BRANDI
RECHTSANWÄLTE

JAHRESRÜCKBLICK 2024 UND AUSBLICK 2025

Informationen zum Datenschutz I Januar 2025

English version

Einleitung

Das Datenschutzrecht im Jahr 2024 war geprägt von verschiedenen Entscheidungen der Behörden und Gerichte zur Interpretation und Anwendung der Bestimmungen der DSGVO. Einen breiten Raum haben dabei Fragestellungen zum Umfang möglicher Schadensersatzansprüche nach Art. 82 DSGVO sowie zur Reichweite des Auskunftsanspruchs nach Art. 15 DSGVO eingenommen. Daneben wurden auch die rechtliche Einordnung verschiedener Techniken zum Nutzer-Tracking sowie die Zulässigkeit der Datenverarbeitung zu Werbezwecken weiter intensiv diskutiert. Im Juli 2024 ist außerdem die neue KI-Verordnung in Kraft getreten, die auch für die Verarbeitung personenbezogener Daten von Relevanz ist. Die neue Verordnung verfolgt einen risikobasierten Ansatz und legt unter anderem fest, welche Anforderungen Anbieter, Betreiber, Händler und Nutzer von KI-Systemen einzuhalten haben.

Am 24. Mai 2024 hat nunmehr schon zum fünften Mal unser BRANDI-Datenschutzrechtstag stattgefunden. Zu Gast bei BRANDI waren Herr Dr. Thilo Weichert, der ehemalige Leiter der Datenschutzaufsichtsbehörde in Schleswig-Holstein (ULD), und Herr Prof. Dr. Eckhard Koch, der Vizepräsident für Forschung, Entwicklung und Transfer der FHDW Paderborn. Wir haben uns mit Herrn Dr. Weichert und Herrn Prof. Dr. Koch zu verschiedenen Fragestellungen zum Thema „Sicherheit beginnt mit Datenschutz“ ausgetauscht. Im Gespräch mit Rechtsanwältinnen und Rechtsanwälten von BRANDI gaben die Gastreferenten spannende Einblicke in verschiedene datenschutzrechtliche Themen, aktuelle Verfahren der Aufsichtsbehörden und ihre tägliche Arbeit.

Den Jahreswechsel haben wir zum Anlass genommen, in unserem traditionellen Jahresrückblick die im vergangenen Jahr schwerpunktmäßig behandelten Themen und besonders relevanten Entwicklungen und Geschehnisse noch einmal Revue passieren zu lassen. Zudem wagen wir einen Ausblick auf das neue Jahr und die für 2025 zu erwartenden Entwicklungen.

Schwerpunktthemen des Datenschutz-Newsletters von BRANDI

In unserem Datenschutz-Newsletter berichten wir jeden Monat über aktuelle Geschehnisse aus dem Datenschutzrecht. Im jeweiligen Schwerpunktthema informieren wir zudem vertieft über ein ausgewähltes datenschutzrechtliches Thema und fassen hierbei die aus datenschutzrechtlicher Sicht relevanten Aspekte und Besonderheiten sowie praxisrelevante Hinweise zusammen. Die Schwerpunktthemen unseres Datenschutz-Newsletters aus dem Jahr 2024 haben wir nachfolgend noch einmal für Sie zusammengefasst:

> Datenschutzkonforme Gestaltung eines Cookie-Banners
>
> Das Verzeichnis der Verarbeitungstätigkeiten - Was ist ein Verfahren und wie viele Verfahren müssen dokumentiert werden?
>
> Datenlöschung - Online und Offline
>
> Messenger-Dienste im Unternehmen
>
> Die Nutzung von Microsoft 365 im Unternehmen
>
> BRANDI-Datenschutzrechtstag zum Thema „Sicherheit beginnt mit Datenschutz“
>
> Gemeinsame Verantwortlichkeit im Konzern
>
> Verwendung von auf KI-Systemen basierenden Chatbots
>
> Führerscheinkontrolle durch den Arbeitgeber
>
> Datenschutz im BEM-Verfahren
>
> Datenschutz beim Dienstrad-Leasing

Viele dieser Themen haben ihren Ursprung in aktuellen Fällen aus unserer Beratungspraxis oder beziehen sich auf seitens der Aufsichtsbehörden veröffentlichte Stellungnahmen und Hinweise oder gerichtliche Entscheidungen und sind besonders praxisrelevant.

