BRANDI
RECHTSANWÄLTE

JAHRESRÜCKBLICK 2020 UND AUSBLICK 2021

Informationen zum Datenschutz I Januar 2021

Einleitung

Das Jahr 2020 hat aufgrund der Ausbreitung des Corona-Virus einige Herausforderungen mit sich gebracht, die so nicht vorhersehbar waren und sich auch in der datenschutzrechtlichen Schwerpunktsetzung niedergeschlagen haben. Der verstärkte Einsatz von IT-Technologien als Maßnahme zur Eindämmung des Virus, beispielsweise bei der Tätigkeit im Home Office oder der Organisation von Online-Besprechungen, hat insoweit in Unternehmen zahlreiche datenschutzrechtliche Fragen aufgeworfen.

Neue Entwicklungen im Datenschutzrecht gab es unabhängig von der Corona-Pandemie auch aufgrund neuer Tendenzen und Vorgaben aus der Rechtsprechung – unter anderem bezüglich des Einsatzes von Cookies und der Datenübermittlung in Drittstaaten – sowie aufgrund von Aktivitäten der Aufsichtsbehörden.

Den Jahreswechsel haben wir zum Anlass genommen, in unserem traditionellen Jahresrückblick wesentliche Datenschutzthemen aus dem Jahr 2020 noch einmal Revue passieren zu lassen; gleichzeitig wagen wir auch einen Ausblick auf das Jahr 2021.

Schwerpunktthemen des Datenschutz-Newsletters von BRANDI

In unserem Datenschutz-Newsletter berichten wir jeden Monat über aktuelle Geschehnisse aus dem Datenschutzrecht und informieren zudem vertieft über jeweils ein ausgewähltes Schwerpunktthema. Für das Schwerpunktthema fassen wir auf wenigen Seiten die wesentlichen datenschutzrechtlichen Besonderheiten und besonders praxisrelevanten Hinweise zu einem Bereich zusammen. Die Schwerpunktthemen unseres Datenschutz-Newsletters aus dem Jahr 2020 haben wir nachfolgend noch einmal zusammengefasst.

> Schutz von Gesundheitsdaten
>
> Die Rechenschaftspflicht der DSGVO
>
> Datenschutzrecht im Zusammenhang mit der Corona-Pandemie
>
> Einsatz mobiler Endgeräte in Unternehmen
>
> Die Benennung des Datenschutzbeauftragten und seine Stellung im Unternehmen
>
> Corona-App als Eintrittskarte?
>
> Datenübermittlung in Drittstaaten
>
> Umgang mit Bewerberdaten
>
> Datenschutz bei Instagram
>
> Umgang mit Löschungsanfragen
>
> AdTech – Digitales Marketing und Datenschutz

Rechtsprechung

Im Mai 2020 kam der Bundesgerichtshof (BGH) in einem Urteil zu dem Ergebnis, dass die wirksame Einholung der datenschutzrechtlichen Einwilligung in die Speicherung von Analyse- und Werbe-Cookies mittels einer vorab angekreuzten Checkbox nicht möglich ist (BGH, Urt. v. 28.05.2020, Az.: I ZR 7/16). Soweit die nationale Regelung gem. § 15 Telemediengesetz (TMG) bisher so interpretiert wurde, dass eine Widerspruchslösung bei Cookies zu Werbezwecken ausreichend sei, bedarf es nun einer europarechtskonformen Auslegung. Der BGH knüpft in seinem Urteil inhaltlich an eine Entscheidung des Europäischen Gerichtshofs (EuGH) an, in der ebenfalls von einem Einwilligungserfordernis ausgegangen wurde (EuGH, Urt. v. 01.10.2019, Az. C-673/17).

Seit dem Urteil besteht für Unternehmen endgültig keine Möglichkeit mehr, Analyse- und Werbecookies ohne aktive Einwilligung der Nutzer zu setzen. Ein bloßer Cookie-Hinweis sowie die Umsetzung einer Widerspruchslösung sind nicht mehr ausreichend. Als Folge haben viele Unternehmen im Jahr 2020 ihre Einbindung von Cookies angepasst und auf eine Einwilligungslösung umgestellt.

Eine weitere Entscheidung, der im vergangenen Jahr viel Beachtung geschenkt worden ist, war das Urteil Schrems II des EuGH im Juli 2020 (EuGH, Urt. v. 16.07.2020, Az. C-311/18). In diesem erklärte der EuGH das EU-US Privacy Shield für unwirksam und konkretisierte die Anforderungen an den Einsatz von EU-Standarddatenschutzklauseln bei Datenübermittlungen in Drittstaaten. EU-Standarddatenschutzklauseln können nach Auffassung des EuGH zwar grundsätzlich weiterhin verwendet werden, es sei allerdings im Einzelfall zu bewerten, ob die Rechte der betroffenen Personen in dem Drittstaat ein gleichwertiges Schutzniveau wie in der EU genießen. Insofern seien gegebenenfalls zusätzliche Schutzmaßnahmen zu ergreifen.

