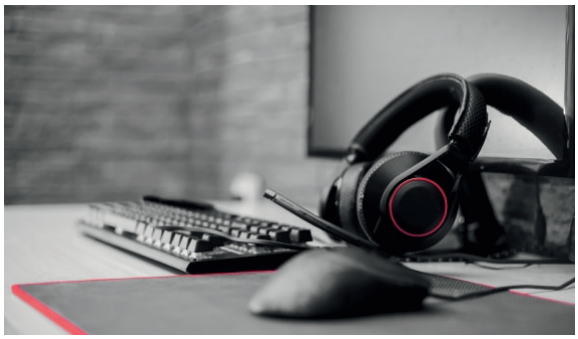
ADVANT Beiten

Datenschutz-Ticker

März 2024



+++ EU-PARLAMENT BESCHLIEßT AI ACT UND CYBER RESILIENCE ACT +++ EUGH: EUROPOL UND MITGLIEDSTAAT HAFTEN GEMEINSAM FÜR DATENSCHUTZVERSTOß +++ OVG NIEDERSACHSEN: GEBURTSDATUM ALS PFLICHTFELD IN WEBSHOP RECHTSWIDRIG +++ BUßGELD VON USD 16,5 MIO. WEGEN VERKAUF VON BROWSER-DATEN +++ EUROPAWEITE PRÜFAKTION ZUM AUSKUNFTSRECHT +++

1. Gesetzesänderungen

+++ AI ACT DURCH EU-PARLAMENT BESCHLOSSEN +++

Das Europäische Parlament hat das Gesetz über künstliche Intelligenz (AI Act) beschlossen. Nach eigener Aussage soll es das weltweit erste verbindliche Gesetz zu KI sein. Ziel des Gesetzes ist, dass nur solche KI-Systeme auf den europäischen Markt gebracht und genutzt werden, die sowohl sicher sind als auch die Grundrechte und Werte der EU respektieren. Der AI Act folgt einem risikobasierten Ansatz, wonach bestimmte KI-Systeme verboten sind, z.B. Emotionserkennungssysteme am Arbeitsplatz sowie das Bewerten von sozialem Verhalten. Sog. Hochrisiko-KI-Systeme sind nur bei Einhaltung bestimmter Pflichten zulässig. Als hochriskant gelten KI-Systeme, die in den Bereichen kritische Infrastruktur, Migration, Grenzkontrollen, Bildung oder Beschäftigung eingesetzt werden. Daneben gelten für alle Systeme Informations- und Transparenzpflichten. Sobald der Rat den AI Act angenommen hat, wird dieser unmittelbar in der gesamten EU gelten und ist – bis auf einige Ausnahmen – 24 Monate nach dem Inkrafttreten uneingeschränkt anwendbar.

Zum Text des AI Act (v. 13. März 2024)

Zur Pressemitteilung des EU-Parlaments (v. 13. März 2024)

+++ EU-PARLAMENT BESCHLIEßT CYBER RESILIENCE ACT +++

Das EU-Parlament hat außerdem den Text für die Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen angenommen, auch Cyber Resilience Act (CRA) genannt. Der CRA soll die NIS2-Richtlinie ergänzen, die sich vor allem mit der Sicherheit der Informations- und Kommunikationstechnik bei kritischer Infrastruktur befasst (siehe AB Blogbeitrag vom 8. Februar 2024). In den Anwendungsbereich des CRA fallen Software- oder Hardwareprodukte sowie mit ihnen verbundene Cloudlösungen. Adressaten sind insbesondere Hersteller, Importeure und Händler. Durch den Grundsatz „Security by Design" werden diese verpflichtet, fortlaufend für die Cybersicherheit der Produkte zu sorgen, und bleiben während des gesamten Lebenszyklus des Produkts dafür verantwortlich. Dazu muss eine ständige Risikobewertung erfolgen, einschließlich zu erfüllender Informationspflichten und Produktdokumentation. Bei Verstößen sieht der CRA Bußgelder von bis zu EUR 15 Mio. oder 5 Prozent des gesamten weltweiten Jahresumsatzes vor. Der CRA muss noch durch den Rat angenommen werden und tritt sodann nach 36 Monaten in Kraft.

