„Weggeforscht“ – der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

7 / 2025
Juli 2025

Wie sicher ist sicher genug?

OVG NRW zu erforderlichen IT-Sicherheitsmaßnahmen im Sinne von Art. 32 DSGVO bei Datenübermittlungen

Die fabelhafte Welt der digitalen Dienste

Die Adressaten des Digital Services Act und ihre Bedeutung für Hochschulen und Forschungseinrichtungen

Einer für alle, alle gemeinsam oder jeder für sich?

Ein Überblick zur Diskussion um die Zentralisierung der Datenschutzaufsicht

Kurzbeitrag: Automatisierte Kontrollen als Gamechanger?

Datenschutzbehörden prüfen Websites vermehrt mithilfe automatisierter Tools auf ihre Datenschutzkonformität

Wie sicher ist sicher genug?

OVG NRW zu erforderlichen IT-Sicherheitsmaßnahmen im Sinne von Art. 32 DSGVO bei Datenübermittlungen

Von Johannes Müller, Münster

Bei der Verarbeitung personenbezogener Daten folgt aus der Datenschutz-Grundverordnung (DSGVO) die Pflicht, angemessene Sicherheitsmaßnahmen zu treffen. Welche Maßnahmen konkret zu ergreifen sind, hängt von den Umständen des Einzelfalls ab. Das Oberverwaltungsgericht Nordrhein-Westfalen (OVG NRW) hat sich in seinem Beschluss vom 20. Februar 2025 (Az. 16 B 288/23)[1] nun mit der Frage beschäftigt, welche Sicherheitsmaßnahmen eine Behörde ergreifen muss, um Daten DSGVO-konform zu übermitteln.

I. Angemessene Sicherheitsmaßnahmen in der DSGVO

Die Vorschriften der DSGVO beschränken sich nicht alleine darauf, die freie Verwendung personenbezogener Daten durch den Verantwortlichen zu beschränken (Art. 6 DSGVO). Der Verantwortliche, der über die Zwecke und Mittel der Datenverarbeitung entscheidet, ist gemäß Art. 32 DSGVO auch verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der Datenverarbeitung zu gewährleisten.[2] Diese Maßnahmen sollen vor allem einen unberechtigten Datenzugriff durch Dritte verhindern. Sofern der Datenverarbeiter keine geeigneten Maßnahmen getroffen hat und es infolgedessen zu einem Datenverlust kommt, kann der Betroffene gemäß Art. 82 DSGVO Schadensersatz vom Datenverarbeiter für erlittene Schäden verlangen.[3] Ein Verstoß gegen Art. 32 DSGVO kann zudem durch Bußgelder der Datenschutzaufsichtsbehörden geahndet werden.[4]

Als mögliche technische und organisatorische Maßnahmen nennt Art. 32 Abs. 1 DSGVO folgende: die Pseudonymisierung und Verschlüsselung personenbezogener Daten (lit. a), die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (lit. b), die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu Ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (lit. c) und ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (lit. d).

---

1 Das Urteil kann unter folgendem Link abgerufen werden https://nrwe.justiz.nrw.de/ovgs/ovg_nrw/j2025/16_B_288_23_Beschluss_20250220.html (alle Links des Beitrags zuletzt abgerufen am 04.06.2025).

2 Hierzu ausführlich McGrath, Der Stand zwischen den Stühlen, DFN-Infobrief Recht 01/2021. Mit der Frage, ob diese Pflicht durch eine Vereinbarung zwischen dem Verantwortlichen und der betroffenen Person abbedungen werden kann, hat sich ausführlich der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit beschäftigt, der Vermerk ist abrufbar unter: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Vermerke_und_Stellungnahmen/Vermerk-Abdingbarkeit_TOMs.pdf . Hierzu besteht auch ein Beschluss der Datenschutzkonferenz. Dieser ist abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf.

3 Müller, ich glaub, es hackt, DFN-Infobrief Recht 4/2024.

4 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat jüngst die Vodafone GmbH wegen Verstoßes gegen Art. 32 DSGVO verwarnt. Die Pressemitteilung ist abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/06_Geldbu%C3%9Fe-Vodafone.html?nn=251944.

In der Praxis stellt sich für Daten verarbeitende Stellen die Frage, welches Maß an IT-Sicherheit im konkreten Fall erforderlich ist.[5] Ein perfektes, absolut sicheres System existiert nicht. Insbesondere menschliche Fehler können stets zu IT-Sicherheitsrisiken führen. Von Daten verarbeitenden Stellen darf keine absolute Sicherheit verlangt werden. Dies würde mit unzumutbaren Kosten einhergehen, durch die in vielen Fällen eine Datenverarbeitung unwirtschaftlich werden würde. Entweder würden die Kosten auf die Kunden der Daten verarbeitenden Stelle umgewälzt werden oder Datenverarbeitungen könnten seltener vorgenommen werden. Daher besteht an einem unzumutbaren Maß an IT-Sicherheit keinerlei Interesse.

Aus Art. 32 Abs. 1 DSGVO ergibt sich, dass für die konkret zu ergreifenden Maßnahmen der Stand der Technik, die Implementierungskosten, die Umstände der Datenverarbeitung sowie die Wahrscheinlichkeit des Eintritts eines Schadens und dessen voraussichtliche Höhe maßgeblich sind.

Art. 32 Abs. 2 DSGVO nennt zudem als einzelnes relevantes Kriterium für das zu ergreifende Schutzniveau das Risiko, das mit der Datenverarbeitung einhergeht. Ein hohes Risiko, etwa bei einer Vielzahl betroffener Personen oder der Offenlegung besonders sensibler Daten, erfordert es auch, höhere Schutzmaßnahmen zu ergreifen.

Gemäß Art. 32 Abs. 3 DSGVO kann als Faktor weiterhin herangezogen werden, ob spezifische Verhaltensregeln oder Zertifizierungsverfahren für die Daten verarbeitende Stelle bestehen und ob diese Verfahren eingehalten wurden. Solche Verhaltensanforderungen können gemäß Art. 40 DSGVO von Verbänden oder anderen Vereinigungen, die Daten verarbeitende Stellen vertreten, ausgearbeitet werden. Sie können insbesondere kleinen und mittleren Unternehmen den Verfahrensaufwand deutlich erleichtern. Die Beachtung solcher Verfahrensregelungen kann aber lediglich als Indiz für die Einhaltung von Art. 32 DSGVO dienen.

Ausnahmsweise können sich für bestimmte Daten verarbeitende Stellen auch konkretere Anforderungen aus spezifischen gesetzlichen Regelungen ergeben. Für Angehörige der Kritischen Infrastrukturen gelten etwa die Bestimmungen der NIS 2-RI.[6]

Für die Mehrzahl der Daten verarbeitenden Stellen existieren hingegen keine konkretisierten Sicherheitsanforderungen. Die Frage, ob die ergriffenen Sicherheitsmaßnahmen den Anforderungen von Art. 32 DSGVO genügt haben, verbleibt eine Frage des Einzelfalls, deren Beantwortung auch vielen Gerichten enorme Schwierigkeiten bereitet. Hierbei wird auch immer zu berücksichtigen sein, welche Sicherheitsmaßnahmen dem aktuellen Stand der Technik entsprechen.

II. Verfahren vor dem VG Köln und OVG NRW

Mit der Frage, ob eine Daten verarbeitende Stelle die erforderlichen Sicherheitsmaßnahmen ergriffen hat, musste sich auch das OVG NRW beschäftigen. Dem ging ein Verfahren vor dem Verwaltungsgericht (VG) Köln voraus. Dieses hatte sich mit der Klage eines Geschäftsmanns auseinanderzusetzen, der beruflich mit explosiven Stoffen handelte und sich als wirtschaftlich Berechtigter im elektronischen Transparenzregister eintragen musste. Aus Sorge um seine Sicherheit stellte er bei der zuständigen Behörde einen Antrag, der sich unter anderem darauf richtete, dass seine personenbezogenen Daten ausschließlich mit einer sicheren Ende-zu-Ende-Verschlüsselung verarbeitet und übermittelt werden dürften. Aufgrund seines Berufs behauptete er, dass eine besondere Gefahr bestehe, dass er Opfer schwerer Straftaten werden könnte. Der Geschäftsmann sah sein Begehren als nicht befriedigt durch die Behörde an und reichte beim VG Köln einen Antrag auf eine einstweilige Verfügung ein. Demnach sollte das Gericht anordnen, dass die Behörde eine sicherere Verschlüsselungstechnik zu verwenden habe. Er argumentierte, dass die von der Behörde genutzte Transportverschlüsselung (TLS) keinen ausreichenden Schutz biete, da sie nur den Transport verschlüssele. Zudem genüge bereits die verwendete Verschlüsselung TLS 1.2. nicht, da seit 2018 TLS 1.3. Stand der Technik sei. Die Behörde hielt dem entgegen, dass ihr Sicherheitskonzept vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert sei. Die verwendete TLS-Verschlüsselung sei ausreichend. Die Kommunikation innerhalb des Netzes des Bundes werde zudem zusätzlich durch eine sogenannte SINA-Box und Client-Zertifikate abgesichert. Eine Ende-zu-Ende-Verschlüsselung mache das Register für

5 Zu der Schwierigkeit dieser Feststellung ausführlich McGrath, Der Stand zwischen den Stühlen, DFN-Infobrief Recht 01/2021.

