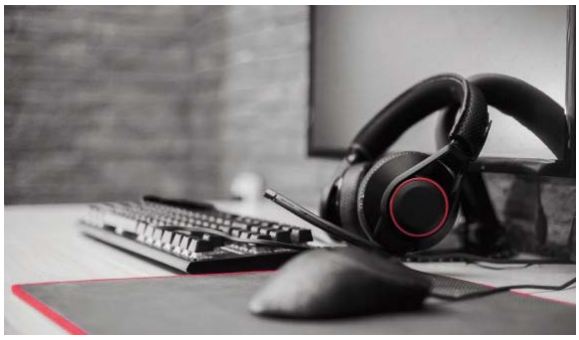
ADVANT Beiten

Datenschutz-Ticker

Juli 2024



+++ DIGITALISIERUNG IM GESUNDHEITSWESEN: NEUERUNGEN FÜR CLOUD-COMPUTING IN KRAFT +++ EUGH: KLAGEBEFUGNIS VON VERBRAUCHERVERBÄNDEN BEI DSGVO-VERSTÖßEN BESTÄTIGT +++ BAG: VERARBEITUNG VON GESUNDHEITSDATEN IM ARBEITSVERHÄLTNIS +++ DATENSCHUTZBEHÖRDE HAMBURG: LARGE LANGUAGE MODELS SPEICHERN KEINE PERSONENBEZOGENEN DATEN +++

1. Gesetzesänderungen

+++ DIGITALISIERUNG IM GESUNDHEITSWESEN: NEUERUNGEN FÜR CLOUD-COMPUTING IN KRAFT +++

Der Bundestag hatte im Dezember 2023 das „Gesetz zur Beschleunigung der Digitalisierung im Gesundheitswesen" (Digital-Gesetz – DigiG) sowie das „Gesetz zur verbesserten Nutzung von Gesundheitsdaten" (Gesundheitsdatennutzungsgesetz – GDNG) beschlossen (siehe AB Datenschutz-Ticker Dezember 2023). Beide Gesetze sind am 26. März 2024 in Kraft getreten, wobei einige Regelungen, die durch das DigiG geändert wurden, nun seit dem 1. Juli 2024 ihre Wirkung entfalten. Dies betrifft unter anderem die Cybersicherheitsvorgaben aus dem SGB V für cloudbasierte Informationssysteme, die zur Verarbeitung von Gesundheits- und Sozialdaten genutzt werden. Solche Informationssysteme müssen nun mit dem „Kriterienkatalog C5" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) konform sein oder jedenfalls ein Zertifikat mit vergleichbarem Sicherheitsniveau aufweisen. Darüber hinaus werden strenge Anforderungen an den Ort der Datenverarbeitungen gestellt und muss die datenverarbeitende Stelle

über eine Niederlassung in Deutschland verfügen. Damit werden Mindestanforderungen an die IT-Sicherheit des Cloud-Einsatzes im Gesundheitswesen aufgestellt.

Zum Wortlaut des DigiG (v. 1. November 2023)

Fragen und Antworten zum DigiG vom Bundesministerium für Gesundheit (v. 25. Juni 2024)

2. Rechtsprechung

+++ EUGH: KLAGEBEFUGNIS VON VERBRAUCHERVERBÄNDEN BEI DSGVO-VERSTÖßEN BESTÄTIGT +++

Der EuGH hat erneut entschieden, dass Verbraucherverbände bei Verstößen gegen die DSGVO klagen dürfen. Der BGH zweifelte an der Zulässigkeit der Klage durch den Verbraucherzentrale Bundesverband (vzvb) gegen Meta Platforms Ireland und legte dem EuGH die Frage vor, ob der vzvb klagebefugt sei. Dies bestätigte der EuGH unter Bezugnahme auf sein Urteil vom 28. April 2022 (Az. C-319/20), in dem er die Voraussetzungen für ein Verbandsklagerecht ausgelegt hatte (siehe AB Datenschutz-Ticker Mai 2022). In der aktuellen Entscheidung klärt der EuGH, ob eine Informationspflichtverletzung bereits eine Rechtsverletzung „infolge der Verarbeitung" darstellt, und bejaht dies. Die Informationspflicht gemäß Art. 13 DSGVO stelle an sich keine Verarbeitung dar. Die Bereitstellung von Informationen nach der DSGVO sei aber Teil des Informationsrechts der Betroffenen und damit Voraussetzung einer rechtmäßigen Verarbeitung nach Art. 6 DSGVO. Damit seien die Rechte der Betroffenen „infolge einer Verarbeitung" verletzt, wenn es zu einem Defizit in der Informationsbereitstellung komme und dadurch beispielsweise eine Einwilligung nicht wirksam erteilt werden konnte.