Zum Text des CRA (v. 12. März 2024)

Zur Pressemitteilung des EU-Parlaments (v. 12. März 2024, Englisch)

2. Rechtsprechung

+++ EUGH: EUROPOL UND MITGLIEDSTAAT HAFTEN GEMEINSAM FÜR DATENSCHUTZVERSTOß +++

Der Europäische Gerichtshof (EuGH) hat entschieden, dass Europol und ein Mitgliedstaat gesamtschuldnerisch haften, wenn aufgrund einer widerrechtlichen Datenverarbeitung im Rahmen der Zusammenarbeit von Europol und diesem Mitgliedstaat ein Schaden eingetreten ist. Aufgrund eins Mordfalls führten die slowakischen Strafbehörden Ermittlungen gegen den Kläger durch und baten Europol um die Extrahierung von Daten von dessen Mobiltelefonen. Nachdem Europol den Behörden die angeforderten Daten übermittelt hatte, veröffentlichte die slowakische Presse Informationen aus intimer Kommunikation des Klägers. Dieser erhob Klage gegen Europol wegen einer Datenschutzverletzung und forderte immateriellen Schadensersatz. Der EuGH entschied, dass die Weitergabe der intimen Daten an die Presse einen Datenschutzverstoß darstellte, für welchen Europol und die Slowakei gemeinsam haften. Nach Auffassung des EuGH muss die betroffene Person lediglich nachweisen, dass es bei der Zusammenarbeit der Behörden zu einer widerrechtlichen Datenverarbeitung gekommen ist. Nicht erforderlich ist, dass die

betroffene Person auch nachweist, welcher dieser beiden Stellen die widerrechtliche Verarbeitung zuzurechnen ist. Dem Kläger wurde Schadensersatz in Höhe von EUR 2.000 zugesprochen.

Zum Urteil des EuGH (v. 5. März 2024, C-755/21 P)

Zur Pressemitteilung des EuGH (v. 5. März 2024)

+++ OVG NIEDERSACHSEN: GEBURTSDATUM ALS PFLICHTFELD IN WEBSHOP RECHTSWIDRIG +++

Das Oberverwaltungsgericht (OVG) Niedersachsen hat festgestellt, dass eine Apotheke in ihrem Online-Shop das Geburtsdatum nicht als zwingende Angabe von den Kunden abfragen darf. Die betreffende Apotheke wurde zunächst vom Landesbeauftragten für den Datenschutz Niedersachsen aufgefordert, es zu unterlassen, unabhängig von der Art des bestellten Medikaments das Geburtsdatum der Besteller abzufragen. Gegen diese Anordnung erhob die Apotheke Klage vor dem Verwaltungsgericht Hannover, welches die Klage abwies. Das OVG Niedersachsen bestätigt diese Auffassung. Die Verarbeitung des Geburtsdatums sei datenschutzrechtlich üblicherweise nicht zur Erfüllung eines Vertrags erforderlich. Insbesondere sei das Datum nicht zur Identifikation der Kunden erforderlich. Selbst für eine Prüfung, ob Minderjährige im Webshop bestellen, könne der Betreiber die Volljährigkeit abfragen und benötige nicht das genaue Geburtsdatum. Es bestehe auch keine gesetzliche Pflicht zur Abfrage des Geburtsdatums, weil die Apotheke die Online-Bestellung nur für rezeptfreie Produkte auf ihrer Website anbiete. Auf berechtigte Interessen könne sie sich ebenfalls nicht berufen, da statt der Abfrage des Geburtsdatums das mildere, gleich effiziente Mittel der Abfrage der Volljährigkeit zur Verfügung stehe. Auch für das etwaige Eintreiben von offenen Forderungen sei das Geburtsdatum nicht erforderlich.

Zum Beschluss des OVG Niedersachsen (v. 23. Januar 2024, 14 LA 1/24)

Zur Pressemitteilung des LfD Niedersachsen (v. 20. März 2024)

+++ VG BERLIN: AUSKUNFTSANSPRUCH AUCH BEI HOHEM RECHERCHEAUFWAND BEGRÜNDET +++

Das Verwaltungsgericht (VG) Berlin hat entschieden, dass ein Auskunftsanspruch nach Art. 15 DSGVO auch dann nicht unverhältnismäßig ist, wenn die Erfüllung für den Verantwortlichen mit einem erheblichen Aufwand verbunden ist. Der Kläger verlangte von einer Behörde, ihm Auskunft über die zu ihm verarbeiteten personenbezogenen