6 Hierzu John, CSIRT, ENISA, BSI, IKT, UNIBÖFI – NIS?, DFN-Infobrief Recht 04/2023 und Geiselmann, Heute schon geNISt?, DFN-Infobrief Recht 04/2025.

Behörden unbrauchbar, da gesetzlich vorgeschriebene behördliche Abfragen dann unmöglich wären.

III. Unterschiedliche Verschlüsselungstechniken

Für das Verständnis der Gerichtsverfahren ist es entscheidend, zwischen den diskutierten Verschlüsselungsmethoden zu unterscheiden. Im Kern geht es dabei um den Unterschied, ob nur der Übertragungsweg der Daten geschützt wird oder ob die Dateninhalte selbst unlesbar gemacht werden.

1. Transportverschlüsselung

Die Transportverschlüsselung baut einen verschlüsselten Kanal zwischen dem Gerät des Nutzers und dem Zielserver auf. Während der Übertragung sind die Daten in diesem Kanal wirksam vor dem Mitlesen durch Dritte geschützt.

Ein wesentliches Merkmal dieser Methode ist jedoch, dass der Schutz am Zielort endet. Der Server des Betreibers muss die Daten entschlüsseln, um sie weiterverarbeiten zu können.

Der Streit um TLS 1.2 gegenüber TLS 1.3 ist dabei eine Frage der Modernität und Sicherheit des eingesetzten Systems. TLS 1.3 ist das direkte Nachfolgersystem und gilt als sicherer und effizienter, da es auf bekannte Schwachstellen älterer Verschlüsselungsverfahren verzichtet. Dennoch ist TLS 1.2 nach wie vor weit verbreitet, da keine Schwachstellen bekannt sind und so ein Upgrade auf TLS 1.3 nicht unbedingt notwendig erachtet wird.[7]

2. Ende-zu-Ende-Verschlüsselung

Einen anderen Ansatz verfolgt die vom Kläger geforderte Ende-zu-Ende-Verschlüsselung. Hier wird nicht nur der Kanal, sondern der Dateninhalt selbst kryptografisch versiegelt. Die Verschlüsselung findet direkt auf dem Gerät des Absenders statt, und nur der vorgesehene Empfänger kann die Daten wieder entschlüsseln.

IV. Beschlüsse des VG Köln des OVG NRW

Das Verwaltungsgericht Köln lehnte in seiner Entscheidung (Az. 13 L 1467/22) den Antrag ab. Es nahm an, dass der Antragsteller nicht ausreichend glaubhaft machen konnte, dass speziell aus der Datenverarbeitung durch das Transparenzregister ein derart hohes und konkretes Risiko für ihn erwächst, welches eine Ende-zu-Ende-Verschlüsselung zwingend erfordern würde. Die allgemeinen Verweise auf seine berufliche Tätigkeit und bereits bestehende Schutzmaßnahmen in anderen Registern reichten dafür nicht aus. Das Gericht bewertete die von der Behörde eingesetzte, BSI-zertifizierte TLS-Verschlüsselung als eine dem Risiko angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahme. Ein verbleibendes Restrisiko bei der digitalen Kommunikation sei als allgemeines Lebensrisiko hinzunehmen.

Gegen die Entscheidung des VG Köln legte der Antragsteller Beschwerde vor dem OVG Münster ein. Auch das OVG Münster teilte jedoch die Auffassung des Antragsgegners und des VG Kölns. Es nahm ebenso an, dass der Antragsteller das von ihm behauptete besondere Risiko nicht glaubhaft gemacht habe. Ohne den Nachweis eines solchen erhöhten Risikos lasse sich ein Anspruch auf eine sicherere Verschlüsselungsmaßnahme nicht aus der DSGVO ableiten. Es sei nicht ersichtlich, dass bei der Behörde eine besonders hohe Wahrscheinlichkeit bestehe, dass sie Opfer von Hackerangriffen werden könnte. Auch das OVG Münster berücksichtigte in seinem Beschluss, dass die Sicherheitstechnik der Behörde vom BSI zertifiziert worden ist. Zudem führte das Gericht aus, dass die TLS-Verschlüsselung nicht die einzige Sicherheitsmaßnahme ist. Es verwies explizit auf die zusätzlichen Sicherungen im Kommunikationsprozess mit anderen staatlichen Stellen, wie die SINA-Box und Client-Zertifikate. Darüber hinaus hat es die im Beschwerdeverfahren ergänzten Ausführungen der Antragsgegnerin berücksichtigt, nach denen bei den jeweiligen Datenübertragungen keine „Zwischenstationen“ existierten, auf denen die Inhalte unverschlüsselt abgelegt wären. Damit wurde angenommen, dass das eingesetzte Verfahren den Anforderungen aus Art. 32 DSGVO genügt.

---

7 A10, Hauptunterschiede zwischen TLS 1.2 und TLS 1.3, abzurufen unter: https://www.a10networks.com/de/glossary/key-differences-between-tls-1-2-and-tls-1-3/ [Stand: 26.05.2025].
Die Entscheidung kann abgerufen werden unter https://openjur.de/u/2517924.html.

V. Relevanz für wissenschaftliche Einrichtungen

Auch wissenschaftliche Einrichtungen müssen sich die Frage stellen, welche Sicherheitsmaßnahmen sie zum Schutz personenbezogener Daten ergreifen. Aus den dargestellten Gerichtsentscheidungen ergibt sich, dass ein absoluter Schutz nicht von Art. 32 DSGVO gefordert wird. Maßgeblich ist vor allem die Wahrscheinlichkeit eines Sicherheitsvorfalls und wie hoch in einem solchen Fall der Schaden ausfallen würde. Demnach sind immer die Umstände des Einzelfalls für die konkret zu ergreifenden Maßnahmen entscheidend. In einer anderen Konstellation hat etwa das Oberlandesgericht (OLG) Schleswig in seinem Urteil vom 18. Dezember 2024 (Az. 12 U 9/24)[8] angenommen, dass eine Ende-zu-Ende-Verschlüsselung für den Versand geschäftlicher E-Mails erforderlich sei und eine Transportverschlüsselung nicht genüge. Das VG Frankfurt hat wiederum in einem Beschluss vom 15. Juli 2022 (Az. 5 L1281/22.F)[9] – -ähnlich wie die zuvor dargestellten Entscheidungen – eine Transportverschlüsselung als ausreichend betrachtet. Den dargestellten Entscheidungen des VG Köln und OVG NRW kann konkret entnommen werden, dass die Gerichte Zertifizierungen durch das BSI anerkennen. Diesen kann eine besondere Bedeutung bei der Frage zukommen, ob ein Sicherheitskonzept den Anforderungen von Art. 32 DSGVO genügt.

8 Das Urteil kann unter dem folgenden Link abgerufen werden: https://www.gesetze-rechtsprechung.sh.juris.de/bssh/document/NJRE001598708.

9 Das Urteil kann unter dem folgenden Link abgerufen werden https://www.lareda.hessenrecht.hessen.de/bshe/document/LARE220003171.

Die fabelhafte Welt der digitalen Dienste

Die Adressaten des Digital Services Act und ihre Bedeutung für Hochschulen und Forschungseinrichtungen

Von Nikolaus von Bernuth, Berlin

Der Digital Services Act (DSA) ist der allgemeine Rechtsrahmen für Dienstleistungen im Internet. Er betrifft also eine Vielzahl an Angeboten. Die meisten seiner Regelungen gelten aber nicht für alle Arten von Diensten, sondern nur für spezifische Dienste wie Online-Plattformen. Um zu beleuchten, welche Regelungen des DSA auch für Hochschulen und Forschungseinrichtungen von Bedeutung sein können, sollen die Adressaten des DSA hier näher definiert und beispielhaft aufgezeigt werden.