Zur Pressemitteilung des vzvb (v. 11 Juli 2024)

Zum Urteil des EuGH (v. 11. Juli 2024, C-757/22)

+++ BAG: VERARBEITUNG VON GESUNDHEITSDATEN IM ARBEITSVERHÄLTNIS +++

Das Bundesarbeitsgericht hat sich mit der Frage beschäftigt, ob die Verarbeitung von Gesundheitsdaten im Arbeitsverhältnis DSGVO-konform ist, wenn dies der Klärung der Arbeitsunfähigkeit dient. In dem Fall war ein Medizinischer Dienst von einer gesetzlichen Krankenkasse mit der Erstellung einer gutachterlichen Stellungnahme zur Arbeitsunfähigkeit eines Versicherten beauftragt worden, der zugleich Arbeitnehmer des Medizinischen Dienstes war. Im Unternehmen war ein striktes Zugriffskonzept auf Gesundheitsdaten umgesetzt. Die Betriebsärztin, die zum Zugriff auf die Gesundheitsdaten berechtigt war, holte vom behandelnden Arzt des Arbeitnehmers zusätzlich Auskünfte über dessen Gesundheitszustand ein, um darauf basierend das Gutachten erstellen zu können. Dagegen ging der Arbeitnehmer gerichtlich mit der Begründung vor, die Verarbeitung seiner Gesundheitsdaten durch seinen Arbeitgeber sei unzulässig. Das BAG entschied, dass es an einem Verstoß fehle, denn die Verarbeitung der Gesundheitsdaten könne auf Art. 9 Abs. 2 lit. h DSGVO gestützt werden und genüge den Garantien des Art. 9 Abs. 3 DSGVO. Dies begründet das Gericht unter anderem damit, dass zugriffsberechtigte Mitarbeiter des Arbeitgebers ohnehin einer beruflichen Verschwiegenheitspflicht und dem Sozialgeheimnis unterlägen. Außerdem fehle es an einer Vorschrift, die besagt, dass der Arbeitgeber nicht zugleich als Medizinischer Dienst auftreten dürfe.

Zur Pressemitteilung zum Urteil des BAG (v. 20. Juni 2024, 8 AZR 253/20)

3. Behördliche Maßnahmen

+++ BUßGELD VON EUR 2,4 MIO. GEGEN ONLINE-PLATTFORM VINTED +++

Die litauische Datenschutzaufsichtsbehörde Valstybinė duomenų apsaugos inspekcija (SDPI) hat ein Bußgeld in Höhe von knapp EUR 2,4 Mio. gegen den Betreiber der Online-Plattform Vinted verhängt, die den Handel mit Secondhand-Kleidung und weiteren Produkten ermöglicht. Das Bußgeldverfahren wurde von der SDPI als federführende Behörde („One-Stop-Shop") in Zusammenarbeit mit Datenschutzbehörden aus Polen, Frankreich, den Niederlanden, Spanien und Deutschland aufgrund diverser Nutzer-Beschwerden geführt. In diesem Zusammenhang stellte

die Behörde fest, dass das Unternehmen Anträgen auf Löschung von Nutzerdaten („Recht auf Vergessenwerden“) nicht nachgekommen war. Darüber hinaus habe der Plattformbetreiber unzulässiges „Shadow Blocking“ betrieben. Inhalte von Nutzern, die im Verdacht standen, gegen die Plattform-Regeln zu verstoßen, wurden also nicht mehr angezeigt, ohne dass diese darüber informiert wurden. Außerdem hatte das Unternehmen keine ausreichenden technischen und organisatorischen Maßnahmen ergriffen, um die Umsetzung der Rechenschaftspflicht zu gewährleisten und nachweisen zu können, dass es Maßnahmen im Hinblick auf nur mangelhaft erfüllte Auskunftsrechte ergriffen hat.

