Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

in den Monaten Juli und August ist häufig die Rede vom Sommerloch. Ist damit auch Sommerpause für unsere Unterrichtungspflicht als Datenschutzbeauftragte aus Art. 39 Abs. 1 a) DSGVO? Aktuell jedenfalls trifft dies nicht zu.

Neben einem Update zu den neuen Standardvertragsklauseln ist es vor allem der Angemessenheitsbeschluss der EU-Kommission für das Vereinigte Königreich und eine Entscheidung des BGH zum Auskunftsrecht, auf die wir Ihre Aufmerksamkeit lenken möchten.

Aufgenommen haben wir auch die Stellungnahme des Europäische Datenschutzausschusses zum Thema Drittstaatentransfers. Die Stellungnahme soll Unternehmen eigentlich helfen, Drittstaatentransfers im Lichte der Schrems II-Entscheidung des EuGHs datenschutzkonform vorzunehmen. Warum diese Anliegen aus unserer Sicht nicht erreicht wird, erklären wir Ihnen in unserem Beitrag.

Unabhängig davon wünsche ich Ihnen einen ruhigen Sommer. Erholen Sie sich gut!

Ihr

Asmus Eggert

Inhalt

Bundesgerichtshof präzisiert den Umfang des Auskunftsrechts (Art. 15 DSGVO)

Ein Lebensversicherungsunternehmen (Verantwortlicher) und ein Versicherter (Betroffener) haben über den Umfang des datenschutzrechtlichen Auskunftsanspruch nach Art. 15 DSGVO bzw. § 34 BDSG alte Fassung gestritten. Der Versicherte verlangte Auskunft über alle bei der Versicherung tatsächlich vorhandenen personenbezogenen Daten, die in der Folge näher spezifiziert wurden. Die Versicherung hatte dem Auskunftsverlangen nicht in vollem Umfang entsprochen.

Im Revisionsverfahren (Az. VI ZR 576/19) hat nun der Bundesgerichtshof (BGH) am 15.06.2021 geurteilt, dass der Auskunftsanspruch nach Art. 15 DSGVO auch die Schreiben der Korrespondenz zwischen den beiden Parteien umfasst. Der Anspruch sei nicht deshalb ausgeschlossen, weil die Schreiben dem Auskunftsersuchenden bereits bekannt sind. Das begründet das Gericht damit, dass der Verantwortliche Auskunft darüber geben soll, ob die in dem Schriftverkehr enthaltenen personenbezogenen Daten aktuell verarbeitet, insbesondere gespeichert werden. Die Auskunft solle den Betroffenen in die Lage versetzen, sich der Datenverarbeitung bewusst zu werden und deren Rechtmäßigkeit zu prüfen. Das etwaige Bewusstsein des Betroffenen, dass die fragliche Korrespondenz einst gewechselt wurde, genüge insoweit nicht, um den Anspruch auszuschließen. Auch könne der Auskunftsberechtigte grundsätzlich wiederholt Auskunft verlangen.

Ferner stellt der BGH klar, dass sich der Anspruch auf die Korrespondenz mit Dritten und auch auf interne Vermerke und interne Kommunikation erstrecke, die Informationen zum Betroffenen enthalten (z.B. Gesprächsvermerke oder Vermerke über den Gesundheitszustand).

Schließlich verweist das Gericht auf die Rechtsprechung des EuGHs, wonach rechtliche Analysen zwar grundsätzlich personenbezogene Daten enthalten können, die auf der Grundlage dieser Daten vorgenommene Beurteilung der Rechtslage selbst stelle aber keine personenbezogenen Daten dar. Auch Daten über Provisionszahlungen des Verantwortlichen an Dritte hätten nach der Rechtsprechung des EuGHs keinen Personenbezug.