I. Einleitung

In der wissenschaftlichen Diskussion um den DSA stehen die Regelungen für sehr große Online-Plattformen im Fokus.[1] Doch Online-Plattformen sind nur ein Adressatenkreis von vielen, für die der DSA spezifische Regelungen vorsieht. Anspruch der Verordnung ist es, einen europäisch harmonisierten Rechtsrahmen für den gesamten digitalen Binnenmarkt zu schaffen. Wichtige Regeln greifen nur für eine kleine Auswahl an Adressaten. Gerade aber für Hochschulen und Forschungseinrichtungen lohnt es sich, die verschiedenen Adressatenkategorien des DSA nachzuvollziehen und mit ihren eigenen Diensten abzugleichen. Dabei können drei Ebenen der Kategorisierung unterschieden werden. Auf erster Ebene befinden sich die Vermittlungsdienste. Auf zweiter Ebene gibt es die schon bekannte Unterscheidung zwischen Diensten reiner Durchleitung, Caching und Hosting. Auf dritter Ebene unterscheidet der DSA schließlich Online-Plattformen, Online-Suchmaschinen sowie sehr große Online-Plattformen bzw. Suchmaschinen.

II. Vermittlungsdienste

Die erste Ebene des DSA ist zugleich der Anwendungsbereich des DSA: Er gilt für alle Vermittlungsdienste, die für Nutzer mit Niederlassungsort oder Sitz in der Union angeboten werden, ungeachtet des Niederlassungsortes des Anbieters dieser Vermittlungsdienste (Art. 2 Abs. 1 DSA). Wer also keinen Vermittlungsdienst betreibt, fällt von vornherein nicht in den Anwendungsbereich des DSA.

Für die Definition des Vermittlungsdienstes verweist der DSA wiederum auf den Begriff „Dienstleistung der Informationsgesellschaft“, Art. 3 lit. g DSA. Dies ist jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.[2]

1. Entgeltlichkeit

Für öffentliche Stellen, zu denen auch öffentliche Hochschulen und Forschungseinrichtungen zählen, könnte das Kriterium „in der Regel gegen Entgelt“ von Bedeutung sein. Dieses ist auch erfüllt, wenn etwa Daten gesammelt werden oder lediglich

1 John, Geschenke verpacken leicht gemacht: Transparenz ist in!, DFN-Infobrief Recht 12/2023; von Bernuth, Im Maschinenraum einer Online-Plattform, DFN-Infobrief Recht 02/25; von Bernuth, Systemische Risiken riesiger Systeme, DFN-Infobrief Recht 09/2024.

2 Art. 3 lit. a DSA mit Verweis auf Art. 1 Abs. 1 lit. b RL (EU) 2015/1535.

kostendeckend gearbeitet wird. Entscheidend ist also nicht, dass konkret für die Nutzung des Dienstes Geld fließt, sondern dass der Dienst generell auf kommerzieller Basis arbeitet.[3] Hierzu hat der deutsche Gesetzgeber in § 7 Abs. 1 Digitale-Dienste-Gesetz (DDG) festgehalten: Für öffentliche Stellen gelten, ohne Rücksicht auf die Entgeltlichkeit, die Art. 4-8 DSA. Diese enthalten die Haftungsprivilegierungen für fremde Inhalte auf den eigenen Diensten, also begünstigende Regelungen.[4] Das DDG ist das deutsche Begleitgesetz zum DSA, das die nationalen Aufsichtszuständigkeiten festlegt und das deutsche Recht mit dem DSA harmonisiert.[5] Es gilt seit dem 17. Februar 2024.

Im Umkehrschluss könnte darauf gefolgert werden, dass die übrigen Normen des DSA, die vor allem Sorgfaltspflichten enthalten, nicht gelten. Anderenfalls hätte der Gesetzgeber wohl auch für sie die Anwendbarkeit normiert. Ohnehin kann das deutsche DDG aber den unionsrechtlichen Begriff „in der Regel gegen Entgelt“ nicht final ausgestalten: Der Vorrang des Unionsrechts besagt, dass die europäischen Gerichte die Auslegungshoheit über Begriffe des Unionsrechts behalten.

Zu beachten ist im Kontext von Hochschulen und Forschungseinrichtungen aber, dass deren Dienste nicht völlig frei zur Verfügung stehen: Sie werden im Rahmen des Nutzungsverhältnisses erbracht, im Gegenzug zur Begleichung von Semesterbeiträgen oder im Rahmen eines Arbeitsverhältnisses. Die Gesetzesbegründung äußert sich nicht zu dieser für Hochschulen durchaus entscheidenden Frage, sodass am Ende die Gerichte über diese Frage entscheiden werden. In der Literatur wird diese Frage bisher kaum diskutiert. Es wird allerdings darauf hingewiesen, dass auch Hochschulen als Dienste der Informationsgesellschaft angesehen werden könnten.[6]

Die Rechtslage ist daher an dieser Stelle nicht eindeutig zu beantworten. Im Zweifel gilt, sich mit den gegebenenfalls einschlägigen Normen vertraut zu machen und ihre Einhaltung sicherzustellen. Insbesondere die Pflichten für Hostingdienste (Art. 16, 17 DSA) könnten bedeutsam werden (dazu sogleich).

2. Vermittlung

Nicht jeder Dienst der Informationsgesellschaft ist auch ein Vermittlungsdienst im Sinne des DSA. Er muss auch eine Dienstleistung erbringen, wie sie in Art. 3 lit. g DSA definiert ist (reine Durchleitung, Caching, Hosting). Diesen Dienstleistungen ist gemeinsam, dass es um die Vermittlung von fremden Informationen geht.[7] Wer also etwa einen Blog betreibt und ausschließlich eigene Inhalte auf dem Blog bereitstellt, nimmt selbst keine Vermittlungstätigkeit wahr und fällt nicht unter den DSA. Der Hostingdienst, über den die Blogwebsite betrieben wird, nimmt hingegen eine Vermittlungstätigkeit wahr: Er vermittelt die (aus seiner Sicht fremden) Inhalte des Blogs an die Besucher der Website.

III. Die einzelnen Vermittlungstätigkeiten

Die Definition der Vermittlungsdienste ist also nicht von der zweiten Ebene zu trennen. Der DSA unterscheidet innerhalb der Vermittlungsdienste zwischen drei Kategorien: reine Durchleitung, Caching und Hosting.

1. Reine Durchleitung

Dienste der reinen Durchleitung bieten an, von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz zu übermitteln oder den Zugang zu einem Kommunikationsnetz zu vermitteln, Art. 3 lit. g i) DSA. Hierbei handelt es sich um die für Hochschulen und Forschungseinrichtungen vielleicht wichtigste Kategorie.

Zugang zu einem Kommunikationsnetz vermitteln insbesondere Accessprovider, also solche Dienste, die einen Internetzugang bereitstellen. Neben kommerziellen Telekommunikationsunternehmen und Betreibern eines offenen WLANs gehören dazu auch Hochschulen und Forschungseinrichtungen, die ihren Mitarbeitenden, Studierenden und gegebenenfalls Gästen Zugang zum Internet vermitteln.

---

3 Vgl. EuGH Urt. v. 15.9.2016 – C-484/14, ECLI:EU:C:2016:689 Rn. 41f. = ZD 2016, 578 – McFadden.

4 Die Haftungsprivilegierungen werden in einem eigenständigen Infobrief vertieft.

5 Dazu: von Bernuth, Kurzbeitrag: The floor is yours, Bundesnetzagentur, DFN-Infobrief Recht 08/2024.

6 Conrad, in: Steinrötter (Hrsg.), Europäische Plattformregulierung (2023), § 3, Rn. 52.

7 Müller-Terpitz/Köhler/Köhler, Art. 3 DSA, Rn. 13.

Ebenfalls als Dienste reiner Durchleitung sind interpersonelle Kommunikationsdienste anzusehen. Dies sind Dienste, die die Kommunikation zwischen individuellen Personen ermöglichen. Dazu zählen klassische Messenger wie Signal, WhatsApp oder Threema, aber auch E-Mail-Anbieter.

An die Dienste der reinen Durchleitung stellt der DSA keinerlei spezielle Sorgfaltspflichten (diese kann allerdings etwa das TKG oder TDDDG enthalten).[8] Im Gegenteil: Sie genießen ein weitreichendes Haftungsprivileg und sind für fremde Inhalte, die sie vermitteln, regelmäßig nicht verantwortlich (Art. 4 DSA). Beachten müssen sie im DSA nur die allgemeinen Pflichten in Art. 9-15 DSA.