Daten zu erteilen und Kopien von sämtlichen Vorgängen zu übersenden, in denen diese Daten enthalten seien. Die Behörde erteilte dem Kläger daraufhin Auskunft über die in den IT-Systemen gespeicherten Daten, die Kategorien sowie die Empfänger dieser Daten. Kopien der Dokumente wurden nicht herausgegeben. Der Kläger erhob daraufhin Klage auf Herausgabe der Kopien. Die Beklagte berief sich in ihrer Verteidigung unter anderem auf einen unverhältnismäßigen Aufwand, da sie zur Erfüllung des Anspruchs mehr als 5.000 Seiten Akten prüfen müsse. Das Gericht gab dem Kläger Recht und bejahte den Kopieanspruch vollumfänglich. Der Kläger habe ein berechtigtes Interesse an der Herausgabe, um potentielle Empfänger selbst zu ermitteln. Auch der mit dem Anspruch verbundene erhebliche Arbeitsaufwand bei der Beklagten führe nicht zu einer Unverhältnismäßigkeit oder einem Rechtsmissbrauch.

Zum Urteil des VG Berlin (v. 6. Februar 2024, 1 K 187/21)

3. Behördliche Maßnahmen

+++ BUßGELD VON EUR 2,8 MIO. GEGEN UNICREDIT NACH CYBERANGRIFF +++

Die italienische Datenschutzbehörde Garante per la Protezione dei Dati Personali (GPDP) hat ein Bußgeld von EUR 2,8 Mio. gegen die italienische Bank UniCredit S.p.A. verhängt. Bereits 2018 meldete die Bank der Behörde einen Sicherheitsvorfall, der zu umfangreichen Untersuchungen durch die GPDP führte. Aufgrund eines Cyberangriffs auf das Banking-Portal von UniCredit waren Vor- und Nachnamen, Startnummern und Identifikationscodes von etwa 778.000 Kunden offengelegt worden. In knapp 7.000 Fällen hatten die Täter zudem die PINs für den Zugriff auf das Portal erbeutet. Die GDPD stellte bei ihrer Untersuchung mehrere Datenschutzverletzungen fest. So hatte die Bank insbesondere keine technischen und organisatorischen Sicherheitsmaßnahmen ergriffen, die geeignet gewesen wären, Cyberangriffe wirksam abzuwehren. Auch gab es keine Vorkehrungen, um Kunden daran zu hindern, schwache PINs zu verwenden. Im Zusammenhang mit der Untersuchung wurde auch ein weiteres Bußgeld von EUR 800.000 gegen die NTT Data Italia verhängt, einen für UniCredit tätigen Auftragsverarbeiter. Dieser hatte die Bank erst verspätet über die Datenpanne informiert und zudem gewisse Dienstleistungen unberechtigterweise an andere Sub-Unternehmer ausgelagert.

Zum Bußgeldbescheid der GPDP (v. 8. Februar 2024, Italienisch)

Zur Pressemitteilung der GPDP (v. 7. März 2024, Italienisch)

+++ BUßGELD VON USD 16,5 MIO. WEGEN VERKAUF VON BROWSER-DATEN +++

Die US-amerikanische Federal Trade Commission (FTC) hat gegen die Avast Limited und deren Tochterunternehmen Avast Software und Jumpshot ein Bußgeld von USD 16,5 Mio., also umgerechnet ca. EUR 15,1 Mio. verhängt. Die von Avast vertriebene Software soll die Privatsphäre der Kunden schützen, indem Online-Tracking durch Dritte verhindert wird. Die Browsererweiterungen und Antiviren-Software, wie z.B. AVG Online Security, sammelten jedoch selbst heimlich Daten der Kunden, z.B. Suchbegriffe, Cookie-Daten und URLs der besuchten Webseiten. Diese Daten verkaufte Avast an über 100 Unternehmen, darunter Google und Microsoft. Die FTC sah darin einen Datenschutzverstoß und ein betrügerisches Verhalten von Avast, da die Daten in Klarform und ohne Einwilligung weitergegeben und das besondere Vertrauen der Kunden in den Schutz ihrer Privatsphäre ausgenutzt wurden. Erschwerend wurde bewertet, dass sich aus den Daten Rückschlüsse auf sensible Informationen wie religiöse und politische Ansichten sowie Gesundheitsdaten der Kunden ziehen ließen. Avast wurde verpflichtet, die bereits gesammelten Daten zu löschen und für eine Weitergabe der Daten zuvor die Einwilligung der Kunden einzuholen.