Rechtsprechung

Nachfolgend finden Sie – thematisch sortiert – einige besonders relevante Gerichtsentscheidungen aus dem Jahr 2024.

Nachdem der EuGH bereits in zwei Entscheidungen aus Dezember 2023 die Voraussetzungen für den Anspruch auf immateriellen Schadensersatz nach Art. 82 DSGVO konkretisiert hat (EuGH, Urt. v. 14.12.2023 - Az. C-340/21 und EuGH, Urt. v. 14.12.2023 - Az. C-456/22), setzte das Gericht sich im Januar 2024 mit der Frage

auseinander, ob ein theoretisches Risiko der missbräuchlichen Verwendung von Daten bereits einen Anspruch auf Schadensersatz rechtfertigt (EuGH, Urt. v. 25.01.2024 - Az. C-687/21). Das Gericht entschied, dass der Schadensersatzanspruch gem. Art. 82 DSGVO lediglich eine Ausgleichsfunktion, aber keine Straffunktion erfüllt. Weiter führte es aus, dass die Person, die den Schadensersatz geltend macht, nicht nur den Verstoß, sondern auch den entstandenen Schaden nachweisen muss. Der Begriff des immateriellen Schadens sei hierbei zwar weit zu verstehen und die Befürchtung des Datenmissbrauchs könne vom Grundsatz her einen immateriellen Schaden darstellen; dieser müsse trotz dessen aber nachgewiesen werden. Ein rein hypothetisches Risiko der missbräuchlichen Verwendung durch einen unbefugten Dritten könne nicht zu einer Entschädigung führen. Im April hat der EuGH die bestehende Rechtsprechung weiter ausdifferenziert (EuGH, Urt. v. 11.04.2024 - Az. C-741/21). Er stellte in Anknüpfung an seine bisherige Rechtsprechung heraus, dass der „Verlust von Kontrolle" zwar vom Grundsatz her unter den Schadensbegriff fällt, der Verstoß gegen Bestimmungen, die dem Betroffenen Rechte verleihen, für sich genommen aber nicht ausreicht, um einen Schadensersatzanspruch zu begründen. Hinsichtlich der Bemessung des Anspruchs entschied das Gericht, dass es Sache der Mitgliedstaaten ist, unter Wahrung der unionsrechtlichen Grundsätze der Effektivität und der Äquivalenz Kriterien zur Bestimmung des Betrags der Entschädigung festzulegen. Die Höhe des Schadensersatzes dürfe jedoch nicht von der Schwere oder Häufigkeit der Verstöße abhängig gemacht werden. Darüber hinaus stellte der EuGH fest, dass eine Haftungsbefreiung des Verantwortlichen durch einen pauschalen Verweis auf das Fehlverhalten Untergebener nicht möglich ist, sondern strikt auf Fälle beschränkt werden muss, in denen der Verantwortliche nachweisen kann, dass kein Kausalzusammenhang zwischen seinem Verhalten und dem Schaden besteht. In zwei weiteren Entscheidungen aus Juni 2024 hat der EuGH sodann nochmals wiederholt, dass Art. 82 DSGVO einen Verstoß gegen die DSGVO, einen Schaden und einen Kausalzusammenhang zwischen Verstoß und Schaden voraussetzt, ein bloßer Verstoß nicht zwangsläufig einen Schadensersatzanspruch begründet und der Schaden vom Betroffenen nachgewiesen werden muss, wobei es dem jeweiligen Gericht freisteht, auch einen geringfügigen Schadensersatz auszusprechen (EuGH, Urt. v. 20.06.2024 - Az. C-182/22 und C-189/22). Zudem verwies das Gericht erneut darauf, dass die Festlegung der Kriterien für die Ermittlung des Umfangs des Schadensersatzes Aufgabe des Rechts der einzelnen Mitgliedstaaten ist, wobei der Äquivalenz- und der Effektivitätsgrundsatz zu beachten sind. Ein zusätzlicher Verstoß gegen nationale Vorschriften ist nach Auffassung des EuGH bei der Bemessung genauso wenig zu berücksichtigen wie Grad der Schwere und Vorsätzlichkeit des Verstoßes. In einer Entscheidung aus Oktober 2024 ging es erneut um die Frage, ob ein Schaden bereits dann angenommen werden kann, wenn personenbezogene Daten durch ein Datenleck bei dem Verantwortlichen in die Hände Dritter geraten bzw. geraten können oder ob es weiterer Umstände wie der illegalen Weitergabe oder eines Missbrauchs bedarf (EuGH, Urt. v. 04.10.2024 - Az. C-200/23). Der EuGH bekräftigte die in seinen bisherigen Urteilen zu diesem Themenbereich angedeutete Tendenz und formulierte noch einmal explizit, dass bereits der Kontrollverlust als immaterieller und damit ersatzfähiger Schaden anzusehen sein kann. Einer zusätzlichen Begründung etwaiger Ängste und Sorgen um einen Missbrauch bedürfe es nicht zwingend. Unter Verweis auf die zuvor dargestellte Rechtsprechung des EuGH hat der BGH schließlich im November 2024 Schadensersatzansprüche im Zusammenhang mit einem Datenschutzvorfall bei dem sozialen Netzwerk Facebook bejaht (BGH, Urt. v. 18.11.2024 - Az. VI ZR 10/24). Die Entscheidung des BGH ist bedeutsam für viele ähnlich gelagerte Klagen, die gerade in Deutschland anhängig sind und bei denen sich die Instanzgerichte womöglich an der Leitentscheidung des BGH orientieren werden.