2. Caching

Die zweite Kategorie an Vermittlungstätigkeiten ist das Caching. Darunter fallen nach der sehr technischen Definition solche Dienstleistungen, die von einem Nutzer bereitgestellte Informationen in einem Kommunikationsnetz übermitteln. Dabei erfolgt beim Caching eine automatische, zeitlich begrenzte Zwischenspeicherung dieser Informationen zu dem alleinigen Zweck, die Übermittlung der Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, Art. 3 lit. g ii) DSA.

Das Caching unterscheidet sich von der reinen Durchleitung also insbesondere durch die Möglichkeit der Zwischenspeicherung aus Effizienzgründen. Hiervon sind primär Proxyserver erfasst, die Informationen zwischenspeichern und so die Geschwindigkeit und Effizienz der Nutzung des Internets erhöhen. Es handelt sich damit um eine für das Internet elementare Dienstleistung, mit der Nutzende jedoch selten bewusst in Kontakt treten.

Auch sogenannte Content-Delivery-Networks wie Netflix oder Spotify fallen nach herrschender Ansicht unter das Caching. Dafür spricht erneut Erwägungsgrund 29 zum DSA, der explizit „Netzwerke zur alleinigen Bereitstellung von Inhalten“ erwähnt. Ebenso sah es ein Urteil auch schon zum zuvor geltenden, inhaltsgleichen § 9 TMG.[9]

Ebenso wie für die Dienste reiner Durchleitung treffen Caching-Dienste keine besonderen Sorgfaltspflichten im DSA. Sie profitieren vom Haftungsprivileg in Art. 5 DSA und müssen ebenfalls alleine die Art. 9-15 DSA beachten.

3. Hosting

Die dritte und wichtigste Kategorie im DSA ist das Hosting, Art. 3 lit. g iii) DSA. Hosting beschreibt die Speicherung von fremden Inhalten im Auftrag eines Nutzers. Unter das Hosting fällt der größte Teil der im Internet angebotenen Dienstleistungen. Einerseits erfasst dies etwa die Bereitstellung von Speicherplatz zum Betrieb einer Website (klassischer Hostprovider). Außerdem fällt in die Gruppe des Hostings aber auch jeglicher Dienst, bei dem Nutzerinhalte gespeichert und öffentlich verbreitet werden. Hosting ist also die Basiskategorie, in die auch Online-Plattformen als spezifische und wichtigste Adressatengruppe im DSA fallen. Für alle Hostingdienste gelten neben dem Haftungsprivileg (Art. 6 DSA) und den allgemeinen Bestimmungen für alle Vermittlungsdienste (Art. 9-15 DSA) die besonderen Pflichten nach Art. 16, 17 DSA, die zur Einrichtung eines Melde- und Abhilfeverfahrens verpflichten.[10]

Für Hochschulen könnte das Hosting relevant werden, wenn es um den Betrieb von Lernplattformen wie Moodle geht. Auf Moodle wird schließlich Speicherplatz bereitgestellt, um Inhalte der Nutzenden in deren Auftrag zu speichern (und für andere abrufbar zu machen). Der Funktion nach handelt es sich also um einen Hostingdienst. Hier könnte den Hochschulen zugutekommen, dass der DSA nur für entgeltliche Dienste greift. Zudem spricht, wie bereits oben erläutert, die Regelung in Art. 7 Abs. 1 DDG dafür, dass der Gesetzgeber nur die Art. 4-8 DSA auf öffentliche Stellen erstrecken wollte. Die Möglichkeit, dass Gerichte dies anders entscheiden, verbleibt aber.

IV. Die Vermittlungsdienste mit speziellen Pflichten

Auf dritter Ebene des DSA spielen nur noch die Hostingdienste eine Rolle. Zugleich stellen diese speziellen Pflichten den mit

8 Dazu Yang-Jacobi, Telemedien out, Digitale Dienste in!, DFN-Infobrief Recht 08/2024.

9 OLG Köln, Urt. v. 9.10.2020 – 6 U 32/20, GRUR 2021, 70, Rn. 76 - HERZ KRAFT WERKE; so auch Gerdemann/Spindler, GRUR 2023, 3, 5.

10 Näher dazu: Geiselmann, Süßer die Beschwerden nie klingen, DFN-Infobrief Recht 12/2024.

Abstand größten Katalog an Sorgfaltspflichten im DSA dar (Art. 18-48 DSA). Da Hosting eine solche Vielzahl an sehr unterschiedlichen Diensten erfasst, differenziert der DSA hier den Adressatenbereich weiter aus. Er folgt dabei einem risikobasierten Ansatz. Je nach Risikopotenzial der Dienstleistung sowie der Größe des Dienstes können ihn mehr Pflichten treffen. Relevant ist in diesem Rahmen die Unterscheidung von Online-Plattformen, Online-Suchmaschinen sowie zuletzt sehr großen Online-Plattformen und Online-Suchmaschinen als eigenständige Kategorie.

1. Online-Plattformen

Hostingdienste, die durch Nutzende bereitgestellte Inhalte nicht nur speichern, sondern in deren Auftrag auch öffentlich verbreiten, definiert der DSA gesondert als „Online-Plattformen" (Art. 3 lit. i DSA). Die öffentliche Verbreitung setzt voraus, dass die Informationen für eine potenziell unbegrenzte Zahl an Dritten bereitgestellt werden (Art. 3 lit. k DSA). Zudem darf die öffentliche Verbreitung keine unbedeutende und reine Nebenfunktion des Dienstes darstellen. So ist etwa die Kommentarspalte eines Online-Auftritts einer Tageszeitung eine solche unbedeutende Nebenfunktion (Erwägungsgrund 13 DSA). Zu den Online-Plattformen gehören klassische soziale Netzwerke wie Facebook oder X, Video-Sharing-Dienste wie YouTube oder TikTok, aber auch Online-Marktplätze wie Amazon oder Temu. Auch Foren und Enzyklopädien wie Reddit oder die Wikipedia sind Online-Plattformen.

Für Diskussionen sorgen insbesondere die Funktionalitäten in großen Messenger-Apps, welche über unbegrenzt große Gruppen und sogenannte Kanäle potenziell eine Vielzahl an Menschen erreichen. Während Messenger in ihrer Grundfunktion keine Hostingdienste sind, können diese Teilfunktionen sie dennoch als Hostingdienst und sogar als Online-Plattform qualifizieren. Jedenfalls für diese Teilfunktionen, die nicht mehr nur als untergeordnete Nebenfunktionen gelten können, müssen die Messenger sich also an die Pflichten für (sehr große) Online-Plattformen halten.[11]

Für Hochschulen könnte der Betrieb von Moodle oder anderer Lernplattformen ein Grund sein, sich die Pflichten für Online-Plattformen genauer anzusehen. Allerdings ist die Moodle-Instanz in aller Regel nur einer definierten Benutzergruppe geöffnet, nämlich Angehörigen der Hochschulen. Daher fehlt es regelmäßig am Merkmal der öffentlichen Verbreitung von Inhalten, das einen potenziell unbegrenzten Adressatenkreis voraussetzt.

2. Online-Suchmaschinen

Seit jeher umstritten ist die Einordnung von Suchmaschinen wie Google, Bing oder Ecosia. Der DSA umgeht die Einordnung in die klassischen Kategorien von Hosting, Caching und reiner Durchleitung, indem er Suchmaschinen gesondert in Art. 3 lit. j DSA definiert. Demnach zählen dazu Dienste, die es Nutzenden ermöglichen, in Form eines Stichworts oder anderer Eingaben eine Anfrage einzugeben und prinzipiell alle Websites nach dieser Eingabe zu durchsuchen und Ergebnisse angezeigt zu bekommen. Der DSA definiert Suchmaschinen zwar als Vermittlungsdienste, ordnet sie aber nicht klar einer der Kategorien zu. Dies liegt wohl an der Heterogenität der Tätigkeit von Suchmaschinen, die je nach Einzelfall zu bestimmen sind. Um Online-Plattformen handelt es sich aus Sicht der Literatur bei Suchmaschinen aber praktisch nie.[12] Suchmaschinen sind insbesondere dann betroffen, wenn der DSA sie explizit adressiert – maßgeblich sind dies die Art. 33ff. DSA.[13]

3. Sehr große Online-Plattformen und Suchmaschinen

Dies führt zur letzten Kategorie an speziell adressierten Diensten. Der europäische Gesetzgeber kam zu dem Schluss, dass die Risikokategorien nicht nur nach Funktionalität des Dienstes ausgerichtet sein sollten. In der Plattformökonomie geht ein besonderes Risikopotenzial von Diensten aus, die sehr groß sind, also viele aktive Nutzende haben. Die Dienste werden aufgrund ihrer Größe auch als systemrelevant bezeichnet.[14] Gem. Art. 33 Abs. 1 DSA gelten Online-Plattformen und Suchmaschinen mit

11 Dazu zuletzt https://www.heise.de/news/WhatsApp-ueberschreitet-EU-Schwellenwert-Strengere-Regulierung-droht-10287130.html (zuletzt abgerufen am 07.04.25).

