Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

neben Corona, dem Dauerthema des Jahres 2020, tritt der Brexit fast etwas in den Hintergrund. Der Austritt des Vereinigten Königreichs aus der EU wird mit dem Ende der Übergangsphase am 31.12.2020 in datenschutzrechtlicher Hinsicht allerdings für alle relevant, die personenbezogene Daten zwischen UK und der EU transferieren. Was nach Ablauf der Übergangsphase zu beachten ist, zeigen wir Ihnen in der aktuellen Beratungsinformation.

Ferner haben wir einen Hinweis auf die Orientierungshilfe der Datenschutzkonferenz zur Videoüberwachung aufgenommen und fassen für Sie zusammen, was Sie bei der E-Mail-Kommunikation beachten müssen.

Aus der aktuellen Rechtsprechung informieren wir Sie über eine Entscheidung des Landgerichts Rostock zur Ausgestaltung des Cookie-Banners. Auch die Entscheidung des Bundesgerichtshofs zu einem Thema außerhalb des Datenschutzes stellen wir Ihnen dar, da es häufig bei uns angefragt wird: Die Informationen zur Streitbeilegung in den AGB und auf der Webseite eines Unternehmens.

Diese Beratungsinformation wird die letzte Ausgabe in diesem Jahr sein. Ein Jahr, das mit den Folgen der Covid-19-Pandemie Sie und uns vor neue Herausforderungen stellt und gestellt hat, auch im Datenschutz. Ein Jahr, das insbesondere aufgrund der Schrems-II-Entscheidung des EuGHs Herausforderungen eröffnet hat, die es gemeinsam mit Ihnen zu bewältigen galt. Aber auch ein Jahr, der guten Zusammenarbeit. Wir, Ihre Datenschützer, sagen daher gerne Danke für Ihr Vertrauen und Ihren Auftrag.

Das mip-Datenschutzteam wünscht Ihnen, Ihren Familien und Kolleg*innen besinnliche Feiertage und einen guten Rutsch ins Neue Jahr. Bleiben Sie gesund!

Ihr

Asmus Eggert

Inhalt

Brexit: Übergangsphase endet am 31.12.2020 – Handlungsbedarf beim Datenschutz?

Am 31.01.2020 ist das Vereinigte Königreich bereits aus der EU ausgetreten. Für die Umsetzung des Austritts gibt es seit dem Austrittstermin bis zum 31.12.2020 eine Übergangsphase. In dieser gilt das Unionsrecht über den Schutz personenbezogener Daten im Vereinigten Königreich für die Verarbeitung der personenbezogenen Daten betroffener Personen weiter. Am 31.12.2020 wird der Übergangszeitraum enden. Was bedeutet das?

Ab dem 01.01.2021 gilt – vorbehaltlich einer Einigung in letzter Sekunde - das Vereinigte Königreich als Drittland im Sinne des Kapitel V der DSGVO. Nach der DSGVO setzt ein Datenaustausch mit einem Drittland voraus, dass das Schutzniveau der europäischen Datenschutzvorgaben nicht untergraben wird. Die EU-Kommission kann dazu eine Angemessenheitsentscheidung treffen. Diese Angemessenheitsentscheidung streben UK und die EU an. Sie liegt jedoch noch nicht vor, und es wird aller Voraussicht nach auch noch eine ganze Weile dauern. Folglich muss man auf andere Instrumente der DSGVO zurückgreifen, um personenbezogene Daten rechtmäßig zu übermitteln.

Alle Unternehmen, die personenbezogene Daten zwischen EU und UK (z.B. mit Konzerngesellschaften, Tochterunternehmen, Dienstleistern, Dienstleistern von Dienstleistern etc.) austauschen, müssen daher aktiv werden und die Voraussetzungen eines rechtskonformen Datenaustausches schaffen.