Im Februar 2024 entschied der BGH erneut, dass aus Art. 15 Abs. 1 und 3 DSGVO kein grundsätzlicher Anspruch auf Herausgabe von Abschriften der Begründungsschreiben samt Anlagen zu Prämienanpassungen in der privaten Krankenversicherung folgt (BGH, Urt. v. 06.02.2024 - Az. VI ZR 15/23). Er führte aus, dass der Begriff der personenbezogenen Daten unter Berücksichtigung der Rechtsprechung des EuGH zwar weit zu verstehen ist, die Schreiben eines Verantwortlichen an eine betroffene Person aber nur insoweit als personenbezogene Daten einzustufen sind, als sie auch tatsächlich Informationen über die betroffene Person enthalten. Der Begriff der „Kopie" beziehe sich insoweit ebenfalls nicht auf ein Dokument als solches, sondern lediglich auf die darin enthaltenen personenbezogenen Daten. Eine Reproduktion von Dokumenten oder ganze Dokumente müssten in der Folge nur dann zur Verfügung gestellt werden, wenn die Kontextualisierung erforderlich sei, um die Verständlichkeit zu gewährleisten. Zur Auslegung des Begriffs „Kopie der personenbezogenen Daten" in Art. 15 Abs. 3 DSGVO hat sich der BGH sodann erneut im März 2024 geäußert (BGH, Urt. v. 15.03.2024 - Az. VI ZR 330/21). Er führte aus, dass ein personenbezogenes Datum dann vorliegt, wenn eine irgendwie geartete Information über eine Person gegeben ist. Dies sei anzunehmen, wenn die Information eine Verknüpfung mit einer konkreten Person aufgrund des Inhalts, des Zwecks oder der Auswirkung der Information aufweise. Der BGH führte insoweit aus, dass eigene Äußerungen bzw. Schreiben eines Betroffenen immer eine Verknüpfung zu seiner Person aufweisen und diese deshalb als Kopie zur Verfügung zu stellen sind, da sie in Gänze einen Personenbezug beinhalten. Bei Schreiben von Dritten sei demgegenüber eine Einzelfallprüfung erforderlich. Enthalten Unterlagen lediglich vereinzelt personenbezogene Daten, seien diese nur dann in Gänze als Kopie zur Verfügung zu stellen, wenn die Kontextualisierung erforderlich sei, um die Datenverarbeitung nachvollziehen und von den Betroffenenrechten Gebrauch machen zu können.

