Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

so wie der Frühling nun erfreulicherweise endlich bei uns Einzug gehalten hat und sich die Natur rasant entwickelt, gibt es auch wieder Neuigkeiten im Bereich des Datenschutzrechts. Über diese möchten wir Sie mit unserer aktuellen Beratungsinformation informieren.

Große Hoffnungen gab es Ende März 2022 in Bezug auf ein neues Datentransferabkommen zwischen der EU und den USA. Doch derzeit sieht es eher so aus, als könnte das Abkommen wiederum keine Rechtssicherheit bringen. Näheres dazu lesen in unserem ersten Beitrag.

Zudem hat der EuGH festgestellt, dass eine Klagebefugnis für Verbraucherschutzverbänden der DSGVO nicht widerspricht und damit für Verbraucherschutzverbände den Weg zur Verfolgung von Datenschutzverstößen freigemacht. Was dies für Unternehmen bedeutet, lesen Sie in unserem Beitrag.

Das oberste französische Verwaltungsgericht, der Conseil d'Eta, hat sich in einer Entscheidung zur Nutzung von Dienstleistern mit US-Muttergesellschaft durch ein europäisches Unternehmen geäußert. Inwiefern nach dieser Entscheidung Dienstleister mit US-Muttergesellschaften genutzt werden können, zeigt unser Beitrag.

Zudem haben wir zwei weitere Gerichtsentscheidungen aufgenommen: Die im Daily Business von Unternehmen häufig anzutreffende Nutzung von Google Fonts, kann zu einem Schadensersatzanspruch führen, wie das LG München entschied. Ferner hat sich das OLG Brandenburg dazu geäußert, ob personenbezogene Daten von Mitarbeitenden zu Abrechnungszwecken an Auftraggeber übermittelt werden dürfen.

Und last but not least, denken Sie daran nicht mehr benötigte 3G-Daten zu löschen. Ein paar Hinweise haben wir am Schluss dieser Beratungsinformation zusammengestellt.

Ich wünsche Ihnen eine spannende Lektüre und einen schönen restlichen Mai!

Ihr Asmus Eggert

Inhalt

Schrems III? - Neues System für den Datenaustausch zwischen der EU und den USA – Reaktion von Max Schrems

Insbesondere aufgrund von Gesprächen zwischen der Präsidentin der Europäischen Kommission, Ursula von der Leyen und dem US-Präsidenten Joe Biden gab es in den vergangenen Wochen Hoffnungen auf ein neues Transatlantik-Datentransferabkommen zwischen der EU und den USA. Ursula von der Leyen hatte am 25. März 2022 in einer Erklärung zusammen mit Joe Biden bekanntgegeben, dass die EU und die USA eine "grundsätzliche Einigung" über ein neues System für den Datenaustausch zwischen der EU und den USA erzielt hätten. Das Abkommen wird von vielen Unternehmen sehnlichst erwartet, da eine datenschutzkonforme Datenübermittlung zwischen den USA und der EU derzeit kaum möglich ist. Als realistischer Zeitpunkt für eine endgültige und vor allem rechtlich verbindliche Einigung wird Ende des Jahres genannt.

Jedoch befürchtet der Datenschutzaktivist Max Schrems, der schon die Vorgängerabkommen (*Safe Harbour* sowie *Privacy Shield)* vor dem Europäischen Gerichtshof (EuGH) gerichtlich zu Fall gebracht hatte, angesichts der aktuellen Absprachen eine Schrems III-Entscheidung. So kommentierte er: "*Wie es derzeit aussieht, könnten wir das gleiche Spiel jetzt ein drittes Mal spielen. Der Deal war offenbar ein Symbol, das von van der Leyen gewollt war, aber keinen Rückhalt der Experten in Brüssel hat, da sich die USA nicht bewegt haben. Besonders empörend ist, dass die USA angeblich den Krieg gegen die Ukraine genutzt haben, um die EU in dieser Wirtschaftsfrage unter Druck zu setzen. [...] Unternehmen drohen weitere Jahre der Rechtsunsicherheit.*"

Praxishinweis: Das Thema Datenaustausch zwischen der EU und den USA bleibt damit wohl auch weiterhin - trotz der Absichtsbekundungen - sehr problematisch. Wer nach den Absichtsbekundungen auf eine schnelle Lösung des Datentransferproblems zwischen der EU und den USA gehofft hatte, dürfte enttäuscht werden. In keinem Fall sollten bereits jetzt Entscheidungen getroffen werden, die auf ein neues Transfer-Abkommen setzen.