Für die Erfüllung des Auskunftsanspruch sei nach dem Urteil des BGH entscheidend, dass die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdeckt. Daran könne es etwa fehlen, wenn der Verantwortliche hinsichtlich bestimmter Kategorien von Auskunftsgegenständen keine Auskunft erteilt hat, z.B. weil er irrigerweise davon ausging, dass er hierüber nicht zur Auskunft verpflichtet sei. Dann könne der Auskunftsberechtigte eine Ergänzung der Auskunft verlangen. Der bloße Verdacht, dass die erteilten Informationen unvollständig oder unrichtig seien, könne dagegen keinen weitergehenden Auskunftsanspruch begründen. Wesentlich für die Erfüllung des Auskunftsanspruchs sei daher die - möglicherweise konkludente - Erklärung des Verantwortlichen, dass die Informationen vollständig seien.

Praxishinweis: Gemäß Art. 15 DSGVO hat eine betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu verlangen, ob personenbezogene Daten, die sie betreffen, verarbeitet werden. Ist dies der Fall, so sind Informationen über die Verarbeitungszwecke, die Kategorien personenbezogener Daten, die verarbeitet werden, die Empfänger oder Kategorien von Empfängern der Daten usw. zu erteilen (vgl. Art. 15 Abs. 1 lit. a) bis h) DSGVO).

Dass interne Vermerke oder interne Mitteilungen zum Umfang des Auskunftsrechts gehören, hat der BGH nun klargestellt und damit den Auskunftsanspruch sehr weit gefasst. Die Entscheidung ist aber auch so zu verstehen, dass sich wiederholende Auskünfte auf Veränderungen beschränken können.

Keine Aussage macht das Gericht in seinem Urteil über den Umfang der Verpflichtung, Kopien der Daten zur Verfügung zu stellen. Hier gehen wir weiterhin davon aus, dass Unterlagen, die dem Betroffenen vorliegen, nicht erneut als Kopie übermittelt werden müssen.

Bei unspezifisch gestellten Auskunftsersuchen mit erheblichem Datenumfang bleibt es daher bei unserer Empfehlung, in 2 Stufen vorzugehen: Informieren Sie in der 1. Stufe über die Kategorien personenbezogener Daten in abstrakter Form verbunden mit dem Angebot, die konkret angeforderten Informationen (Schreiben, Vermerke, E-Mails, Befunde etc.) in einer 2. Stufe zu erteilen.

BayLDA fordert Unternehmen auf, die Nutzung von Mailchimp einzustellen

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat in einer Entscheidung festgestellt, dass die Nutzung des Tools Mailchimp durch ein deutsches Unternehmen rechtswidrig war.

In der Entscheidung hatte das BayLDA beanstandet, dass das Unternehmen in zwei Fällen E-Mail-Adressen an Mailchimp übermittelt hatte, um Newsletter zu versenden. Dabei hatte das Unternehmen nicht geprüft, ob zusätzliche Maßnahmen im Sinne des Urteils des Gerichtshofs der Europäischen Union in der Rechtssache Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) ("Schrems II") erforderlich waren, um die Übermittlung datenschutzkonform zu gestalten. Es gäbe zumindest Anhaltspunkte dafür, dass Mailchimp als "elektronischer Kommunikationsdienstleister" grundsätzlich dem Datenzugriff durch US-Geheimdienste ausgesetzt sein könnte. Daher sei die Übermittlung personenbezogener Daten in die USA ohne weitere Schutzmaßnahmen als rechtswidrig anzusehen.

Praxishinweis: Das Tool Mailchimp wird von vielen Unternehmen für den Versand von Newslettern an Kunden genutzt. Die Unternehmen, die das Tool nutzen, sollten daher prüfen und dokumentieren, ob und wenn ja welche zusätzlichen datenschützende Maßnahmen entsprechend den Anforderungen des Schrems II-Urteils des EuGHs ergriffen wurden oder sie sollten alternativ auf ein Tool eines Anbieters aus der EU/dem EWR mit Datenverarbeitung in der EU/EWR umsteigen. Die gleiche Problematik stellt sich im Übrigen für alle Tools von Anbietern, die nicht aus der EU/EWR stammen, und/oder die personenbezogene Daten außerhalb der EU/EWR verarbeiten.