Mit Urteil aus Juli 2024 hat der EuGH ein weiteres Mal die Voraussetzungen für Verbandsklagen präzisiert (EuGH, Urt. v. 11.07.2024 - Az. C-757/22). Das Gericht hat entschieden, dass Art. 80 Abs. 2 DSGVO so auszulegen ist, dass eine befugte Einrichtung eine Verbandsklage erheben kann, wenn sie geltend macht, dass die Rechte einer betroffenen Person ihres Erachtens „infolge einer Verarbeitung" verletzt wurden. Eine beachtliche Verletzung könne sich insoweit auch aus der Missachtung der Pflicht zur Information nach Art. 12 und 13 DSGVO ergeben. Da eine Verarbeitung personenbezogener Daten unter Verletzung des Informationsrechts gegen die Vorgaben der DSGVO verstoße, sei die Verletzung dieses Rechts als Verstoß gegen die Rechte der betroffenen Person „infolge einer Verarbeitung" i.S.v. Art. 80 Abs. 2 DSGVO anzusehen. In der Folge stelle das Informationsrecht und damit mittelbar auch die Informationspflicht ein Recht dar, bei dessen Verletzung von dem Verbandsklagemechanismus Gebrauch gemacht werden könne.

Im Oktober 2024 hat sich der EuGH mit zwei Fällen der Datenverarbeitung zu Werbezwecken beschäftigt. In der ersten Entscheidung ging es inhaltlich um die Frage, wie lange soziale Online-Dienste wie Facebook Daten, die für Werbezwecke gesammelt wurden, speichern dürfen und ob die Online-Dienste berücksichtigen müssen, um welche Art von Daten es sich handelt (EuGH, Urt. v. 04.10.2024 - Az. C-446/21). Der EuGH führte aus, dass der Grundsatz der Datenminimierung einer unbegrenzten und hinsichtlich der Art der Daten unterschiedslosen Verarbeitung entgegensteht. Außerdem berechtige die Veröffentlichung eines bestimmten Datums soziale Online-Dienste wie Facebook nicht dazu, thematisch verbundene Daten, die nicht auf dem gleichen Wege veröffentlicht wurden, zu verknüpfen und diese Verknüpfungen dann zu Werbezwecken zu nutzen. In der zweiten Entscheidung hat der EuGH konkretisiert, unter welchen Voraussetzungen die Übermittlung von personenbe-

zogenen Daten zu Marketingzwecken auf die Rechtsgrundlage der berechtigten Interessen i.S.v. Art. 6 Abs. 1 S. 1 lit. f) DSGVO gestützt werden kann (EuGH, Urt. v. 04.10.2024 - Az. C-621/22). Das Gericht führte hierzu aus, dass eine Datenverarbeitung auf Basis berechtigter Interessen unter drei kumulativen Voraussetzungen rechtmäßig ist: Von dem Verantwortlichen oder einem Dritten muss ein berechtigtes Interesse wahrgenommen werden, die Verarbeitung muss zur Verwirklichung des berechtigten Interesses erforderlich sein und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person dürfen nicht überwiegen. Das erforderliche berechtigte Interesse müsse darüber hinaus nicht gesetzlich geregelt, sondern lediglich rechtmäßig sein.

Entwicklungen in der Gesetzgebung

Seit dem 17. Februar 2024 ist der Digital Services Act (DSA), der bereits am 16. November 2023 in Kraft getreten ist, vollständig anwendbar. Der DSA schafft verschiedene neue Pflichten für Anbieter digitaler Dienste, die Verbrauchern Waren, Dienstleistungen oder Inhalte vermitteln; darunter die Pflicht zur Einrichtung einer zentralen Kontaktstelle für Behörden und Nutzer, Erläuterungspflichten in den AGB sowie die Pflicht zur jährlichen Veröffentlichung von Transparenzberichten. Bei einem Verstoß gegen den DSA kann die zuständige Behörde – in Deutschland die Bundesnetzagentur – Bußgelder in Höhe von bis zu 6 % des weltweiten Jahresumsatzes verhängen.