12 Müller-Terpitz/Köhler/Holznagel, Art. 3 DSA, Rn. 86.

13 Vertieft zu Suchmaschinen im DSA: Sesing-Wagenpfeil, CR 2023, 113.

14 Denga, in: Steinrötter (Hrsg.), Europäische Plattformregulierung, § 6.

mehr als 45 Mio. aktiven Nutzenden in der Europäischen Union als sehr große Dienste. Dazu zählen nicht nur Nutzende, die Inhalte selbst teilen, sondern auch, wer die Plattformen ausschließlich passiv zum Konsum von Informationen verwendet (Art. 3 lit. p DSA). Alle Online-Plattformen und Suchmaschinen müssen nach Art. 24 Abs. 2 DSA halbjährlich veröffentlichen, wie viele monatlich aktive Nutzende sie durchschnittlich in den vergangenen 6 Monaten in der EU hatten. Übersteigt dieser Wert die Marke von 45 Mio., stuft die Kommission den Dienst als sehr große Online-Plattform/Suchmaschine ein (Art. 33 Abs. 4 DSA). [15]

Für die sehr großen Online-Plattformen und Suchmaschinen gelten insbesondere die wichtigen Pflichten zum Management systemischer Risiken. Sie können außerdem von Forschenden im Rahmen des Datenzugangs nach Art. 40 DSA erforscht werden.[16] Für Hochschulen und Forschungseinrichtungen ist diese Kategorie von Diensten also vornehmlich als Forschungsobjekt von Bedeutung.

V. Fazit

Der DSA baut auf der althergebrachten Unterscheidung von Vermittlungsdiensten zwischen reiner Durchleitung, Caching und Hosting auf. Diese Kategorien sind aus Sicht vieler in der Literatur überkommen.[17] Das zeigt sich auch in der Struktur des DSA, der diese Dreiteilung nur für die Haftungsprivilegierungen aufrechterhält. Sodann differenziert der DSA insbesondere in der Gruppe der Hostingdienste und definiert Online-Plattformen als die wohl wichtigste Gruppe an Adressaten. Die meisten Pflichten treffen aber sehr große Online-Plattformen mit mehr als 45 Mio. aktiven Nutzenden in der EU.

Hochschulen und Forschungseinrichtungen profitieren als Diensteanbieter jedenfalls von den Haftungsprivilegierungen in Art. 4-8 DSA. Ob sie auch unter die Pflichten für Hostingdienste fallen, wenn sie etwa Lernplattformen betreiben, kann zu diesem Zeitpunkt nicht abschließend beantwortet werden. Hier müssen die europäischen Gerichte für Klärung sorgen.

---

15 Die Liste aller aktuell benannten Dienste: https://digital-strategy.ec.europa.eu/de/policies/list-designated-vlops-and-vloses.

16 Dazu von Bernuth, Systemische Risiken riesiger Systeme, DFN-Infobrief Recht 09/2024; von Bernuth, Im Maschinenraum einer Online-Plattform, DFN-Infobrief Recht 02/25.

17 Siehe nur Hofmann/Specht-Riemenschneider, ZGE 2021, 48, 111.

Einer für alle, alle gemeinsam oder jeder für sich?

Ein Überblick zur Diskussion um die Zentralisierung der Datenschutzaufsicht

Von Ole-Christian Tech, Münster

Die Auswüchse des deutschen Exekutivföderalismus machen auch vor der Datenschutz-Grundverordnung (DSGVO) keinen Halt. Die Einhaltung der DSGVO, obwohl sie eine europaweit gleichermaßen gültige Verordnung im Sinne des Art. 288 Abs. 2 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) ist, wird nicht von einer europäischen Behörde überwacht, sondern von Aufsichtsbehörden der jeweiligen Mitgliedstaaten. In Deutschland ist hierfür jedoch nicht eine Behörde zuständig, sondern gleich 18, eine für den Bund und 16 für die Länder. Die Ausnahme hiervon ist wiederum in Bayern zu finden, wo gleich zwei Behörden vorhanden sind, eine für den öffentlich-rechtlichen und eine für den privatwirtschaftlichen Bereich.

I. Problemaufriss

Diese geschilderte Situation der vorhandenen Anzahl an Aufsichtsbehörden in Deutschland stellt Politik und Datenwirtschaft zunehmend vor Probleme. Nicht nur führen die ineffizienten Doppel- und Mehrfachstrukturen zu erheblichen Kosten und Reibungsverlusten in der Zusammenarbeit der Behörden untereinander, sie drohen auch, die Wirksamkeit der Datenschutzaufsicht insgesamt zu gefährden.

Insbesondere mit Blick auf drängende Fragen der Datenwirtschaft, wie dem Personenbezug in Large Language Modellen oder der Möglichkeit, die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO als Grundlage für das KI-Training zu nutzen, herrschen innerhalb des föderalen Systems divergierende Rechtsinterpretationen zwischen den Behörden. Beobachter sprechen hier oftmals auch von einem „Nord-Süd-Gefälle“, wonach die norddeutschen Datenschutzbehörden tendenziell als industriefreundlicher wahrgenommen werden als ihre süddeutschen Amtskollegen.

Die divergierenden Rechtsansichten der Aufsichtsbehörden führen in der Praxis zu erheblicher Rechtsunsicherheit bei Daten verarbeitenden Unternehmen.[1] Dies kann in der Konsequenz sogar zu einem Forum-Shopping in Gestalt eines regelrechten „Behörden-Hoppings“ führen, bei dem datenschutzrechtlich Verantwortliche versuchen, strengere Aufsichtsbehörden zu umgehen.[2]
Zudem sind die Behörden jeweils personell unterschiedlich und darüber hinaus auch sachlich sehr ungleich ausgestattet, was eine effiziente Aufsichtspraxis zusätzlich erschwert.

II. Lösungsansätze

Aus diesen Gründen entbrannte jüngst die Diskussion um eine Zentralisierung der Datenschutzaufsicht. Die Regierungskoalition aus SPD und CDU/CSU formuliert im Koalitionsvertrag etwas schwammig: „Wir reformieren die Datenschutzaufsicht und bündeln sie beim Bundesdatenschutzbeauftragten.“[3] Doch wie

1 Thiel in: Taeger/Gabel § 40 BDSG Rn. 4.

2 Vgl. Martini/Botta, DÖV 2022, 605 (614).

3 https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf, S. 65, Zeile 2095.

genau sollte eine solche aussehen und ist eine solche rechtlich überhaupt zulässig?[4]

Konkret werden zwei Vorschläge diskutiert:

- die Institutionalisierung der Datenschutzkonferenz (DSK) und
- die Übertragung der Kompetenzen auf die Bundesebene, namentlich an die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI).

