf den Leitlinien des EDSA aus dem Jahr 2024 zur rechtskonformen Anwendung dieses Erlaubnistatbestands. Der Katalog soll der systematischen Prüfung des berechtigten Interesses und der Interessenabwägung in ihren wesentlichsten Punkten dienen.

Darüber hinaus kann mit einer Beantwortung der Fragen zugleich die für einen Rückgriff auf die Erlaubnisgrundlage der berechtigten Interessen notwendige Dokumentation einfacher gelingen.

Erklärtes Ziel ist es, mit dem Katalog für Praktikerinnen und Praktiker den Arbeitsalltag zu erleichtern und die Einschätzung der Zulässigkeit von Datenverarbeitungsvorgängen zu vereinfachen. Der Fragebogen soll zudem die Entscheidungsfindung der Hamburgischen Aufsichtsbehörde transparenter gestalten.

Aktuelle Entwicklungen im IT-Sicherheitsrecht

Die EU-Cyberstrategie kommt immer mehr zum Tragen: Am 06.03.2026 endete die Registrierungsfrist für NIS-2-Adressaten (Spoiler: rund 2/3 der adressierten Unternehmen haben sich dennoch noch nicht registriert), am 17.03.2026 ist das KRITIS-Dachgesetz in Kraft getreten und das Durchführungsgesetz zum Cyber Resilience Act ist vor Kurzem als Referentenentwurf vorgelegt worden. Anlass genug für ein aktuelles Update.

Die EU verschärft die Regulierung der Cybersicherheit, um die EU resilienter aufzustellen. Rund 30.000 Unternehmen werden von den Neuregelungen im BSIG erfasst, das in Umsetzung der NIS-2-Richtlinie novelliert wurde und seit wenigen Tagen umfassend greift. Für die knapp 5.000 KRITIS-Anlagenbetreiber in Deutschland gelten zudem ab dem 17.03.2026 die vornehmlich ergänzenden Anforderungen des KRITIS-Dachgesetzes, fokussiert auf die physische Sicherheit. Ab Herbst 2027 sind überdies digitale Produkte besonders sicher zu gestalten, im Einklang mit dem Cyber Resilience Act, zu dem aktuell das nationale Durchführungsgesetz beraten wird.

BSIG und NIS-2-Richtlinie

Zum 06.12.2025 ist das novellierte BSIG in Kraft getreten. Drei Monate später, am 06.03.2026, endete die Registrierungsfrist. Alle rund 30.000 erfassten Unternehmen müssten mithin nunmehr registriert

sein – laut Presseberichterstattung waren am 09.03.2026 aber nur rund 11.000 Unternehmen tatsächlich registriert.

Wichtig ist für all jene, die adressiert sind, aber die Registrierung noch nicht vorgenommen haben, dies nunmehr aktiv anzugehen. Es ist nicht zu erwarten, dass überschaubare Fristversäumnisse in Bußgeldverfahren enden, auch wenn dies theoretisch möglich wäre. Regulatorisch kritisch – mit Bußgeldrisiken – kann es aber dann werden, wenn die Registrierung ganz unterbleibt und erst etwa im Rahmen eines Cyberincidents offenbar wird, dass trotz Adressatenstellung Pflichten aus dem BSIG nicht eingehalten wurden.

Angesichts dessen sollten Unternehmen, soweit nicht bereits geschehen, sorgfältig ihre Betroffenheit prüfen und sich dann aktiv für oder – dokumentiert – gegen eine Registrierung entscheiden. Wir führen seit geraumer Zeit unzählige Betroffenheitsanalysen durch und sehen häufig, dass Unternehmen von einem -positiven – Ergebnis überrascht sind. Grund dafür ist die enorm weite Anwendbarkeit der Pflichten, die nicht nur auf kritische Infrastrukturen begrenzt sind und meist sogar schon dann greifen, wenn in einer Unternehmensgruppe ein IT-Shared Service für andere Gruppenunternehmen erbracht wird.

Unternehmen, die vom BSIG erfasst sind, müssen sich registrieren, erhebliche Sicherheitsvorfälle melden und nach § 38 Abs. 3 BSIG die Geschäftsleiter schulen: Ein erprobtes Schulungsprogramm bietet Loschelder etwa in Kooperation mit Wessing&Partner und der Bitkom Akademie an: NIS-2 Geschäftsleiterschulung nach aktuellen BSI-Empfehlungen | Bitkom Akademie

Materiell muss ein angemessenes Cyberrisikomanagement implementiert werden. Dies ist das Herzstück des BSIG – letztlich aber auch für nicht-BSIG-Adressaten verpflichtend, aus Art. 32 DSGVO für personenbezogene Daten und aufgrund der aktuellen Bedrohungslage als allgemeine Geschäftsführungspflicht zur Abwehr von Schäden von der eigenen Gesellschaft.