DSK veröffentlicht Leitfaden zur Verschlüsselung von E-Mails mit personenbezogenen Daten

Die Deutsche Datenschutzkonferenz (DSK) hat am 16.06.2021 eine Leitlinie zum Versand und Empfang von E-Mails mit personenbezogenen Daten herausgegeben. Insbesondere gibt es hier Hinweise zu den Anforderungen an die Verschlüsselung von E-Mails.

Der Leitfaden listet erforderliche Verfahren für den Versand und Empfang von E-Mails für Diensteanbieter und andere Beteiligte auf. Darüber hinaus skizziert der Leitfaden eine Reihe von Maßnahmen, die je nach dem Grad des Risikos für die Rechte und Freiheiten der betroffenen Personen ergriffen werden können.

Praxishinweis: Der Leitfaden sollte zum Anlass genommen werden, die verschiedenen Szenarien der Übermittlung personenbezogener Daten per E-Mail auf ihre Risiken hin zu analysieren und ggf. eine Arbeitsanweisung für Mitarbeiter abzuleiten.

Werden E-Mail-Adressen für den Empfang von Nachrichten, z. B. auf der Website, zur Verfügung gestellt, sollte die Sensibilität der zu erwartenden Daten geprüft werden. In Abhängigkeit davon sollten entweder weitere Schutzmechanismen (z. B. verpflichtende TLS-Verschlüsselung) eingeführt oder es sollte geprüft werden, ob andere, datenschutzkonforme Kommunikationswege genutzt werden können (z.B. verschlüsselt übertragene Daten per Web-Formular).

EU-Kommission trifft positive Angemessenheitsbeschluss für UK

Die Europäische Kommission gab am 28.06.2021 bekannt, dass sie zwei Angemessenheitsbeschlüsse für das Vereinigte Königreich gefasst hat, einen im Rahmen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) (DSGVO) und einen im Rahmen der Datenschutzrichtlinie im Hinblick auf die Strafverfolgung (Richtlinie (EU) 2016/680).

Mit dem Angemessenheitsbeschluss können also nun personenbezogene Daten ungehindert aus der EU in das Vereinigte Königreich fließen. Der Beschluss stellt klar, dass Daten im Vereinigten Königreich ein im Wesentlichen gleichwertiges Schutzniveau wie nach EU-Recht genießen. Die

Angemessenheitsbeschlüsse erleichtern damit auch die korrekte Umsetzung des Handels- und Kooperationsabkommens zwischen der EU und dem Vereinigten Königreich, das ebenfalls den Austausch personenbezogener Daten vorsieht.

Die Kommission hat die Gültigkeit der beiden Angemessenheitsbeschlüsse allerdings auf die Dauer von 4 Jahren befristet. Darüber hinaus betonte die Kommission, dass sie die Rechtslage im Vereinigten Königreich in dieser Zeit weiterhin beobachtet. Senke das Vereinigte Königreich das derzeit geltende Schutzniveau, werde die Kommission eingreifen und die Beschlüsse aufheben.

Praxishinweis: Für die nächsten 4 Jahre ist der Datenfluss in das Vereinigte Königreich durch die Angemessenheitsentscheidung der Kommission gesichert. Sollte das Vereinigte Königreich jedoch grundlegende Änderungen an der DSGVO vornehmen, kann die Kommission die Angemessenheitsentscheidung auch schon vor Ablauf der 4 Jahre zurückziehen. Die Angemessenheitsentscheidung steht ohnehin auf wackligen Beinen. Unter anderem hatte das Europäische Parlament die Kommission aufgefordert, aufgrund der dort geltenden Überwachungsgesetze keinen Angemessenheitsbeschluss für Großbritannien zu erlassen. Daher müssen alle Unternehmen Daten zwischen EU und UK austauschen die Situation im Auge behalten. Wir werden Sie weiterhin über das Thema unterrichten.

Fristen für die neuen Standardvertragsklauseln

Wir hatten in der letzten Beratungsinformation über die neuen Standardvertragsklauseln (SVK) berichtet. Diese wurden am 07.06.2021 im Europäischen Amtsblatt veröffentlicht.