1. Institutionalisierung der Datenschutzkonferenz (DSK)

Für die Durchführung der DSGVO sind die europäischen Mitgliedstaaten zuständig, vgl. Art. 51 Abs. 1 DSGVO. Die DSGVO selbst verlangt dabei von den Mitgliedstaaten lediglich, dass die Aufsichtsbehörden unabhängig sind, vgl. Art. 52 DSGVO. Organisatorisch überlässt die DSGVO den Mitgliedstaaten die Entscheidung, eine oder mehrere unabhängige Behörden zu schaffen, vgl. Art. 51 Abs. 1 DSGVO. Abgesehen von Deutschland hat von dieser Option zur Pluralität jedoch kein Mitgliedstaat Gebrauch gemacht.[5] Der Grund hierfür liegt in den in Deutschland „historisch gewachsenen Strukturen" des Exekutivföderalismus sowie darin, dass einzelne Bundesländer wie etwa Hessen bereits frühzeitig Datenschutzgesetze erlassen hatten.[6]

In der Praxis spielt daher die bereits 1978 ins Leben gerufene Datenschutzkonferenz als gemeinsames Forum der deutschen Datenschutzaufsicht eine wichtige Rolle.[7]

Exkurs DSK:
Die Datenschutzkonferenz ist ein Zusammenschluss der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder. Sie soll die Datenschutzgrundrechte wahren und schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts erreichen und gemeinsam für seine Fortentwicklung eintreten.[8] Zu diesem Zweck veröffentlicht sie regelmäßig Entschließungen, Orientierungshilfen, Standardisierungen, Pressemitteilungen sowie Beschlüsse und Stellungnahmen. Anders als der Europäische Datenschutzausschuss (EDSA), der auf den ersten Blick eine ähnliche Funktion auf europäischer Ebene erfüllt,[9] hat die DSK jedoch keine gesetzliche Grundlage, sondern ist lediglich als informelles Gremium in der Form eines nicht eingetragenen Vereins öffentlichen Rechts organisiert.[10] Ihre Beschlüsse und Orientierungshilfen sind daher rechtlich nicht bindend.[11]

Die diskutierten Konzepte zur Zentralisierung der Datenschutzaufsicht zielen daher auch auf die Institutionalisierung dieses unverbindlichen Gremiums und seiner Beschlüsse ab.[12] So wird erwogen, die DSK gesetzlich im Bundesdatenschutzgesetz (BDSG) oder in einem sogenannten Bund-Länder-Staatsvertrag zu verankern und hierin die Befugnis zu verbindlichen Mehrheitsbeschlüssen zu schaffen.[13] Während dies im Bereich der Aufsicht über die privatwirtschaftliche Datenverarbeitung aufgrund der dem Bund zugeschriebenen Kompetenz nach Art. 74 Abs. 1 Nr. 1, 11 und 12 Grundgesetz (GG) möglich ist, stellt sich dies für die Aufsicht über die öffentlich-rechtliche Datenverarbeitung differenzierter dar.[14] Art. 74 Abs. 1 Nr. 1, 11 und 12 GG übertragen die Gesetzgebungszuständigkeit für das bürgerliche Recht, das Recht der Wirtschaft und der Arbeit auf den Bund. Dadurch ist die Kompetenz kraft Sachzusammenhangs aus

4 Martini/Botta, DÖV 2022, S. 605 – 616; Wissenschaftliche Dienste, WD 3 - 3000 - 014/25 vom 14.03.2025.

5 Selmayr in: Ehmann/Selmayr, Datenschutz-Grundverordnung Art. 51 Rn. 22f.

6 Vgl. Thiel in: Taeger/Gabel § 40 BDSG Rn. 1.

7 Selmayr in: Ehmann/Selmayr, Datenschutz-Grundverordnung Art. 51 Rn. 26.

8 https://www.datenschutzkonferenz-online.de/media/dsk/Geschaeftsordnung_DSK_Stand_Februar-2024.pdf S. 2.

9 Siehe hierzu bereits Tech, EDSA fighting Irish in: DFN-Infobrief Recht 05/2025.

10 Martini/Botta, DÖV 2022, 605 (607).

11 Martini/Botta, DÖV 2022, 605 (607).

12 Martini/Botta, DÖV 2022, 605 (608).

13 Martini/Botta, DÖV 2022, 605 (608).

14 Martini/Botta, DÖV 2022, 605 (608f.).

der konkurrierenden Gesetzgebungszuständigkeit für diese Bereiche festgelegt. Dagegen haben die Länder die alleinige Befugnis über die Ausführung der Landesgesetze und somit auch über die der Landesdatenschutzgesetze für die öffentlich-rechtliche Datenverarbeitung. Dies folgt aus dem Grundsatz der Eigenstaatlichkeit der Länder und dem in Deutschland im GG verankerten Föderalismus.

Eine Institutionalisierung der DSK im Rahmen des BDSG könnte sich somit nur auf die Aufsichtstätigkeit im Bereich der privaten Datenverarbeitung beziehen. Für eine umfassende Institutionalisierung der DSK, die auch den öffentlichen Verarbeitungssektor umfasst, kommt nur ein Bund-Länder-Staatsvertrag in Betracht.

An dieser Stelle bestünde die Möglichkeit der Einrichtung einer zentralen Geschäftsstelle bei der BfDI für Koordinationsaufgaben.[15] Hierdurch könnte sodann auf bereits zum Teil bestehende Strukturen im Rahmen der zentralen Anlaufstelle (ZASt) zurückgegriffen werden, die die Entscheidungsfindung der deutschen Aufsichtsbehörden für den EDSA steuert.

Die Vorteile eines solchen Vorgehens liegen dabei auf der Hand: Das verbindliche Verfahren würde eine einheitlichere Rechtsauslegung und -anwendung fördern und daher Rechtssicherheit für die Datenwirtschaft schaffen. Durch diese Einheitlichkeit würde es auch nicht mehr zu einem „Forum-Shopping“ zwischen Behörden kommen.

Gleichzeitig blieben hierdurch aber auch komplexe Doppelstrukturen weiterhin bestehen und die Abstimmungs- und Koordinierungserfordernisse im Rahmen der DSK selbst würden sich auch kaum verringern.

2. Übertragung der Kompetenzen auf die Bundesebene

Die zweite Variante sieht eine generelle Übertragung der Aufsichtskompetenzen für den Bereich der Privatwirtschaft auf die BfDI vor - entweder durch Änderung des BDSG, durch Schaffung eines gesonderten Gesetzes für den Datenschutz bei Privaten oder wiederum durch den Abschluss eines Bund-Länder-Staatsvertrags. Rechtlich lässt sich diese Verwaltungskompetenz auf Art. 87 Abs. 3 Satz 1 GG stützen, da dem Bund in diesem Bereich auch die Gesetzgebungskompetenz zukommt.[16] Auch hierfür müsste der Bund das BDSG in §§ 9 Abs. 1 und 40 Abs. 1 anpassen. Insbesondere die Länder sehen ein solches Vorgehen kritisch und befürchten den Verlust von lokaler Expertise und regionaler Beratungsangebote. Inwieweit dieser Verlust angesichts des in der Regel ohnehin grenzüberschreitenden Charakters der Datenverarbeitung im Bereich der Privatwirtschaft aber tatsächlich zu befürchten ist, bleibt zweifelhaft.

Eine solche Befugnisübertragung hätte zudem den Nebeneffekt, dass die Gerichtszuständigkeit für Klagen gegen die Entscheidungen der in Bonn ansässigen BfDI nach § 52 Nr. 2 VwGO in Verbindung mit § 17 Nr. 2 Justizgesetz NRW beim Verwaltungsgericht (VG) Köln liegt. Somit würden auch divergierende Auslegungen der DSGVO auf verwaltungsgerichtlicher Ebene minimiert werden,[17] was wiederum die Rechtssicherheit erhöht.

Fraglich ist jedoch, ob die BfDI die notwendige personelle und inhaltliche Ausstattung für eine derartige Ausweitung ihrer Aufgaben aufweist. Zwar verfügt die BfDI über mehr als 400 Planstellen und war zuletzt die am schnellsten wachsende Bundesbehörde (116 % zwischen 2017 und 2021). Derzeit sind jedoch etwa 100 Stellen unbesetzt, und einige Stimmen bezweifeln, dass diese angesichts des Fachkräftemangels zeitnah besetzt werden können.[18]

III. Ausblick

Die neue Bundesregierung hat mit ihrem Vorstoß zur Reform der Datenschutzaufsicht ein zentrales Problem der wirtschaftlichen Wettbewerbsfähigkeit in Deutschland identifiziert und adressiert. Eine genauere Betrachtung des Problems legt jedoch offen, dass es keine „einfache“ Lösung für das komplexe Problem zu geben scheint. Ein konkreter Gesetzentwurf wird insofern die Vorzüge und Nachteile der jeweiligen Zentralisierungslösungen

15 https://www.lto.de/recht/hintergruende/h/datenschutz-aufsicht-bfdi-koalitionsvertrag-datenschutzbeauftragte-bonn.

16 Martini/Botta, DÖV 2022, 605 (615).

17 Martini/Botta, DÖV 2022, 605 (615).

18 https://www.lto.de/recht/hintergruende/h/datenschutz-aufsicht-bfdi-koalitionsvertrag-datenschutzbeauftragte-bonn.

abwägen müssen. Das Ergebnis dieses Prozesses wird jeweils von Daten verarbeitenden Stellen in Wirtschaft, Wissenschaft und Forschung mit Spannung erwartet.