Reaktion von Max Schrems: https://lnkd.in/dD4SyHae
Die Presseerklärung des Weißen Hauses: https://lnkd.in/eKKwkdUc
Die Presseerklärung der Europäischen Kommission: https://lnkd.in/eP8Nc_G3
Statement des EDPB (Englisch): https://lnkd.in/esb-KMEb

Sollten Sie Fragen zur datenschutzkonformen Datenübermittlung zwischen den USA und der EU haben, helfen wir Ihnen gerne weiter.

EuGH: Klagebefugnis von Verbraucherschutzverbänden – Abmahnungsgefahr

Der Europäische Gerichtshof (EuGH) hat im Rahmen einer Vorlagefrage unter dem Aktenzeichen C-319/29 entschieden, dass Verbraucherschutzverbände eine Klagebefugnis haben, um DSGVO-Verstöße geltend zu machen. Es ist dabei nicht erforderlich, dass es zuvor einen Auftrag durch einen Betroffenen gab. Ziel ist es den Schutz personenbezogener Daten auf hohem Niveau zu garantieren.

Dem Vorabentscheidungsverfahren ging ein Rechtsstreit des Verbraucherzentrale Bundesverband e.V. (VZBV) gegen Meta (zuvor Facebook) Ireland Ltd. voraus.

Der VZBV beanstandete vor dem Landgericht Berlin unlautere Hinweise in der App von Meta, die Nichteinhaltung der Anforderungen an eine wirksame datenschutzrechtliche Einwilligung sowie eine unangemessene Benachteiligung der Nutzer durch deren AGB.

Der Bundesgerichtshof (BGH) legte dem Europäischen Gerichtshof (EuGH) in diesem Verfahren u.a. Frage vor, ob Verstöße gegen die Datenschutzgrundverordnung (DSGVO) überhaupt von einem Verbraucherschutzverband geltend gemacht werden dürfen.

Der EuGH bejahte mit seinem Urteil nun diese Frage. Solche Klagen könnten unabhängig von der konkreten Verletzung des Recht einer betroffenen Person auf den Schutz ihrer Daten und ohne entsprechenden Auftrag erhoben werden. Die Klagebefugnis unterliegt laut EuGH gerade keiner Einzelfallprüfung in Bezug auf die Verletzung der Rechte einzelner Personen. Ausreichend sei, dass der Verband geltend macht, dass eine Verarbeitung personenbezogener Daten gegen die Rechte des Einzelnen schützende Bestimmungen der DSGVO verstößt und somit geeignet ist die Rechte Betroffener zu verletzen.

Mithin müsse sich die Klage lediglich auf die Verletzung von Rechten stützen, die einer natürlichen Person infolge einer Verarbeitung ihrer personenbezogenen Daten erwachsen können. Dies sei bei der Unterlassungsklage des VZBV gegen Meta der Fall, da Verstöße gegen Art. 12 Abs. 1 S. 1, Art. 13 Abs. 1 lit. c) und lit. e) DSGVO vorlägen.

Das Urteil des EuGH finden Sie hier: https://lnkd.in/eTjtWcJc

Praxishinweis: Unternehmen müssen nun mit entsprechenden Abmahnungen von Verbraucherschutzverbänden bei Datenschutzverstößen rechnen und sollten dieser Gefahr durch eine Überprüfung, ob die datenschutzrechtlichen Anforderungen eingehalten werden, zuvorkommen. Besonderes Augenmerk sollte auf die Unternehmens-Webseite und dort vorhandene Einwilligungserklärungen, Datenschutzinformationen und Cookie-Banner gelegt werden.

Urteil des Conseil d´Eta zur Frage des ausreichenden Schutzes personenbezogener Daten bei US-Dienstleistern

Der Conseil d´Eta, Frankreichs oberstes Verwaltungsgericht, entschied am 12. März 2021, dass der Datentransfer zu Amazon Web Services (AWS) in den USA unter Einhaltung bestimmter Bedingungen rechtmäßig erfolgen kann. Konkret ging es um die Plattform Doctolib, welche bei Amazon Web Services (AWS) gehostet wird.