Da an diese Veröffentlichung im Amtsblatt der Ablauf der Fristen für die Gültigkeit der alten Standardvertragsklauseln geknüpft ist, möchten wir an die sich daraus ergebenden konkreten Fristen erinnern. Gemäß Art. 4 Abs. 1 des Beschlusses tritt dieser Beschluss nämlich am zwanzigsten Tag nach seiner Veröffentlichung in Kraft, also am 27.06.2021. Daraus ergeben sich folgende Fristen:

1. Die neuen Standardvertragsklauseln sind **spätestens ab dem 27.09.2021 zwingend für Neuverträge** zu verwenden.
2. **Spätestens bis zum 27.12.2022 muss eine Umstellung sämtlicher Altverträge** auf die neuen Standardvertragsklauseln erfolgt sein.

Praxishinweis: Prüfen Sie, in welchen Vertragsbeziehungen in Ihrem Unternehmen Standardvertragsklauseln eingesetzt werden und beachten Sie eine rechtzeitige Umstellung auf die neuen Standardvertragsklauseln. Für Neuverträge empfehlen wir schon jetzt, ausschließlich auf Basis der neuen Standardvertragsklauseln zu arbeiten.

EDPB verabschiedet endgültige Empfehlung zu ergänzenden Maßnahmen für die Übermittlungen personenbezogener Daten in Drittländer

Der Europäische Datenschutzausschuss (EDPB) gab am 21.06.2021 bekannt, dass er die endgültige Fassung seiner Empfehlungen 01/2020 zu ergänzenden Maßnahmen für Übermittlungen personenbezogener Daten in Drittländer angenommen hat. Der Europäische Datenschutzausschuss ist eine unabhängige europäische Einrichtung. Sie hat sich zum Ziel gesetzt, die einheitliche Anwendung der Datenschutz-Grundverordnung sicherzustellen und die Zusammenarbeit zwischen den Datenschutzbehörden der EU zu fördern.

Die Empfehlungen sollen die für die Verarbeitung Verantwortlichen und die Auftragsverarbeiter, die als Datenexporteure tätig sind, bei ihrer Pflicht unterstützen, gegebenenfalls geeignete ergänzende Maßnahmen zu ermitteln und umzusetzen, um ein im Wesentlichen gleichwertiges Schutzniveau für in Drittländer übermittelte Daten sicherzustellen.

Der EDPB beschreibt in seiner Empfehlung sechs Schritte, die Datenexporteure berücksichtigen müssen, wenn sie die Rechtmäßigkeit von Datenübermittlungen in Drittländern bewerten:

- **1. Schritt**: Bestandsaufnahme aller Drittstaatentransfers, hierzu gehören auch Cloud-Dienste, die zwar eine Datenverarbeitung auf Servern in EU/EWR zusichern, Remote-Zugriffe aus Drittländern wie den USA aber nicht ausschließen (z.B. AWS, Azure oder Salesforce)
- **2. Schritt**: Übermittlungsinstrument und dessen Rechtsgrundlage für Drittstaatentransfer nach Art. 44 ff. DSGVO ermitteln (z.B. Angemessenheitsbeschluss, Standardvertragsklauseln, Binding Corporate Rules oder Einwilligung der Betroffenen)
- **3. Schritt**: Bewertung der Wirksamkeit des in Schritt 2 ermittelten Übermittlungsinstruments als Garantie für die Sicherstellung eines mit der EU vergleichbaren Datenschutzniveaus
- **4. Schritt**: Ermittlung zusätzlicher (technischer) Maßnahmen zur Absicherung der Drittlandübermittlung – D.h. ist das Ergebnis in Schritt 3, dass die Sicherstellung eines mit der EU vergleichbaren Datenschutzniveaus durch das Übermittlungsinstrument nicht erreicht wird (beispielsweise sind für die USA Standardvertragsklauseln oder Binding Corporate Rules keine ausreichende Garantie, siehe Schrems II-Urteil des EuGH), müssen zusätzliche Maßnahmen zur Absicherung des Drittstaatentransfers ermittelt werden. Sofern in diesem Fall keine zusätzlichen Maßnahmen verfügbar sind, darf grundsätzlich kein Datentransfer erfolgen.
- **5. Schritt**: Implementierung zusätzlicher Maßnahmen, sofern solche identifiziert wurden - Abhängig vom gewählten Übermittlungsinstrument müssen weitere Verfahrensschritte eingehalten werden, um die zusätzlichen Maßnahmen (siehe Schritt 4) im Verhältnis zum Datenimporteur zu vereinbaren und zu dokumentieren. Sofern dies z. B. als Ergänzung zu den (ansonsten unveränderten) Standardvertragsklauseln geschieht, ist keine Genehmigung der Aufsichtsbehörden hierfür notwendig. Anders ist dies aber, wenn die Standardvertragsklauseln direkt modifiziert werden (siehe Art. 46 Abs. 3 lit. a) DSGVO).
- **6. Schritt**: Neubewertung in angemessenen Abständen