Zur Pressemitteilung der Behörde (v. 2. Juli 2024, Englisch)

+++ BUßGELD VON EUR 6,4 MIO. GEGEN ITALIENISCHES ENERGIEUNTERNEHMEN +++

Die italienische Datenschutzbehörde Garante per la Protezione dei Dati Personali (GPDP) hat gegen ein Energieunternehmen ein Bußgeld in Höhe von rund EUR 6,4 Mio. festgesetzt. Bei der Behörde hatte es zahlreiche Beschwerden über unerwünschte Telefonanrufe durch das Unternehmen gegeben. Die Behörde stellte fest, dass für die telefonische Kontaktaufnahme keine Einwilligung der Betroffenen vorlag. Manche Betroffene wurden sogar angerufen, obwohl sie sich in ein öffentliches Register eingetragen hatten, um nicht kontaktiert zu werden. Außerdem verhängte die Behörde ein Verbot jeglicher Weiterverarbeitung der auf unzulässige Weise erlangten Daten.

Zum Bußgeldbescheid der Behörde (v. 6. Juni 2024, Italienisch)

+++ BUßGELD VON EUR 1,3 MIO. GEGEN SCHWEDISCHE BANK +++

Die schwedische Datenschutzbehörde Integritetsskyddsmyndigheten (IMY) hat ein Bußgeld in Höhe von umgerechnet rund EUR 1,3 Mio. gegen eine Bank verhängt. Die Behörde stellte fest, dass die Bank auf ihrer Website und in ihrer App in unzulässiger Weise das Analyse-Tool Facebook-Pixel (jetzt Meta-Pixel) verwendete, wodurch Informationen über beispielsweise Wertpapierbestände und Kontonummern von Kunden an Meta übermittelt wurden. Es waren bis zu einer Million Kunden betroffen. Das Bußgeldverfahren folgte auf eine Selbstanzeige der Bank. Die Behörde warf der Bank vor, dass sie keine geeigneten technischen

und organisatorischen Maßnahmen ergriffen hatte, um ein angemessenes Sicherheitsniveau für die personenbezogenen Daten der Nutzer von Website und App zu gewährleisten.

Zur Pressemitteilung der Behörde (v. 25. Juni 2024, Schwedisch)

Zum Bußgeldbescheid der Behörde (v. 24. Juni 2024, Schwedisch)

4. Stellungnahmen

+++ ABKOMMEN ZWISCHEN DER EU UND JAPAN ZU DATENVERKEHR IN KRAFT +++

Das seit 2019 geltende EU-Japan Economic Partnership Agreement (EPA) wurde zum 1. Juli 2024 um den Datenverkehr für den digitalen Handel erweitert. Ziel ist die Vereinfachung der Übertragung von Daten im wirtschaftlichen Kontext des digitalen Handels und ein effizienter Datenverkehr zwischen Japan und der EU. Mit der Erweiterung wurde ein rechtliches Umfeld geschaffen, durch welches der Datenaustausch für Finanzdienstleistungen oder E-Commerce ohne umständliche Verwaltungs- und Speicheranforderungen ermöglicht wird. Das Abkommen fördert das Konzept des sog. „Data free flow with trust", welches als Leitprinzip für die internationale Zusammenarbeit beim Datenverkehr gilt. Dadurch sollen willkürliche Beschränkungen im grenzüberschreitenden Datenverkehr beseitigt werden sowie wirtschaftliche und soziale Standards durch die Datennutzung erhalten und verbessert werden.

Zur Pressemitteilung der Europäischen Kommission (v. 1. Juli 2024)

+++ DATENSCHUTZBEHÖRDE HAMBURG: LARGE LANGUAGE MODELS SPEICHERN KEINE PERSONENBEZOGENEN DATEN +++

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) hat ein Diskussionspapier zu „Large Language Models und personenbezogenen Daten“ veröffentlicht. Hierin stellt die Behörde fest, dass die bloße Speicherung eines Large Language Models (LLM) keine Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO darstellt. Denn durch die sog. Tokenisierung des Inputs würden sämtliche Texte in kleine Bruchstücke aufgeteilt, sodass sich in den meisten Fällen kein Personenbezug mehr herstellen lasse, auch weil das LLM keine ganzen

Wörter enthält. Weiter führt die Behörde aus, dass, sofern beim Training und/oder Output personenbezogene Daten verarbeitet werden, diese Verarbeitungsvorgänge den Anforderungen der DSGVO entsprechen müssen. Ein datenschutzwidriges Training des LLM soll sich aber nicht auf die Rechtmäßigkeit des Einsatzes eines LLM in einem KI-System auswirken. Mangels Speicherung personenbezogener Daten im LLM könnten die Betroffenenrechte der DSGVO nicht das Modell selbst zum Gegenstand haben. Ansprüche auf Auskunft, Löschung oder Berichtigung seien vielmehr an den Verantwortlichen für Input und Output zu richten.