Am 14. Mai 2024 ist das Telemediengesetz (TMG) außer Kraft getreten und wurde durch das Digitale-Dienste-Gesetz (DDG) ersetzt. Im Zuge der Einführung des DDG wurde gleichzeitig auch der Name des Ende 2021 in Kraft getretenen Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) in Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) umbenannt.

Die neue Verordnung zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Verordnung über künstliche Intelligenz, KI-Verordnung) ist sodann am 12. Juli 2024 im Amtsblatt der EU veröffentlicht worden, nachdem das Europäische Parlament der Verordnung im März zustimmte. Die KI-Verordnung ist am 1. August 2024 in Kraft getreten und die Umsetzungsfristen haben begonnen. Mit einigen Ausnahmen gelten die neuen Regelungen ab dem 2. August 2026. Die neue Verordnung sieht verschiedene Verpflichtungen für KI-Systeme vor, die von den jeweiligen Risiken und Auswirkungen abhängig sind. Als hochriskant werden unter anderem Systeme eingestuft, die in den Bereichen kritische Infrastruktur, allgemeine und berufliche Bildung oder Beschäftigung und die für private und öffentliche Dienstleistungen in bestimmten Bereichen der Strafverfolgung sowie im Zusammenhang mit Migration und Grenzmanagement, Justiz und demokratischem Prozess genutzt werden.

Aktivitäten von Aufsichtsbehörden

Die Datenschutz-Aufsichtsbehörden der Mitgliedstaaten der EU haben auch 2024 wieder unterschiedliche datenschutzrechtliche Themen aufgegriffen. Neben der Verhängung von Bußgeldern aufgrund von Datenschutzverstößen stand dabei auch die Veröffentlichung von Stellungnahmen und Hinweisen zu ausgewählten Themen im Vordergrund.

Bußgelder

Die tschechische Aufsichtsbehörde hat im April 2024 ein Bußgeld in Höhe von 13,9 Mio. Euro wegen Verstoßes gegen Art. 6 und 13 Abs. 1 DSGVO verhängt. Das betreffende Unternehmen hatte von den Nutzern seiner Antivirensoftware Daten erhoben und diese ohne das Vorliegen einer Rechtsgrundlage an seine Schwesterunternehmen übermittelt. Die Aufsichtsbehörde stellte außerdem fest, dass die Nutzer seitens des Unternehmens nicht ausreichend über die besagte Datenübermittlung informiert wurden. Aus Sicht der Aufsichtsbehörde war der Verstoß vor allem deshalb besonders schwerwiegend, weil es sich bei dem Verantwortlichen um einen der führenden Experten für Cybersicherheit handelt.

Im Juni 2024 hat die italienische Aufsichtsbehörde (GPDP) ein Bußgeld in Höhe von 6,4 Mio. Euro sowie verschiedene andere Maßnahmen gegen das Unternehmen Eni Plenitude S.p.A. Società Benefit wegen unerwünschter Telefonanrufe verhängt. Das Unternehmen kontaktierte zahlreiche Personen, um für seine Produkte zu werben. Im Rahmen ihrer Untersuchung stellte die GPDP fest, dass diverse Kontaktaufnahmen erfolgten, ohne dass die Betroffenen zuvor ihre Zustimmung erteilt hatten. Die GPDP stellte in der Folge Verstöße gegen Art. 5 (Grundsätze der Datenverarbeitung), 6 (Rechtmäßigkeit der Verarbeitung), 24 (Verantwortung des Verantwortlichen), 25 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen und 28 (Auftragsverarbeitung) DSGVO fest.