Praxishinweis: Prüfen Sie, ob es im Rahmen Ihrer geschäftlichen Aktivität zum Datenaustausch mit Unternehmen (z.B. Dienstleistern oder von diesen Dienstleistern eingesetzte Unterauftragnehmer oder aber auch konzernangehörige Unternehmen) kommt, die

a) über einen satzungsmäßigen Sitz und/oder eine Niederlassung in UK verfügen;
b) innerhalb der EU ansässig sind und über Rechenzentren in UK verfügen.

Wenn ja, ist folgendes zu tun:

- Implementierung geeigneter Garantien, z. B. über EU-Standarddatenschutzklauseln, beim Datenaustausch zwischen Konzerngesellschaften über Binding Corporate Rules oder
- Einführung von Ausnahmen für bestimmte Fälle, wie die ausdrückliche Einwilligung der betroffenen Person oder die Übermittlung zur Erfüllung eines Vertrages mit der betroffenen Person;
- Anpassung der Datenschutzinformation bzw. Datenschutzerklärung. Die betroffenen Personen sind bei der Datenerhebung explizit über Datentransfers in Drittlandländer zu informieren;
- Anpassung des Verzeichnisses der Verarbeitungstätigkeiten;
- Überprüfung der Datenschutz-Folgenabschätzungen Ihres Unternehmens auf Auswirkungen bzgl. der Datenübermittlung ins Vereinigte Königreich.

Für britische Unternehmen, die personenbezogene Daten mit EU-Unternehmen austauschen, bleiben auch bei Verlassen des Europäischen Wirtschaftsraums (EWR) die europäischen Datenschutzbestimmungen von enormer Bedeutung. Wenn außereuropäische Unternehmen ihr Waren- und Dienstleistungsangebot weiterhin an in der EU befindliche Personen richten, befinden sie sich weiterhin im Anwendungsbereich der europäischen Datenschutzbestimmungen (sog. Marktortprinzip). Als britisches Unternehmen ist insbesondere zu prüfen,

- ob die Pflicht zur Benennung eines Unionsvertreters nach Art. 27 EU-DSGVO besteht (umgekehrt ist für Unternehmen, die auf dem britischen Markt ohne Niederlassung vor Ort tätig sind, ggf. einen Vertreter nach Art. 27 UK-DSGVO zu benennen),

- welche Aufsichtsbehörde in der EU zuständig ist,
- ob auch für die EU ein Datenschutzbeauftragter benannt werden muss (z. B. nach BDSG),
- ob die EU-Standarddatenschutzklauseln abgeschlossen wurden oder ggf. ein Angemessenheitsbeschluss von UK für die EU vorliegt.

Wenn Sie Unterstützung benötigen, sprechen Sie Ihren Berater an.

Videoüberwachung: Datenschutzkonferenz hat neue Orientierungshilfe veröffentlicht

Die Datenschutzkonferenz (DSK) ist ein Gremium, das sich aus den unabhängigen Datenschutzbehörden des Bundes und der Länder zusammensetzt. Sie hat die Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen und gemeinsam für seine Fortentwicklung einzutreten. Zu diesem Zweck veröffentlicht sie auch sog. Orientierungshilfen. Im September dieses Jahres hat sie nun eine überarbeitete Orientierungshilfe zum Thema „Videoüberwachung durch nicht-öffentliche Stellen“ herausgebracht: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf. Sie finden in der Orientierungshilfe eine umfangreiche Darstellung inkl. der Themen „Überwachung von Mitarbeitern“, „Überwachung in der Gastronomie“ oder „Einsatz von Dashcams, Tür- und Klingelkameras, Drohnen und Wildkameras“. Die Orientierungshilfe enthält zudem eine Checkliste mit Punkten, die zu beachten sind.

E-Mail-Kommunikation und Datenschutz

Darf ich eine E-Mail an einen offenen E-Mail-Verteiler versenden oder nicht?