Inwieweit die Wissenschaft und insbesondere die Hochschulen betroffen sein werden, ist noch nicht final abzusehen. Grundsätzlich liegt die Gesetzgebungskompetenz hinsichtlich der Hochschulen jedoch bei den Ländern, sodass auch die Ausführung dieser Gesetze Ländersache ist. Die Zulässigkeitsregeln für die Datenverarbeitung öffentlicher Stellen sind somit Teil der Staatlichkeit der Länder. Eine etwaige Zentralisierung würde öffentliche Hochschulen somit nicht betreffen. Auf privatwirtschaftliche Forschungs- und Bildungseinrichtungen hätte eine Zentralisierung jedoch unmittelbare Auswirkungen.

DFN Infobrief-Recht-Aktuell

• Arbeitsrecht: Digitale Entgeltabrechnung durch digitales Mitarbeiterpostfach

Das Bundesarbeitsgericht (BAG) hat mit Urteil vom 28. Januar 2025 – 9 AZR 48/24 – entschieden, dass der gesetzliche Anspruch auf Erteilung einer Entgeltabrechnung wirksam durch Einstellen in ein passwortgeschütztes digitales Mitarbeiterpostfach erfüllt werden kann. Es genügt, dass die Abrechnung an einer elektronischen Ausgabestelle bereitgestellt wird. Die im digitalen Mitarbeiterpostfach gespeicherte elektronische Entgeltabrechnung entspricht der gesetzlich vorgeschriebenen Textform.

Hier erhalten Sie den Link zur Pressemitteilung:
https://www.bundesarbeitsgericht.de/presse/entgeltabrechnungen-als-elektronisches-dokument/

• Datenschutzrecht: Geldbußen gegen Vodafone in Höhe von 45 Mio. Euro

Die Bundesbeauftragte für den Datenschutz und Informationsfreiheit hat gegen die Vodafone GmbH zwei Geldbußen in einer Gesamthöhe von 45 Mio. Euro verhängt. Es handelt sich dabei um verschiedene Sachverhalte, denen zugrunde lag, dass die Vodafone GmbH für sie tätige Partneragenturen nicht in ausreichendem Umfang datenschutzrechtlich überprüft und überwacht hatte (Art. 28 Abs. 1 S. 1 DSGVO). Weiterhin wurden Verstöße gegen Art. 32 Abs. 1 DSGVO verwarnt, da Schwachstellen in bestimmten Vertriebssystemen festgestellt wurden. Sicherheitsmängel beim Authentifizierungsprozess bei der Nutzung des Onlineportals „MeinVodafone“ führten schließlich zu einer weiteren Geldbuße in Höhe von 30 Mio. Euro.

Hier erhalten Sie den Link zur Pressemitteilung:
https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/06_Geldbu%C3%9Fe-Vodafone.html

• IT-Sicherheitsrecht: Cybersicherheitsempfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI) für E-Mail-Sicherheit

Das BSI hat eine Cybersicherheitsempfehlung für die E-Mail-Sicherheit veröffentlicht. Sie richtet sich an Unternehmen, die E-Mails mit einer eigenen Domain senden und empfangen. Ziel ist es, bereits vorhandene Standards in der Umsetzung zu verbessern, indem häufige Fehler aufgezeigt und konkrete technische Nutzungsempfehlungen gegeben werden.

Hier erhalten Sie den Link zur Handlungsempfehlung:
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_155.pdf?__blob=publicationFile&v=5

Kurzbeitrag: Automatisierte Kontrollen als Gamechanger?

Datenschutzbehörden prüfen Websites vermehrt mithilfe automatisierter Tools auf ihre Datenschutzkonformität

von Anna Maria Yang-Jacobi, Berlin

Seit 2024 nutzen Datenschutzbehörden in Deutschland automatisierte Prüf-Instrumente bei ihrer Überwachungstätigkeit. Bisher erfolgten vor allem automatisierte Kontrollen von Websites. Das Problem bei Websites ist oft eine fehlende oder unzureichende Einbindung von Einwilligungsbannern (auch bekannt als Cookie-Banner), auch und gerade wenn Drittdienste auf der Website genutzt werden. Hochschulen und Forschungseinrichtungen sollten auf einen datenschutzkonformen Web-Auftritt achten.

I. Automatisierte Prüfungen von Websites

Die Einhaltung der DSGVO gehört nach Art. 57 Abs. 1 lit. a, lit. f, lit. h DSGVO zu den Aufgaben der Datenschutzbehörden. Zusätzlich überprüfen sie auch die Einhaltung von Teilen des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG). Lange Zeit gab es allerdings wiederholt Kritik, dass die deutsche Behördenlandschaft bei der Durchsetzung von Datenschutzvorschriften nicht konsequent genug sei.[1] Die Knappheit an Personalressourcen, finanziellen Möglichkeiten und technischen Mitteln taten ihr Übriges in Sachen Durchsetzungsdefizit. Doch seit dem vergangenen Jahr scheint frischer Wind in einigen Datenschutzbehörden zu wehen. IT-Labore werden etabliert und automatisierte Prüfungstools kommen in zunehmendem Maß zum Einsatz; bisher vor allem bei der Überprüfung von Websites auf ihre Datenschutzkonformität. Als jüngstes Beispiel ist eine Prüfung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) zu nennen. Mitte April 2025 machte die Behörde bekannt, dass sie 1.000 in Hamburg betriebene Websites mithilfe eines automatisierten Tools auf die datenschutzkonforme Einbindung von Drittdiensten überprüft hat.[2] Anlass für die Prüfung waren Beschwerden zum Tracking durch Drittdienste auf Websites, ohne dass die Besucher:innen vorher in das Tracking eingewilligt hatten. Die überprüften Websites wurden nach dem Zufallsprinzip ausgewählt. Bei 185 der geprüften Websites stellte der HmbBfDI Mängel fest.

Der HmbBfDI ist aber nicht die erste Behörde, die automatisierte Prüfungstools einsetzt. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) überprüfte bereits 2024 mehr als 350 Websites von bayerischen Betreiber:innen teilweise automatisiert.[3] Die Prüfung betraf die Frage, ob beim Öffnen einer Website auf der ersten Ebene des Einwilligungsverarbeitungsbanners (sog. Cookie-Banner) neben der Zustimmungsmöglichkeit eine Möglichkeit zur Ablehnung der Verarbeitung vorliegt. Eine Ablehnung soll ähnlich leicht erfolgen können wie

1 Dachwitz/Fanta, 24.5.2023: https://netzpolitik.org/2023/5-jahre-datenschutzgrundverordnung-die-fuenf-groessten-schwaechen-der-dsgvo/ (alle Links dieses Beitrags wurden zuletzt am 28.5.2025 abgerufen).

2 Pressemitteilung, 24.4.2025: https://datenschutz-hamburg.de/news/tracking-durch-drittdienste-185-von-1000-geprueften-websites-muessen-nachbessern.

3 Pressemitteilung, 9.4.2024, https://www.lda.bayern.de/media/pm/pm2024_02.pdf.

eine Zustimmung.[4] 350 Websites genügten den Anforderungen nicht und wurden benachrichtigt. Die Betreiber:innen hatten danach die Möglichkeit, sich zu den Feststellungen zu äußern und die Websites anzupassen.

Durch die automatisierten Prüfungen kann allerdings auch eine viel größere Anzahl an Websites kontrolliert werden. Im Mai 2024 erklärte die Sächsische Datenschutz- und Transparenzbeauftragte (SDTB), dass ihre Behörde mithilfe eines automatisierten Tools 30.000 Websites von Unternehmen, Vereinen und öffentlichen Stellen mit Sitz in Sachsen auf den rechtswidrigen Einsatz von Google Analytics untersucht hat.[5] Auf 2.300 dieser Websites wurden die Daten von Google Analytics[6] ohne die Einwilligung der Nutzer:innen erhoben. Die Betreiber:innen wurden im Anschluss aufgefordert, auf ihren Websites nachzubessern. Die Maßnahme zeigte Wirkung. Eine Nachuntersuchung der SDTB im Oktober 2024 ergab, dass viele Websites angepasst wurden.[7]

Weitere Datenschutzbehörden könnten dieser Durchsetzungspraxis folgen und in Zukunft ebenfalls automatisierte Prüfungen durchführen. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit stellte in seinem Tätigkeitsbericht für das Jahr 2024 ein Toolkit vor, das verschiedene Prüf-Tools miteinander verbindet, um eine umfassende technische Analyse von Websites effizient zu ermöglichen. Der Ablauf einer solchen Prüfung und die Funktionen werden in dem Bericht genauer erklärt.[8] Auch der Europäische Datenschutzausschuss (EDSA) bietet seit Anfang 2024 ein Open-Source-Tool für automatisierte Überprüfung von Websites an.[9]

II. Einwilligungen auf Websites und bei Einbindung von dritten Diensten

Beim Betrieb von Websites sind sowohl datenschutzrechtliche Vorgaben nach dem TDDDG[10] als auch nach der DSGVO einzuhalten. In den untersuchten Fällen ging es um Cookie-Banner in unterschiedlichen Konstellationen. Cookie-Banner begegnen Internetnutzer:innen beim Besuch von Websites häufig und informieren über eine geplante Speicherung oder Nutzung von Daten. Cookies selbst sind Textdateien, die beim Aufruf einer Website erzeugt und gespeichert werden.[11] Über Cookies können diese Informationen auf dem Endgerät der Nutzer:innen gespeichert werden. Sie können aber auch Trackingzwecken dienen und die Aktivität von Website-Besucher:innen nachverfolgen. Dabei ist es wichtig, dass Nutzer:innen selbst entscheiden können, ob ihre Daten für Nutzungsprofile verwendet werden dürfen.