In der Folgezeit haben verschiedene Stellen Umsetzungsempfehlungen und Stellungnahmen zu dem Urteil veröffentlicht. Der Europäische Datenschutzausschuss (EDSA) empfiehlt etwa als zusätzliche Schutzmaßnahme bei internationalen Datentransfers insbesondere eine Verschlüsselung, bei der ausschließlich der

Datenexporteur über den Schlüssel verfügt und deshalb faktisch ein Zugriff des Datenimporteurs und damit auch der drittstaatlichen Sicherheitsbehörden auf die Daten ausgeschlossen ist. Unternehmen waren aufgrund des Urteils im letzten Jahr gehalten, ihre Datenübermittlungen in Drittstaaten zu prüfen und zur Umsetzung des Urteils gegebenenfalls zusätzliche Maßnahmen zu treffen.

Der EuGH hatte sich außerdem im Oktober 2020 in zwei Entscheidungen erneut mit dem Thema Vorratsdatenspeicherung zu befassen. Er bestätigte in seinen Urteilen vom 06.10.2020 (Rechtssache C-623/17 sowie die verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18), dass das EU-Recht nationalen Rechtsvorschriften entgegenstehe, die einen Anbieter elektronischer Kommunikationsdienste zur allgemeinen und unterschiedslosen Übertragung oder Speicherung von Verkehrsdaten und Standortdaten zum Zwecke der Verbrechensbekämpfung verpflichten. Ausnahmen könnten sich aber in Situationen ergeben, in denen ein Mitgliedstaat einer schwerwiegenden Bedrohung der nationalen Sicherheit gegenüberstehe, die sich als tatsächliche und gegenwärtige oder vorhersehbare Gefahr erweise.

Aktivitäten von Aufsichtsbehörden

Die Datenschutzaufsichtsbehörden wurden im Jahr 2020 ebenfalls bezogen auf verschiedene datenschutzrechtliche Themen tätig, unter anderem wurden Bußgelder aufgrund von Datenschutzverstößen verhängt und Stellungnahmen zu ausgewählten Themen veröffentlicht.

Bußgelder

Das in Deutschland bisher höchste Bußgeld für Datenschutzverstöße in Höhe von 35 Mio. Euro wurde gegen H&M verhängt. H&M wurde die Überwachung von mehreren hundert Mitarbeitern eines Servicecenters durch die Center-Leitung vorgeworfen. Durch Gespräche mit den Mitarbeitern seien durch Vorgesetzte Informationen zu dem Privatleben der Mitarbeiter erfasst worden. Die Daten seien auch für eine Auswertung und Profilbildung genutzt worden.

Für Schlagzeilen sorgte auch ein Bußgeld gegen den Telekommunikationsdienstleister 1&1 wegen der Herausgabe einer Telefonnummer ohne ausreichende Authentifizierung. Die ehemalige Lebensgefährtin eines Kunden von 1&1 hatte im Callcenter die Telefonnummer ihres früheren Lebenspartners erfragt, indem sie sich als dessen Ehefrau ausgegeben hatte und zur Authentifizierung nur Name und Geburtsdatum ihres früheren Lebensgefährten hatte nennen müssen. Die so erlangte Telefonnummer nutzte sie für Belästigungen. Das Bußgeld wurde von dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zunächst auf 9,5 Millionen Euro festgelegt. Das Landgericht Bonn hat das Bußgeld anschließend zwar dem Grunde nach bestätigt, der Höhe nach jedoch deutlich reduziert auf 900.000 € (LG Bonn, Urt. v. 11.11.2020, Az. 29 OWi 1/20 LG) .

Ein weiteres Bußgeld in Höhe von 1,2 Mio. Euro wurde von dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) Baden-Württemberg gegen die AOK Baden-Württemberg wegen eines Verstoßes gegen die Pflichten zur Sicherheit der Datenverarbeitung nach Art. 32 DSGVO verhängt. Die AOK hatte bei der Erhebung personenbezogener Daten im Rahmen verschiedener Gewinnspiele nicht ausreichend sichergestellt, dass eine Nutzung der Daten zu Werbezwecken nur mit entsprechender Einwilligung des Betroffenen erfolgt.

Stellungnahmen

Die Aufsichtsbehörden äußerten sich in verschiedenen Stellungnahmen zu datenschutzrechtlichen Themen. Im Mai 2020 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) Hinweise zu dem Einsatz von Google Analytics. Darin gibt sie Gestaltungshinweise zur Einholung einer wirksamen Einwilligung und beschreibt die Anforderungen an eine Information des Nutzers sowie zusätzliche Schutzmaßnahmen, die ergriffen werden sollen. Ein rechtmäßiger Einsatz von Google Analytics sei in der Regel nur aufgrund einer wirksamen Einwilligung des Nutzers möglich. Nach Auffassung der DSK bestehe eine gemeinsame Verantwortlichkeit zwischen Google und dem Google-Analytics-Anwender.

Zahlreiche Reaktionen von Aufsichtsbehörden hat das Urteil Schrems II hervorgerufen. Die DSK forderte verantwortliche Stellen dazu auf, ihre Datentransfers in Drittstaaten zu überprüfen. Bei Datenübermittlungen in die USA reichen nach ihrer Auffassung Standardvertragsklauseln ohne zusätzliche Schutzmaßnahmen grundsätzlich nicht aus. Die Wertungen des Urteils seien zudem auch auf verbindliche interne Datenschutzvorschriften („BCR") übertragbar.