Auf den ersten Blick eine harmlose Frage, aber eine solche E-Mail kann bei einem großen Empfängerkreis erhebliche finanzielle Risiken für das verantwortliche Unternehmen mit sich bringen. Auf einen laxen Umgang mit E-Mail-Adressen reagieren die Aufsichtsbehörden je nach Einzelfall auch mit Bußgeldbescheiden. Als Prüffeld haben die Aufsichtsbehörden das Thema jedenfalls erkannt. So ist einer Pressemitteilung[1] des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) zu entnehmen, dass dem datenschutzrechtlichen Rahmen bei der E-Mail-Kommunikation in vielen Unternehmen keine ausreichende Bedeutung beigemessen wird.

Die datenschutzrechtliche Relevanz der E-Mail-Adressen von Kunden, Lieferanten und Geschäftspartnern folgt daraus, da diese grundsätzlich immer einer konkreten Person zugeordnet sind. Eine Person ist damit identifiziert oder zumindest identifizierbar. Üblicherweise setzt sich die E-Mail-Adresse aus dem Vor- und/oder Nachnamen des Ansprechpartners zusammen, z.B. *vorname.nachname@unternehmen.de*.

Beim Versand einer E-Mail an einen falschen Empfänger oder Empfängerkreis, wird die E-Mail-Adresse oder werden die -Adressen den anderen Adressaten, der Inhalt der Nachricht und ggfs. Dateianhänge offengelegt. Das ist ein Datenschutzverstoß, der entsprechend der Regeln der DSGVO innerhalb der kurzen Fristen (72 h) zu prüfen und ggf. auch an die Aufsichtsbehörde zu melden ist.

Im Arbeitsalltag ist der fehlerhafte Versand von E-Mails nicht vollständig auszuschließen. Das Unternehmen muss daher vorbeugend über organisatorische Maßnahmen sicherstellen, dass Fehler beim Versand von E-Mails und damit das Risiko eines Datenschutzverstoßes vermieden werden.

[1] BayLDA, PM v. 28.06.2013, abrufbar unter: https://web.archive.org/web/20140709073416/http://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2013/pm004.html

Praxishinweis: Definieren Sie klare Regeln für die Nutzung des dienstlichen E-Mail-Accounts und sensibilisieren Sie Ihre Mitarbeiter*innen im Umgang mit Verteilerlisten, Anhängen sowie Cc- und Bcc-Feldern. Listen mit personenbezogenen Daten sollten per E-Mail nur verschlüsselt versendet werden (bei Excel-Listen z.B. durch einen Passwortschutz auf der Datei).

Da Sie das Risiko, falsch versendeter E-Mails niemals vollständig ausschließen können, verbinden Sie die vorgenannten Maßnahmen stets auch mit einer Information zum Umgang und Vorgehen bei einer Datenpanne. Bitte vergessen Sie deshalb auch nicht, Ihre Mitarbeiter*innen über interne Meldewege bei eingetretenen Datenpannen, z.B. infolge einer falsch versendeten E-Mail sowie die 72-Stunden-Frist aufzuklären.

Sowohl bei der Anpassung Ihrer internen E-Mail-Richtlinie, der Sensibilisierung Ihrer Mitarbeiter*innen und auch bei der Implementierung eines passgenauen Incident-Managements unterstützen Sie unsere Berater gerne.

Datenschutzinformation – Verweise auf EU-US Privacy Shield entfernen!

In den letzten Beratungsinforationen hatten wir Sie bereits ausführlich über die Folgen der Ungültigkeit des EU-US Privacy Shields und die daraus abzuleitenden Maßnahmen informiert. Leider stellen wir bei der Sichtung von Datenschutzinformationen bzw. Datenschutzerklärungen von Webseiten immer wieder fest, dass weiterhin auf das EU-US Privacy Shield als Rechtsgrundlage verwiesen wird. Bitte prüfen Sie, ob der Verweis auf das EU-US Privacy Shield lediglich nicht aktualisiert wurde oder ob tatsächlich noch Daten auf dessen Basis übermittelt werden. Sollten weiter unverändert Daten zu US-Dienstleistern übermittelt werden, ist das ein Verstoß gegen die DSGVO. Wird den Aufsichtsbehörden dieser Verstoß angezeigt, müssen diese handeln und dagegen vorgehen. Als Unternehmen setzt man sich insofern einem Bußgeldrisiko aus.