Doctolib ist ein Portal zur Terminvereinbarung von Arztbesuchen und war im Zuge der Corona-Pandemie in Frankreich vom Gesundheitsministerium mit der Verwaltung von Online-Impfterminen betraut worden. Doctolib nutzt für das Hosten der Daten die Amazon Web Services Sarl in Luxemburg, eine Tochtergesellschaft der Amazon Web Services in den USA. Französische Berufsverbände und Gewerkschaften waren der Ansicht, dass die Nutzung der Amazon Web Services durch Doctolib einen Datenschutzverstoß darstelle. Da die Amazon Web Services Sarl ein Tochterunternehmen der AWS in den USA ist, bestünde das Risiko von Zugriffsanfragen durch US-Behörden im Rahmen von US-Überwachungsprogrammen. Daher beantragten sie beim Conseil d'Etat in einem Eilverfahren eine Aussetzung des Vertrags zwischen Doctolib und dem Gesundheitsministerium.

Auch der Conseil d'Etat folgt der vom EuGH geforderten Voraussetzungen für ein angemessenes Datenschutzniveau. Da der sogenannte CLOUD Act US-Unternehmen dazu verpflichtet, US-Behörden den Zugriff auf alle Daten unabhängig vom Speicherort zu gewähren, sei es nicht notwendig, dass die Daten tatsächlich in die USA übermittelt werden. Es ist lediglich notwendig, dass der Hauptsitz des Dienstleisters in den USA liegt und dass die Daten in dessen Zugriffsbereich liegen. In welchem Teil der Welt die Daten gespeichert werden ist insofern völlig irrelevant. Die Entscheidung des französischen Gerichts zeigt jedoch, dass amerikanische Unternehmen dennoch als Dienstleister in Anspruch genommen werden können.

Im Ergebnis kam es auf folgende Punkte an:

- Für den Fall eines Zugangsantrags einer ausländischen Behörde hatten Doctolib und AWS Sarl ein spezielles Verfahren vereinbart, das u.a. vorsieht, dass AWS Sarl jeden allgemeinen Zugangsantrag einer Behörde anfechten werde.

- **Die von AWS Sarl gehosteten Daten sind verschlüsselt und der Schlüssel wird von einer in Frankreich ansässigen dritten Partei und nicht von AWS Sarl verwaltet (Bring your own key - BYOK).**
- Es würden keine Gesundheitsdaten an Doctolib übermittelt und daher auch nicht von AWS Sarl gehostet.
- Die Daten werden nach drei Monaten gelöscht. Die Daten können auch früher gelöscht werden, wenn von der betroffenen Person gewünscht.

Mehr dazu in folgendem Urteil des Conseil d´Eta (Französisch): https://lnkd.in/eNHcFja6 und in folgendem Artikel der IAPP (Englisch): https://lnkd.in/dPt5-eR

Praxishinweis: Die Entscheidung zeigt, dass US-Dienstleister unter bestimmten Rahmenbedingungen genutzt werden können. Kernelement einer datenschutzrechtlich zulässigen Nutzung ist die Verschlüsselung der Daten, so dass ein US-Dienstleister (oder Anbieter aus einem anderen Nicht-EU/EWR-Staat) allenfalls verschlüsselte Daten herausgeben kann. Wichtig ist, dass der Dienstleister keinen Zugriff auf den Schlüssel haben darf (Bring your own key - BYOK).

LG München: 100,00 EUR Schadensersatz für Nutzung von Google Fonts

Google stellt im Rahmen von Google Fonts in einer interaktiven Bibliothek ca. 1.300 Schriftarten in Form von freien Lizenzen zur Verfügung. Webseitenbetreiber können diese frei, ohne Lizenzgebühren, verwenden. Nachteil: Bei Verwendung der Schriftarten wird eine Serververbindung zu Google LLC in den USA aufgebaut und von dort aus werden die Schriften geladen. Die IP-Adresse des Webseitennutzers wird an Google in die USA und damit einen unsicheren Drittstaat übermittelt.