Im TDDDG finden sich unter anderem die gesetzlichen Regelungen zum Speichern und Abruf von Informationen auf den Endgeräten. § 25 Abs. 1 TDDDG legt den Grundsatz fest, dass Nutzende einwilligen müssen, wenn Informationen in der Endeinrichtung gespeichert werden oder auf diese auf dem Endgerät gespeicherten Informationen zugegriffen wird. § 25 Abs. 2 Nr. 2 TDDDG regelt eine Ausnahme des Einwilligungsgrundsatzes, wenn die Informationen zur Erbringung des Dienstes erforderlich sind. Sofern die Nutzung bestimmter Funktionen auf einer Website essenziell ist, sind es technisch erforderliche Cookies und es bedarf keiner Einwilligung der Nutzenden. Beispiele sind die Speicherung von Spracheinstellungen oder die Authentifizierung der Nutzenden für die Dauer der Sitzung. Bei technisch nicht notwendigen Cookies, wie zum Beispiel Cookies zu Werbezwecken,

---

4 Der Landesbeauftragte für den Datenschutz Niedersachsen und in der Folge auch das VG Hannover beschäftigten sich ebenfalls mit dieser Thematik. Im Urteil wurde festgestellt, dass bei Verwendung einer „Alle akzeptieren“ auch eine „Alles ablehnen“-Schaltfläche auf der ersten Ebene von Cookie-Banner verwendet werden muss. Siehe dafür, Pressemitteilung, 20.5.2025, https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/urteil-zu-manipulativem-cookie-banner-alles-ablehnen-schaltflache-ist-ein-muss-241960.html.

5 Pressemitteilung, 13.6.2024, https://www.medienservice.sachsen.de/medien/news/1076636.

6 Zum Einsatz von Google Analytics siehe Baur, Unmaskiert wird abkassiert!, DFN-Infobrief Recht 8/2019.

7 Tätigkeitsbericht Datenschutz 2024 der Sächsischen Datenschutz- und Transparenzbeauftragten, S. 41, 43, https://www.datenschutz.sachsen.de/download/taetigkeitsberichte/Taetigkeitsbericht_Datenschutz_2024.pdf.

8 53. Tätigkeitsbericht zum Datenschutz für das Jahr 2024, S. 218 ff.: https://datenschutzarchiv.org/fileadmin/Dokumente/2024/TB_Hessen_LfD_53_2024_de.pdf.

9 https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/edpb-website-auditing-tool_en.

10 Zum TDDDG siehe Yang-Jacobi, Telemedien out, Digitale Dienste in!, DFN-Infobrief Recht 8/2024. Genaueres zum Inhalt siehe John, TTDSG – Die Profis in spe, DFN-Infobrief Recht 5/2021.

11 Siehe zu Cookies vor allem John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 1/2022.

ist eine Einwilligung jedoch zwingend erforderlich.[12] Die Einwilligung erfolgt in der Regel über die bekannten Cookie-Banner.[13] Sie muss freiwillig im Sinne des § 25 Abs. 1 TDDDG, Art. 4 Nr. 11 DSGVO erfolgen. So sollen Cookie-Banner Nutzende bei ihrer Entscheidung nicht leiten (sog. „nudging"). Teilweise werden auch genauere Vorgaben zur Gestaltung vertreten.[14]

In dem Zusammenhang ist eine weitergehende Unterscheidung zwischen First-Party-Cookies, die von der aufgerufenen Website selbst gesetzt werden, und Third-Party-Cookies, die von einer fremden Domain gesetzt werden, möglich. Die technische Notwendigkeit kann bei beiden Cookie-Arten vorliegen. Dritte Dienste können Analyse-Dienste, Karten-Dienste oder auch Social-Media-Plug-Ins/Buttons sein. Sie dienen der statistischen Analyse von Besucherzahlen, Verweildauer oder auch besuchten Seiten und Aktionen oder zeigen Standorte auf einer Karte an. Das Verhalten der Nutzenden kann dadurch erfasst und ausgewertet werden. Gerade bei Drittdiensten, die Informationen in der Endeinrichtung des Endnutzenden speichern, § 25 Abs. 1 TDDDG, oder auch personenbezogene Daten über mehrere Websites hinweg sammeln und umfangreiche Nutzerprofile erstellen, ist eine Einwilligung für eine rechtmäßige Datenverarbeitung notwendig, Art. 6 Abs. 1 S. 1 lit. a DSGVO.[15] Wenn diese also unmittelbar bei Aufruf der Website aktiviert werden und keine Einwilligung erfolgt, liegt ein Verstoß gegen die datenschutzrechtlichen Regelungen vor.

III. Bedeutung für Hochschulen und Forschungseinrichtungen

Die neuen Möglichkeiten von Datenschutzbehörden durch IT-Labore und die darin durchführbaren automatisierten Prüfungen werden vermutlich zu mehr Kontrollen führen. Auch Hochschulen und Forschungseinrichtungen sollten ihre bestehenden und künftigen Websites auf Datenschutzkonformität überprüfen. Dazu gehört neben einer Datenschutzerklärung nach Art. 13, 14 DSGVO, auch eine – im Idealfall einrichtungsweit einheitliche – Handhabung von Cookie-Bannern und Drittdiensten. Sofern dritte Dienste (zu Analysezwecken oder um Standorte anzuzeigen) nicht zwingend notwendig sind, sollte darauf verzichtet werden. Falls Drittdienste dennoch auf den Websites eingebunden werden, ist auf eine gesonderte und wirksame Einwilligung zu achten. Die Drittdienste dürfen dann nur bei den Nutzer:innen aktiviert werden, die die entsprechende Einwilligung erteilt haben.

12 Eine Ausnahme stellen die sogenannten Paywall-Cookies bei Medienkonzernen dar.

13 Um der Vielzahl der Cookie-Banner entgegenzuwirken, sind sogenannte Personal/Privacy Information Management Systeme zur Einwilligungsverwaltung vorgesehen, § 26 TDDDG. Zur seit 1.4.2025 in Kraft getretenen Einwilligungsverwaltungsverordnung siehe Schöbel, Das Ende der Cookie-Banner, DFN-Infobrief Recht 3/2025.

14 Bereits 2022 erhob die Verbraucherzentrale NRW Klage gegen Google wegen der Ausgestaltung ihrer Cookie-Banner. Google änderte die Cookie-Banner dahingehend, sodass das Verfahren für erledigt erklärt wurde und ohne Urteil endete, siehe Palenberg, Google brings light into the dark pattern, DFN-Infobrief 2/2023.

15 Dies gilt gerade für Google-Drittdienste, siehe die jüngst ergangene Entscheidung des VG Hannover, Urt. v. 19.3.2025, Az. 10 A 5385/22, BeckRS 2025, 10472, Rn. 76 ff.

Impressum

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: dfn-verein@dfn.de

Texte:

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Universität Münster und der Freien Universität Berlin.

Universität Münster
Institut für Informations-,
Telekommunikations- und Medienrecht
-Zivilrechtliche Abteilung-
Prof. Dr. Thomas Hoeren
Leonardo Campus 9, 48149 Münster

Tel. (0251) 83-3863, Fax -38601

E-Mail: recht@dfn.de

Freie Universität Berlin
Professur für Bürgerliches Recht,
Wirtschafts-, Wettbewerbs- und
Immaterialgüterrecht
Prof. Dr. Katharina de la Durantaye, LL. M. (Yale)
Van't-Hoff-Str. 8, 14195 Berlin

Tel. (030) 838-66754

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht", der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: https://anchor.fm/fsr-dfn