Der EDPB weist hierbei ausdrücklich darauf hin, dass die Ergebnisse dieser Bewertung und die ggf. getroffenen Maßnahmen zu dokumentieren sind, um dies gegenüber den Aufsichtsbehörden in Erfüllung der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nachweisen zu können.

Interessant an der Empfehlung sind u.a. die in Anhang 2 befindlichen Anwendungsfälle. Im Folgenden finden Sie eine kurze und vereinfachte Darstellung ausgewählter Fälle des Anhangs 2:

- **Fall 1:** Ein Datenexporteur nutzt einen Hosting-Anbieter in einem Drittland zur Speicherung personenbezogener Daten, z. B. für Backup-Zwecke -> **Ok**, sofern vor (!) Übermittlung eine leistungsfähige Verschlüsselung erfolgt.
- **Fall 2**: Ein Datenexporteur pseudonymisiert die von ihm gehaltenen Daten, bevor er sie zur Analyse ins Drittland übermittelt, z. B. zu Forschungszwecken. -> **Ok**, sofern Pseudonymisierung tatsächlich jeglichen Personenbezug aufhebt.
- **Fall 6**: Ein Datenexporteur beauftragt einen Cloud-Service-Anbieter oder anderen Auftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten, die im Drittland nach den Anweisungen des Datenexporteurs erfolgt. -> **Nicht Ok**, für den EDPB ist nach dem heutigen Stand der Technik keine wirksame technische Maßnahme vorstellbar, die im Falle eines solchen Zugangs die Verletzung der Rechte betroffener Personen verhindern könnte.
- **Fall 7**: Ein Datenexporteur stellt personenbezogene Daten Unternehmen in einem Drittland zur Verfügung, um sie für gemeinsame Geschäftszwecke zu verwenden. Eine typische

Konstellation wäre etwa, dass ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter personenbezogene Daten an einen in einem Drittland ansässigen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, übermittelt. Der Datenimporteur kann die Daten, die er empfängt, z. B. dazu nutzen, Personaldienstleistungen für den Datenexporteur zu erbringen, für die er dessen Personaldaten braucht, oder dazu, mit Kunden des Datenexporteurs, die in der Europäischen Union wohnen, per Telefon oder E-Mail zu kommunizieren. -> **Nicht Ok**, für den EDPB ist nach dem heutigen Stand der Technik keine wirksame technische Maßnahme vorstellbar, die im Falle eines solchen Zugangs die Verletzung der Rechte betroffener Personen verhindern könnte.

Praxishinweis: Gerade für die praxisrelevanten Fälle 6 und 7 scheidet nach Ansicht des EDPB ein rechtskonformer Drittstaatentransfer aus. Für Unternehmen bedeutet dies, entweder die Transfers zu stoppen (oft praktisch nicht möglich) oder im Rahmen eines risikobasierten Ansatzes die Transfers mit der überragenden Bedeutung für die Unternehmensprozesse und zusätzlichen Maßnahmen (und ggf. unter Absicherung durch entsprechende Gutachten) zu rechtfertigen. Nach der Stellungnahme des EDPB ist das Eis für risikobasierte Ansätze allerdings noch dünner geworden.

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: Stefan Ax, Asmus Eggert

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