Praxishinweis: Prüfen Sie die eigene Datenschutzinformation. Wenn Sie Unterstützung bei der Bewertung und Anpassung benötigen, sprechen Sie uns an.

Einen aktuellen Podcast zu dem Thema hat die Rheinland-Pfälzische Aufsichtsbehörde kürzlich veröffentlicht. Hier der Link für Interessierte:
https://www.datenschutz.rlp.de/fileadmin/lfdi/Podcast/Datenfunk_Podcast_07.html

LG Rostock: Anforderungen an das Cookie-Banner einer Webseite

Für das Setzen von nicht notwendigen Cookies (d.h. insbesondere solche zur Marketinganalyse) ist die Einwilligung des Nutzers erforderlich. Dies haben sowohl der EuGH als auch der BGH bereits entschieden. Wir hatten darüber berichtet. Nunmehr hat das Landgericht Rostock ein Cookie-Banner beurteilt, das in gleicher oder ähnlicher Ausgestaltung bei vielen Webseiten im Einsatz ist.

Es ging um ein Cookie-Banner, bei dem die Ankreuzhäkchen für die Kategorien „Notwendig“, „Präferenzen“, „Statistiken“ und „Marketing“ bereits vorausgewählt waren. Durch die Betätigung des „OK“-Buttons sollten die Nutzer der Verwendung von Cookies zustimmen. Über „Details anzeigen“ bestand die Möglichkeit, eine Liste der verwendeten Cookies und u.a. deren Zuordnung zu den einzelnen Kategorien einzusehen. Eine gesonderte Aus- oder Abwahlmöglichkeit bestand an dieser Stelle nicht. Unter den auf der Seite verwendeten Cookies befanden sich auch Tracking- und Analysetools wie z.B. Google-Analytics. Der Bundesverband der Verbraucherzentralen (vzbv) mahnte den Betreiber der Plattform wegen dieser Darstellung ab und verlangte Unterlassung.

Die Plattformbetreiberin wies die Abmahnung zurück und änderte das angezeigte Cookie-Banner. Das geänderte Banner sah nun eine grün hinterlegte Schaltfläche „Cookies zulassen“ und eine hellgrau hinterlegte Schaltfläche „Nur notwendige Cookies zulassen vor“. Daneben war ein Link „Details anzeigen“ vorhanden. In diesem waren ebenfalls wieder alle Cookies vorausgewählt. Diese Änderung genügte nach Ansicht des Bundesverbands der Verbraucherzentralen (vzbv) jedoch noch immer nicht den Anforderungen an eine wirksame Einwilligung.

Das Landgericht Rostock ist der Ansicht des Bundesverbands der Verbraucherzentralen (vzbv) gefolgt und entschied, dass selbst die geänderte Version des Cookie-Banners die Vorauswahl im Cookie-Banner nicht zur Einholung einer wirksamen Einwilligung geeignet war: *„Der Umstand, dass der Nutzer bei dem nun verwendeten Cookie-Banner auch die Möglichkeit hat, über den Bereich „Nur notwendige Cookies verwenden" seine Einwilligung auf technisch notwendige Cookies zu beschränken, ändert an der Beurteilung nichts. Insoweit ist festzuhalten, dass dieser Button gar nicht als anklickbare Schaltfläche zu erkennen ist. Zudem tritt er auch neben dem grün unterlegten und damit als vorbelegt erscheinenden „Cookie zulassen"-Button in den Hintergrund. Diese Möglichkeit wird von einer Vielzahl der Verbraucher deshalb regelmäßig gar nicht als gleichwertige Einwilligungsmöglichkeit wahrgenommen werden. Daran ändert auch der Einleitungstext nichts, da dieser bereits nicht darüber aufklärt, welche Cookies wie vorbelegt sind und damit durch welchen Button, welche Cookies „aktiviert“ werden."*