Die Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen (LDI NRW) änderte im April 2020 ihren Prozess für die Meldung von Datenschutzvorfällen. Für die Meldung von Datenschutzvorfällen steht nun ein Onlineformular zur Verfügung.

Besondere Herausforderungen aufgrund der Corona-Pandemie

Für besondere Herausforderungen sorgte im Jahr 2020 die Corona-Pandemie. Bei der verstärkten Auslagerung von Tätigkeiten in das Home Office haben Unternehmen sicherzustellen, dass das allgemein im Unternehmen festgelegte Datenschutzniveau auch im Fall von Heimarbeit nicht unterschritten wird. Auch im Rahmen weiterer Maßnahmen, etwa der Abfrage von Kontaktdaten zur Nachverfolgung von Infektionsketten, sind die datenschutzrechtlichen Anforderungen einzuhalten.

Bei der Konzeption der Corona Warn-App waren ebenfalls datenschutzrechtliche Aspekte zu berücksichtigen. Eine zentrale Funktion der App ist die Risiko-Ermittlung, die auf der Bewertung basiert, in welchem Umfang Kontakt mit Personen bestanden hat, die später positiv auf Covid-19 getestet wurden. Die Daten zu dem jeweiligen Nutzer der App werden ausschließlich lokal auf dem jeweiligen Gerät gespeichert, eine zentrale Datenspeicherung ist nicht vorgesehen.

Aufgrund der vermehrten Durchführung von Online-Besprechungen waren datenschutzrechtliche Aspekte bei dem Einsatz von Videokonferenzsystemen ebenfalls ein viel behandeltes Thema im Jahr 2020. Die DSK hat in diesem Zusammenhang im Oktober 2020 eine Orientierungshilfe zu Videokonferenzsystemen herausgegeben, die verantwortlichen Stellen als Hilfestellung bei der Umsetzung der datenschutzrechtlichen Anforderungen an die Durchführung von Videokonferenzen dienen soll.

Ausblick 2021

Verschiedene Datenschutzthemen aus dem Vorjahr werden auch im Jahr 2021 weiterhin eine Rolle spielen, außerdem ist mit neuen Themen zu rechnen.

Als Reaktion auf das Urteil Schrems II hat die Europäische Kommission bereits im November 2020 einen Entwurf überarbeiteter Standardvertragsklauseln veröffentlicht, der die Anforderungen des EuGH aufgreift. Mit der in Aussicht stehenden verbindlichen Veröffentlichung neuer Standardvertragsklauseln im Amtsblatt der EU bleibt zu hoffen, dass Rechtssicherheit bei der Datenübermittlung

in Drittstaaten geschaffen wird. Voraussichtlich entsteht durch die Neuregelungen allerdings auch ein nicht unerheblicher Handlungsbedarf.

Die deutsche EU-Ratspräsidentschaft hat im November 2020 einen überarbeiteten Entwurf für die E-Privacy-Verordnung vorgelegt. Die Verordnung soll die Vertraulichkeit elektronischer Kommunikation stärken. Es bleibt abzuwarten, ob es in der Folgezeit zu einer Einigung über den Entwurf und einer Verabschiedung der Verordnung kommen wird, nachdem das Regelwerk eigentlich schon parallel zur DSGVO gelten sollte. Mit einem Inkrafttreten ist aber selbst nach einer Verständigung nicht vor 2023 zu rechnen.

Fragen des internationalen Datentransfers werden sich zukünftig auch bei Datenübermittlungen nach Großbritannien stellen. Bis zum 31.12.2020 galt aufgrund der Art. 126, 127 des Abkommens über den Austritt des Vereinigten Königreichs Großbritannien und Nordirland aus der Europäischen Union und der Europäischen Atomgemeinschaft das Unionsrecht und damit auch die DSGVO für das Vereinigte Königreich fort.

Aufgrund des Brexit-Abkommens zwischen der EU und dem Vereinigten Königreich vom 31.12.2020 gilt das Vereinigte Königreich für einen weiteren Übergangszeitraum von vier Monaten, der auf bis zu sechs Monate verlängert werden kann, bei Übermittlungen personenbezogener Daten nicht als Drittstaat im Sinne der DSGVO. Es bleibt abzuwarten, wie sich die Rechtslage nach dem Übergangszeitraum darstellen wird. Ohne einen entsprechenden Angemessenheitsbeschluss wird das Vereinigte Königreich zu einem „unsicheren" Drittstaat werden, sodass die Anforderungen der Art. 44 ff. DSGVO zu beachten sind.

Über die datenschutzrechtlichen Herausforderungen und Geschehnisse, die das Jahr 2021 mit sich bringen wird, wird das Datenschutzteam von BRANDI Sie natürlich auch im neuen Jahr in seinem Datenschutz-Newsletter auf dem Laufenden halten.

Johanna Schmale

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 890
F +49 521 96535 - 113
M johanna.schmale@brandi.net