Zur Entscheidung der FTC (v. 19. Januar 2024, Englisch)

+++ EUROPÄISCHE KOMMISSION VERSTÖßT BEI NUTZUNG VON MICROSOFT 365 GEGEN DATENSCHUTZ +++

Der Europäische Datenschutzbeauftragte (EDSB) hat festgestellt, dass die Europäische Kommission Microsoft 365 datenschutzwidrig einsetzt und damit gegen die DSGVO verstößt. Insbesondere hat es die Kommission nach Auffassung des EDSB versäumt, ausreichende Garantien für die Verarbeitung von personenbezogenen Daten außerhalb der EU/des EWR zu ergreifen. Darüber hinaus habe die Kommission in ihrem Vertrag mit Microsoft nicht hinreichend festgelegt, welche Arten personenbezogener Daten zu welchen expliziten und spezifizierten Zwecken bei der Nutzung von Microsoft 365 erhoben werden. Der EDSB hat der Kommission daher umfassende Abhilfemaßnahmen auferlegt, die im Anhang zu seiner Pressemitteilung aufgelistet sind und bis zum 9. Dezember 2024 erfüllt werden müssen. Ebenfalls ab diesem Stichtag ist die Kommission verpflichtet, alle Datenströme an Microsoft und deren Unterauftragsverarbeiter in Drittländern, für die kein Angemessenheitsbeschluss vorliegt, auszusetzen.

Zur Pressemitteilung des EDSB (v. 11. März 2024, Englisch)

4. Stellungnahmen

+++ EUROPAWEITE PRÜFAKTION ZUM AUSKUNFTSRECHT +++

Der Europäische Datenschutzausschuss (EDSA) hat auf Vorschlag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) die Umsetzung des Auskunftsrechts als Thema seiner dritten koordinierten Prüfaktion ausgewählt und diese nun gestartet. In Deutschland nehmen die Datenschutzbehörden aus Bayern (BayLDA), Brandenburg, Mecklenburg-Vorpommern, Niedersachsen, Rheinland-Pfalz, dem Saarland und Schleswig-Holstein sowie der BfDI teil. Ziel der Aktion ist es, zu beurteilen, wie privat- und öffentlich-rechtliche Organisationen das Auskunftsrecht in der Praxis umsetzen und inwiefern weitere Maßnahmen oder Klarstellungen durch die Datenschutzbehörden sinnvoll sind. In einem ersten Schritt werden dazu Fragebögen an Unternehmen und Organisationen versendet. Auf deren Grundlage sollen in einem zweiten Schritt ggf. weitere behördliche Untersuchungen eingeleitet werden. Die Ergebnisse der Aktion sollen gemeinsam analysiert und über weitere Maßnahmen entschieden werden. Der EDSA wird die Ergebnisse dieser Analyse nach Abschluss der Maßnahmen veröffentlichen.

Zur Pressemitteilung der Datenschutzkonferenz (v. 28. Februar 2024)

Zur Pressemitteilung des EDSA (v. 28. Februar 2024, Englisch)

+++ EDSA VERÖFFENTLICHT STELLUNGNAHME ZUM BEGRIFF DER HAUPTNIEDERLASSUNG +++

Der Europäische Datenschutzausschuss (EDSA) hat aufgrund einer Anfrage der französischen Datenschutzbehörde eine Stellungnahme zum Begriff der Hauptniederlassung und zu den Kriterien für die Anwendung des One-Stop-Shop-Mechanismus verabschiedet. Die Ermittlung der Hauptniederlassung ist wichtig, um in grenzüberschreitenden Fällen die federführende Aufsichtsbehörde festzustellen. Der EDSA ist der Auffassung, dass der Ort der zentralen Verwaltung nur dann als Hauptniederlassung angesehen werden kann, wenn diese Entscheidungen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten trifft und befugt ist, solche Entscheidungen umzusetzen. Keine Hauptniederlassung liegt nach Meinung des EDSA vor, wenn die Entscheidung über die Zwecke und Mittel außerhalb der Europäischen Union getroffen wird. Dann soll der One-Stop-Shop-Mechanismus nicht anwendbar sein.

Zur Stellungnahme des EDSA (v. 13. Februar 2024, Englisch)

Zur Pressemitteilung des EDSA (v. 14. Februar 2024)

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
©Beiten Burkhardt
Rechtsanwaltsgesellschaft mbH

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

Hinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

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

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 Freiburg

Heinrich-von-Stephan-Straße 25 | 79100 Freiburg

Dr. Birgit Münchbach

+49 761 150984-22
vCard

Büro München

Ganghoferstraße 33 | 80339 München

Katharina Mayerbacher

+49 89 35065-1363
vCard

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