Darüber hinaus hatte die Betreiberin der Seite zahlreiche Social Media- und Analyse-Tools (hier insbesondere: *Google Analytics*) auf der Webseite eingebunden. Das Gericht vertritt die Auffassung, dass hier eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vorliegt. Über diese hätte die Betreiberin in der Datenschutzerklärung auch informieren müssen. Hinsichtlich dieser Einschätzung verweist das Gericht auf den Beschluss der Datenschutzkonferenz vom 12.05.2020.

Praxishinweis:

- Prüfen Sie die Ausgestaltung Ihres Cookie-Banners. Es sollten keine Voreinstellungen getroffen sein. Damit ist sichergestellt, dass Nutzer*innen eine aktive Entscheidung treffen können; vermeiden Sie bei der Gestaltung des Zustimmungsbuttons Gewichtungen, die manipulierenden Charakter haben.

- Prüfen Sie beim Einsatz von Google Analytics, ob die Datenschutzinformation die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO abbildet.

Wenn Sie Unterstützung benötigen, sprechen Sie Ihren Berater gerne an.

BGH: Informationen zur Streitbeilegung auf Webseiten und AGB erforderlich!

Seit dem 01.02.2017 müssen Online-Händler*innen Verbraucher gemäß § 36 Abs. 1 Verbraucherstreitbeilegungsgesetz (VSBG) darüber informieren, inwieweit sie bereit oder verpflichtet sind, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen. Die Informationspflicht betrifft zwar nicht den Datenschutz, sie wird z.B. im Rahmen der Ausgestaltung des Impressums dennoch oft auch mit den Datenschutzbeauftragten erörtert.

Der BGH (Urt. v. 22.9.2020 – XI ZR 162/19) entschied nun, dass die entsprechenden Informationen sowohl auf der Webseite als auch in den AGB erscheinen müssen, wenn der Unternehmer solche verwende.

Praxishinweis:

Es gibt hier zwei Themen zu beachten, einmal **Online Dispute Resolution (ODR) gemäß Art. 14 Abs. 1 ODR-Verordnung** und **Alternative Dispute Resolution (ADR) gemäß §§ 36, 37 VSBG**.

Von der **Informationspflicht gemäß Art. 14 Abs. 1 ODR-Verordnung** sind fast alle **Onlinehändler*innen** erfasst. Konkret sind alle Unternehmen mit Sitz in der EU betroffen, die (auch) an EU-Verbraucher Waren und/ oder Dienstleistungen verkaufen bzw. Dienstleistungen erbringen, sofern diese ihre Leistungen dabei auf einer Webseite oder sonst auf elektronischem Weg (z.B. per E-Mail) anbieten **und der Verbraucher die Bestellung dann über die Webseite oder sonst auf elektronischem Weg (z.B. per E-Mail) ausführt**.

Die **Informationspflicht nach §§ 36, 37 VSBG** trifft alle Unternehmen, sofern diese eine Webseite betreiben oder AGB haben (es besteht allerdings keine Pflicht sich nur wegen ADR eine Webseite oder AGB zuzulegen). Ausgenommen davon sind lediglich Unternehmen, die am 31. Dezember des Vorjahres weniger als zehn Beschäftigte hatten, § 36 Abs. 3 VSBG, und nicht an einem Streitbeilegungsverfahren teilnehmen.

Sollten Sie hier Unterstützung benötigen, helfen gerne die Kollegen von Eggert & Partner.

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, Yanick Röhricht, 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 § 55 Abs. 2 RStV: Asmus Eggert