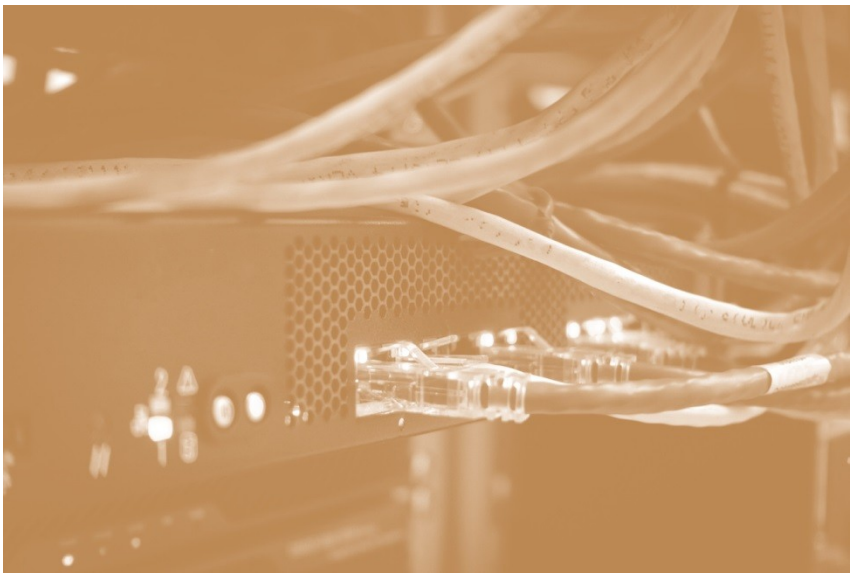
KRITIS-Dachgesetz und CER-Richtlinie

Ergänzend zur NIS-2-Richtlinie und dem BSIG ist am 17.03.2026 das KRITIS-Dachgesetz in Umsetzung der CER-Richtlinie in Kraft getreten. Das Gesetz fokussiert sich auf die physische Sicherheit kritischer Anlagen und ergänzt so das BSIG und die NIS-2-Richtlinie. KRITIS-

Betreiber müssen sich auch nach diesem Gesetz registrieren, Strategien zur Resilienz erarbeiten und umsetzen und Vorfälle melden.

Cyber Resilience Act

Komplettiert wird die neue IT-Sicherheitsregulierung ab Herbst 2027 mit spezifischen Sicherheitsvorgaben für digitale Produkte. Nach dem nun vorliegenden Referentenentwurf zur Durchführung des Cyber Resilience Act wird auch insofern das BSI (Bundesamt für die Sicherheit in der Informationstechnik) die zentrale Behörde in Deutschland werden. Angesichts der damit zu erreichenden Bündelung des Cybersachverstands in einer Behörde erscheint das folgerichtig. Der Referentenentwurf ist hier abrufbar.



Zu guter Letzt

Aus verschiedenen Anlässen erfolgten aufsichtsbehördliche Prüfungen mit teils erheblichen Bußgeldern unter anderem bei einem öffentlichen Verkehrsbetrieb in Stockholm, der Social-Media-Plattform X (vormals Twitter), dem französischen Telekommunikationsdienstleister „Free" sowie einem Krankenhausbetreiber in Spanien.

- **Öffentlicher Verkehrsbetrieb in Stockholm muss 1,4 Mio. Euro Bußgeld zahlen aufgrund des unzulässigen Einsatzes von Körperkameras im Rahmen einer Fahrscheinkontrolle**

Ein öffentlicher Verkehrsbetrieb in Stockholm stattete seine Fahrscheinkontrolleure mit Körperkameras aus, um anlässlich der Fahrkartenkontrolle die Fahrgäste zu filmen. Dies sollte zum Schutz der Arbeitnehmer erfolgen. Die schwedische Datenschutzbehörde sah darin eine Verletzung mehrerer DSGVO Bestimmungen. Insbesondere seien Fahrgäste nur unzureichend über die Aufnahmen unterrichtet worden.