Weil die schwedische Avanza Bank AB den Facebook-Pixel nutzte und wegen falscher Einstellungen Daten von bis zu einer Million Kunden an Meta übermittelte, verhängte die schwedische Aufsichtsbehörde (IMY) im Juni 2024 ein Bußgeld in Höhe von 15 Mio. SEK wegen Verstoßes gegen Art. 5 Abs. 1 lit. f), 32 Abs. 1 DSGVO. IMY war der Ansicht, das Unternehmen habe keine ausreichenden Sicherheitsmaßnahmen ergriffen, um die Datenübermittlung zu verhindern oder jedenfalls frühzeitig zu erkennen.

Nachdem die niederländische Datenschutzaufsichtsbehörde (AP) wegen der Verletzung von Informationspflichten und Verstoßes gegen den Transparenzgrundsatz bereits im Dezember 2023 ein Bußgeld in Höhe von 10 Mio. Euro gegen Uber verhängt hatte, erhielt das Unternehmen von der AP im August 2024 ein weiteres Bußgeld in Höhe von 290 Mio. Euro wegen der Übermittlung der Daten von europäischen Fahrern – darunter auch sensible Daten wie Konto-, Zahlungs- und Standortdaten, Ausweispapiere und strafrechtliche und medizinische Daten – ohne ausreichende Schutzmaßnahmen in die USA.

Aufgrund der teilweise unverschlüsselten Speicherung von Nutzer-Passwörtern hat die irische Datenschutzbehörde (DPC) im September 2024 ein Bußgeld in Höhe von 91 Mio. Euro gegen die Meta Platforms Ireland Limited verhängt. Die DPC stellte im Anschluss an ihre Untersuchung fest, dass Meta hierdurch in mehrerlei Hinsicht gegen die Vorgaben der DSGVO verstoßen hat: gegen Melde- und Dokumentationsverpflichtungen im Zusammenhang mit Datenschutzverstößen (Art. 33 DSGVO) sowie gegen Art. 5 Abs. 1 lit. f) DSGVO und Art. 32 Abs. 1 DSGVO wegen unzureichender technischer und organisatorischer Maßnahmen.

Ein weiteres Bußgeld in Höhe von 310 Mio. Euro verhängte die DPC im Oktober 2024 gegen die LinkedIn Unlimited Company. Inhaltlich ging es um die Verarbeitung der personenbezogenen Daten von LinkedIn-Nutzern zum Zwecke der Verhaltensanalyse und der gezielten Werbung sowie die Rechtmäßigkeit, Fairness und Transparenz der Prozesse. Die DPC stellte unter anderem fest, dass es an einer Rechtsgrundlage für die in Rede stehenden Datenverarbeitungsprozesse fehlte. Zudem liege ein Verstoß gegen die Informationspflichten der Art. 13 und 14 DSGVO sowie den Grundsatz der Fairness aus Art. 5 Abs. 1 lit. a) DSGVO vor.

Stellungnahmen und Hinweise

Die Bonner EuroPriSe Cert GmbH hat im Februar 2024 als erste Stelle in Deutschland von der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) die Befugnis erhalten, Datenverarbeitungsprozesse von Auftragsverarbeitern

zu zertifizieren. Das von der EuroPriSe Cert GmbH ausgestellte Zertifikat „European Privacy Seal“ soll Auftragsverarbeitern bescheinigen, dass ihre Datenverarbeitungsprozesse den Anforderungen des europäischen Datenschutzrechts entsprechen.

Im Mai 2024 hat die Sächsische Datenschutz- und Transparenzbeauftragte (SDTB) etwa 30.000 sächsische Internetauftritte im Hinblick auf Datenschutzverstöße untersucht. Dabei setzte sich die SDTB vor allem auch mit der Nutzung des Dienstes Google Analytics auseinander. Im Rahmen ihrer Überprüfung stellte die Datenschutzbeauftragte fest, dass Webseitenbetreiber den geltenden Anforderungen in 2.300 Fällen nicht in erforderlichem Umfang nachkamen. Die Betroffenen wurden aufgefordert, die Datenschutzverstöße zu beseitigen und alle rechtswidrig erhobenen Daten zu löschen.