Zum Diskussionspapier des HmbBfDI

+++ BAFIN: UMSETZUNGSHINWEISE ZU DORA +++

Ab dem 17. Januar 2025 müssen Unternehmen im Finanzsektor den Digital Operational Resilience Act (DORA) beachten. DORA stellt als europäische Verordnung IT-Compliance-Anforderungen auf und soll damit den Finanzmarkt vor Cyberrisiken und IT-Sicherheitsvorfällen schützen. Dafür hat die BaFin nun Umsetzungshinweise für das Risikomanagement in der Informations- und Kommunikationstechnologie (IKT) erlassen. In ihrer ca. vierzigseitigen unverbindlichen Hilfestellung werden die bank- und versicherungsaufsichtlichen Anforderungen an die Informationstechnik praxisbezogen beleuchtet. Als Neuerung greift die Hilfestellung unter anderem die Einführung einer IKT-Geschäftsfortführungsleitlinie auf. Diese soll konkret für IKT-Vorfälle einen Fahrplan vorsehen, insbesondere zur Schadensbegrenzung verbunden mit der Wiederaufnahme der Tätigkeiten. Auch im Rahmen der Wiederherstellungspläne gilt mehr Weitsicht, denn die Auswirkungen des Klimawandels, Insider-Angriffe, politische und soziale Instabilität und großflächige Stromausfälle sollen nun mitberücksichtigt werden.

Zur Pressemitteilung der BaFin (v. 8. Juli 2024)

Zum Wortlaut des DORA

Ihre Ansprechpartner

Für Rückfragen sprechen Sie den ADVANT Beiten Anwalt Ihres Vertrauens an oder wenden Sie sich direkt an das ADVANT Beiten Datenschutz-Team:

Büro Frankfurt
Mainzer Landstrasse 36 | 60325 Frankfurt am Main

Dr. Andreas Lober

+49 69 756095-582
vCard

Susanne Klein, LL.M.

+49 69 756095-582
vCard

Lennart Kriebel

+49 69 756095-582
vCard

Fabian Eckstein, LL.M.

+49 69 756095-582
vCard

Jason Komninos, LL.M.

+49 69 756095-582
vCard

Mirjam Kaiser

+49 69 756095-582
vCard

Büro Düsseldorf
Cecilienallee 7 | 40474 Düsseldorf

Mathias Zimmer-Goertz

+49 211 518989-144
vCard

Christian Frederik Döpke, LL.M.
+49 211 518989-144
vCard

Büro München
Ganghoferstrasse 33 | 80339 München

Katharina Mayerbacher

+89 35065-1363
vCard

Dr. Birgit Münchbach

+89 35065-1312
vCard

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH ist Mitglied von ADVANT, einer Vereinigung unabhängiger Anwaltskanzleien. Jede Mitgliedskanzlei ist eine separate und eigenständige Rechtspersönlichkeit, die nur für ihr eigenes Handeln und Unterlassen haftet. Dieser Datenschutz-Ticker wurde in Zusammenarbeit mit den ADVANT Partnerkanzleien Nctm und Altana erstellt.

REDAKTION (verantwortlich)
Dr. Andreas Lober | Rechtsanwalt

BB-Datenschutz-Ticker@advant-beiten.com
www.advant-beiten.com

Hinweis: Zur besseren Lesbarkeit verzichten wir auf die Verwendung männlicher und weiblicher Sprachformen. Wir verwenden das generische Maskulinum, womit alle Geschlechter gleichermaßen gemeint sind.

Zur Newsletter Anmeldung

E-Mail weiterleiten

Hinweise

Diese Veröffentlichung stellt keine Rechtsberatung dar.

Wenn Sie künftig keine Informationen erhalten möchten, können Sie sich jederzeit abmelden.

Impressum

ADVANT Beiten
Beiten Burkhardt Rechtsanwaltsgesellschaft mbH
(Herausgeber)
Ganghoferstraße 33, 80339 München
AG München HR B 155350/USt.-Idnr: DE-811218811
Weitere Informationen (Impressumsangaben) unter:
https://www.advant-beiten.com/de/impressum