In seinem Urteil vom 20.01.2022, Az. 3 O 17493/20 hat das Landgericht München entschieden, dass die automatisierte Weitergabe von IP-Adressen ohne Einwilligung des Nutzers durch die Nutzung von Google Fonts an Google einen unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht des Nutzers darstellt. Werden Google Fonts also online von Google-Servern bezogen, so kann das Recht auf informationelle Selbstbestimmung des Nutzers verletzt sein. Das Landgericht München erkennt Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) nicht als Rechtsgrundlage für die Weitergabe der IP-Adressen an. Als Begründung wird angeführt, dass eine Nutzung von Google Fonts auch durch lokale Speicherung der Google Fonts möglich sei. Bei einer solchen lokalen Nutzung unterbleibt bei Aufruf der Internetseite die Übermittlung der IP-Adresse an Google Server.

Das Landgericht sprach dem Kläger neben einem Unterlassungsanspruch auch einen immateriellen Schadenersatz gemäß Art. 82 Abs. 1 DSGVO in Höhe von 100,00 EUR zu.

Das Urteils finden Sie hier: https://openjur.de/u/2384915.html

Praxishinweis: Viele Unternehmen nutzen Google Fonts auf ihrer Webseite. Die datenschutzkonforme Einbindung von Google Fonts erfolgt über lokales Hosten auf dem eigenen Server. Auf den Online-Abruf direkt bei Google sollte verzichtet werden.

OLG Brandenburg: Übermittlung personenbezogener Daten von Mitarbeitenden zu Abrechnungszwecken an Auftraggeber

Dürfen personenbezogene Daten von Mitarbeitenden zu Abrechnungszwecken vom Dienstleister an den Auftraggeber übermittelt werden? Das OLG Brandenburg bejaht dies für die Namen der Mitarbeitenden, deren Stundennachweise über die für den Auftraggeber erbrachten Zeiten sowie den Bruttolohn als Nachweis zur Zahlung des Mindestlohnes. Als Rechtsgrundlage sieht das OLG Brandenburg Art. 6 Abs. 1 lit. f DSGVO (sog. berechtigtes Interesse).

Link zum Urteil: https://lnkd.in/eq7f9ZQg

BayLDA und LDI NRW: Verarbeitung von 3G-Daten im Arbeitsverhältnis

Verarbeitung von 3G-Daten im Arbeitsverhältnis: Bayerisches Landesamt für Datenschutzaufsicht ('BayLDA')

Das Bayerische Landesamt für Datenschutzaufsicht ("BayLDA") hat am 25. März 2022 aktualisierte häufig gestellte Fragen ("FAQs") zur Verarbeitung des COVID-19-Impf-, Test- oder Genesenenstatus (bekannt als 3G/3G plus/2G) im Beschäftigungsverhältnis veröffentlicht.

Insbesondere wird in den FAQs darauf hingewiesen, dass die bundesweite 3G-Zugangsregelung des § 28b des Infektionsschutzgesetzes vom 20. Juli 2000 ("IfSG"), die alle Beschäftigten betraf, mit Ablauf des 19. März 2022 ausgelaufen ist. Allerdings ermächtigt § 28a Abs. 8 Nr. 3 IfSG zum Erlass von Landesverordnungen. Auf Grundlage dieser Landesverordnungen kann eine 3G-Zugangsregelung in Betrieben, Einrichtungen oder Diensten, die der Öffentlichkeit zugänglich sind, in konkret zu benennenden Gemeinden oder bestimmten Gebieten erlassen werden. Voraussetzung hierfür ist allerdings, dass eine konkrete Gefahr einer sich dynamisch ausbreitenden Infektionssituation besteht und der Landtag dies als konkrete Gefahr und die Anwendung einer entsprechenden Maßnahme in der jeweiligen Gemeinde oder im jeweiligen Bundesland festgestellt hat. Die FAQs weisen darauf hin, dass die Ausübung der Verordnungsermächtigung und damit die Anordnung von 3G-Zugangsregelungen nunmehr in die Zuständigkeit der jeweiligen Bundesländer fällt.