Angesichts der zunehmenden Relevanz von Digitalisierung und künstlicher Intelligenz im Bewerbungsverfahren hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) im Juni 2024 ein Positionspapier zu Bewerberdatenschutz und Recruiting veröffentlicht. Dabei stellte er zunächst heraus, dass Bewerbungsunterlagen eine Vielzahl sensibler Daten enthalten, weshalb der datenschutzkonforme Umgang von größter Wichtigkeit sei, und ging anschließend auf die unterschiedlichen Phasen des Recruiting-Prozesses sowie einige konkrete Fragestellungen ein.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) hat im Juni 2024 über eine Informationskampagne zu den Regeln des Datenschutzes bei Newslettern und E-Mail-Werbung informiert. Ziel der Kampagne war es, die Verantwortlichen für die Thematik zu sensibilisieren und die Anzahl von Verstößen zu verringern.

Ausblick 2025

Verschiedene Datenschutzthemen aus den Vorjahren, wie etwa Fragestellungen rund um das Auskunftsrecht nach Art. 15 DSGVO sowie die Ausgestaltung des Nutzer-Trackings und die rechtskonforme Einholung und Verwaltung von Nutzereinwilligungen, werden auch im Jahr 2025 eine Rolle spielen. Daneben ist mit neuen datenschutzrechtlichen Themen zu rechnen.

Dem EuGH liegen derzeit zwei Vorabersuchen zu der Frage, wann eine Auskunftsanfrage missbräuchlich ist, vor (Rechtssache C-416/23). In einem der beiden Fälle geht es um die potentiell manipulative Nutzung des Rechts auf Auskunftsersuchen in einem exzessiven Ausmaß. In dem anderen Fall geht es um Auskunftsanfragen, die aufgrund ihrer Quantität rechtsmissbräuchlich sein könnten. Die Entscheidung des EuGH in dieser Sache bleibt mit Spannung abzuwarten.

Anfang September 2024 hat die Bundesregierung in Umsetzung von § 26 TDDDG die Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (EinwV) verabschiedet. Die neue Verordnung sieht unter anderem vor, dass der Dienst zur Einwilligungsverwaltung bei der erstmaligen Inanspruchnahme eines digitalen Dienstes durch den Endnutzer dessen Einstellungen speichert, und gibt vor, welche Einwilligungen mittels des Dienstes verwaltet werden können. Außerdem ist geregelt, welche Voraussetzungen ein Verwaltungsdienst erfüllen muss, um nutzerfreundlich zu sein. Bundestag und Bundesrat müssen der neuen Verordnung noch zustimmen.

Darüber hinaus haben das Bundesministerium für Arbeit und Soziales (BMAS) und das Bundesministerium des Innern und für Heimat (BMI) Anfang Oktober 2024 ihren Referentenentwurf eines Gesetzes zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt (Beschäftigtendatengesetz, BeschDG) vorgelegt. Ziel des Gesetzes ist es, einen Ausgleich zwischen den Interessen der Betriebe und der Beschäftigten zu schaffen und die Beschäftigten in der digitalen Arbeitswelt zu schützen. Der Referentenentwurf sieht unter anderem umfassende Regelungen zur Erforderlichkeitsprüfung sowie der Einwilligungserteilung im Arbeitsverhältnis vor. Inwieweit das Vorhaben in der nächsten Legislaturperiode nach den Neuwahlen wieder aufgegriffen wird und welche Änderungen dann noch vorgesehen werden, bleibt abzuwarten.

Über die datenschutzrechtlichen Geschehnisse und Herausforderungen, die das Jahr 2025 mit sich bringt, wird das Datenschutzteam von BRANDI Sie natürlich auch im neuen Jahr auf dem Laufenden halten. Außerdem möchten wir Sie in mittlerweile bewährter Tradition bereits jetzt zu unserem nächsten Datenschutzrechtstag einladen. Die Veranstaltung findet am 16. Mai 2024 statt. Freuen Sie sich schon jetzt auf interessante Vorträge und spannende Diskussionen. Mit uns diskutiert Prof. Ulrich Kelber, ehemaliger Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI).

Christina Prowald

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net