Nachdem der Verkehrsbetrieb die Verletzung der Informationspflicht bestritten hatte, bat das mit dem Rechtsstreit befasste schwedische Gericht den EuGH (Urteil vom 18.12.2025 – C-422/23) um Auslegung der DSGVO. Dieser kam zu dem Schluss, dass die Aufnahme einer Person durch eine am Körper getragene Kamera eine Datenerhebung unmittelbar bei der betroffenen Person ist. Dies wirkt sich auf Informationspflichten aus, die ein Verantwortlicher erfüllen muss (es gilt dann Art. 13 DSGVO und nicht Art. 14 DSGVO).

Für erforderlich erachtet wurden ein Kurzhinweis vor Ort sowie vollständige Datenschutzhinweise auf einer Website oder in einer Informationsbroschüre. Dies entspricht dem üblichen Vorgehen bei einer Videoüberwachung.

- **Der französische Mobilfunkanbieter „Free Mobil" sowie die Muttergesellschaft „Free" müssen nach einer Datenpanne 42 Mio. Euro Bußgeld zahlen**

Im Oktober 2024 konnten durch einen Cyberangriff auf 24 Millionen Kundenverträge von „Free Mobil" und „Free" zugegriffen werden. Teil der Daten waren Adressen und auch IBAN-Nummern. Die französische Datenschutzbehörde CNIL veröffentlichte am 08.01.2026 ihre Bußgeldentscheidung, gestützt datenschutzrechtliche Versäumnisse, die den Cyberangriff begünstigt hätten. Kritisiert wurden

unzureichend gesicherte VPN-Zugänge sowie ineffektive Erkennungssysteme für Angriffe.

Zudem kritisierte die Behörde den Umgang mit Betroffenen, die nur unzureichend über das Datenleck informiert worden seien. Es sei aus den Kommunikationsmaßnahmen nicht klar geworden, welche Folgen der Cyberangriff für die Betroffenen hat und wie sie sich vor einem Missbrauch der Daten schützen können.

- **Zu frühe Löschung von Patientendaten verhindert die Erfüllung eines Auskunftsersuchens durch den Patienten – 1,2 Mio. Euro Bußgeld für Klinikbetreiber**

Der Betroffene hatte in einer Klinik für ein MRT eine CD mit vorangegangenen Untersuchungsergebnissen abgegeben. Vier Monate nach der Behandlung bat er um Aushändigung der MRT-Aufnahmen sowie der CD. Die Klinik teilte ihm jedoch mit, dass die Daten – wie im Untersuchungsvertrag festgelegt – nach einem Monat gelöscht wurden.

Die spanische Datenschutzbehörde hielt dies für unzulässig. Anders als der Klinikbetreiber argumentierte, handle es sich bei den MRT-Bildern um medizinische Dokumente, die in die Patientenakte hätten eingepflegt werden müssen. Es sei nicht ausreichend, dass die Auswertungsdaten des behandelnden Arztes in der Patientenakte verfügbar sind. Entsprechend sei eine ausreichend lange Speicherung der Daten erforderlich gewesen.

- **EU-Kommission erlässt 120 Mio. Euro Bußgeld gegen X (vormals Twitter) wegen Verstößen gegen den Digital Services Act**

In einer ersten Entscheidung über die Nichteinhaltung des Digital Services Act (DSA) hat die EU-Kommission eine Geldbuße in Höhe von 120 Mio. Euro gegen X verhängt. Bemängelt wurde die irreführende Gestaltung des „blauen Häkchens“, die mangelnde Transparenz des Werbeanzeigenarchivs und die Nichtgewährung des Zugriffs für Forschenden auf die öffentlich zugänglichen Daten von X. Ähnliches ist im Datenschutzrecht von der Gestaltung der Cookie Banner (Stichwort: Nudging) bekannt.

Die blauen Häkchen würden Nutzende darüber täuschen, dass es sich um verifizierte Konten handelt, obwohl sich diese durch ein monatliches Abo kaufen ließen. Zudem wurden Anfragen zum

Werbeanzeigenarchiv unnötig lang bearbeitet, sodass deren Sinn verfehlt werde. Auch würden entscheidende Informationen fehlen, sodass Rechte von Nutzenden verletzt werden. Zudem sei X durch den DSA verpflichtet, Forschenden öffentlich zugängliche Daten zur Verfügung zu stellen. Dies würde jedoch aufgrund der Ausgestaltung der AGBs von X verhindert.

Die EU-Kommission gewährte X eine Frist zum Aufsetzen eines Handlungsplans, der auf die Verstöße angemessen reagieren soll.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49 221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49 221 65065-200
simon.kohm@loschelder.de

Dennis Pethke, LL.M.
+49 221 65065-337
dennis.pethke@loschelder.de

Rebecca Moßner
+49 221 65065-337
rebecca.mossner@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de