Darüber hinaus stellen die FAQs klar, dass mit dem Auslaufen der 3G-Zugangsregelung die bundesrechtliche Verpflichtung des Arbeitgebers, die Einhaltung der Nachweispflicht täglich zu kontrollieren und die Kontrolle zu dokumentieren, entfällt. In der Konsequenz bedeutet dies, dass es keine Rechtfertigung mehr für die Aufbewahrung der personenbezogenen Daten zum "G"-Status und etwaige Gültigkeitszeiträume oder hinterlegte Nachweise auf der Grundlage des IfSG gibt. Die FAQs betonen daher, dass alle Unterlagen und Kopien von "G"-Nachweisen **unverzüglich zu löschen sind**. Etwas anderes gilt nur, wenn der Arbeitgeber die Weiterverarbeitung ausnahmsweise auf eine andere Rechtsgrundlage stützen kann, insbesondere bei schutzbedürftigen Einrichtungen.

Darüber hinaus wird in den FAQs dargelegt, dass der Freistaat Bayern von der Übergangsfrist des § 28a Abs. 10 IfSG Gebrauch gemacht und die Bayerische Infektionsschutzmaßnahmenverordnung an die geänderte Rechtslage angepasst hat. Beispielsweise kann in bestimmten Bereichen in Bayern weiterhin eine 3G-Zugangsregelung für Beschäftigte in Betrieben mit Kundenkontakt erlassen werden.

Verarbeitung von 3G-Daten im Arbeitsverhältnis: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen ("LDI NRW")

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen ("LDI NRW") hat am 23. März 2022 eine Pressemitteilung zur Löschung personenbezogener Daten von Beschäftigten und zur Vernichtung von Nachweisen der COVID-19-Impfung, der Genesung oder des negativen Testergebnisses ("3G-Nachweis") veröffentlicht, nachdem mit der letzten Änderung des Infektionsschutzgesetzes die Pflicht zur Vorlage eines 3G-Nachweises am Arbeitsplatz abgeschafft wurde. Der LDI NRW stellte insbesondere fest, dass die Speicherung der personenbezogenen Daten der Beschäftigten im Zusammenhang mit COVID-19 nicht mehr erforderlich ist, da die Rechtsgrundlage für die Erhebung dieser Daten weggefallen ist, und dass die Arbeitgeber diese Daten **unverzüglich löschen sollten.**

Darüber hinaus erklärte der LDI NRW, dass einige Arbeitgeber sogar 3G-Nachweise kopiert oder eingescannt hätten, obwohl dies nach dem IfSG nicht zulässig sei. Dementsprechend forderte der LDI NRW die Arbeitgeber auf, alle 3G-Nachweise unverzüglich und rechtssicher zu entsorgen. Konkret wies der LDI NRW darauf hin, dass:

- Gesundheitsdaten der Beschäftigten und Daten zur Ermittlung von Kontaktpersonen vollständig und dauerhaft vernichtet werden müssen und
- für in Papierform gesammelte Daten ein geeigneter Schredder der Sicherheitsstufe vier oder höher nach DIN 66399 verwendet werden sollte, da ein Zerreißen von Hand nicht ausreicht.

Praxishinweis: Nach der Entschärfung der Covid-19-Maßnahmen sollte überprüft werden, ob alle Daten, die nun nicht mehr benötigt werden, auch tatsächlich schon vernichtet wurden.

Die Pressemitteilung des Bayerischen Landesamts für Datenschutzaufsicht finden Sie hier: https://www.lda.bayern.de/media/veroeffentlichungen/FAQ-Sammlung_zur_Verarbeitung_von3G_Arbeitspaltz.pdf

Impressum

mip Consult GmbH
Wilhelm-Kabus-Straße 9
10829 Berlin
Tel: +49 (0) 30 – 20 88 999 – 00
Fax: +49 (0) 30 – 20 88 999 – 88
Redaktion: Asmus Eggert, Nora Lynn Rodiek

Internet: www.sofortdatenschutz.de und www.blog.sofortdatenschutz.de
E-Mail: sofortdatenschutz@mip-consult.de

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider
Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 121869
USt.-Identnr.: DE249276018
Verantwortlich nach § 18 Abs. 2 MStV: Asmus Eggert