BRANDI
RECHTSANWÄLTE

BRANDI IM GESPRÄCH MIT DEM LANDESDATENSCHUTZBEAUFTRAGTEN

Einleitung

Ein Interesse für den Datenschutz und die Informationsfreiheit zu wecken und die Bürgerinnen und Bürger mit diesen Themen zu erreichen, sind zentrale Anliegen von Herrn Dr. Stefan Brink, dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg. Herr Dr. Brink übt das Amt, in das er von dem Landtag in Baden-Württemberg für die Dauer von sechs Jahren gewählt wurde, seit dem 01.01.2017 aus. In zahlreichen Veröffentlichungen, Tagungsbeiträgen und Vorträgen trägt er zu dem Fachdiskurs bei, macht seine Anliegen von Datenschutz und Informationsfreiheit durch Veranstaltungen, Interviews und andere Formate mit Bürgerinnen und Bürgern aber auch der breiten Öffentlichkeit verfügbar.

Auf dem IT- und Datenschutztag am 30.09.2021 war Herr Dr. Brink zu Gast bei BRANDI in Bielefeld. In Gesprächen sowohl mit Rechtsanwältinnen und Rechtsanwälten von BRANDI als auch mit einigen unserer Mandantinnen und Mandanten gab er einen spannenden Einblick in verschiedene datenschutzrechtliche Themen und die tägliche Arbeit einer Datenschutzaufsichtsbehörde.

In dem ersten Teil der Veranstaltung ging es unter anderem um rechtliche Fragestellungen bezüglich des Einsatzes von Cookies, der Freiwilligkeit von Einwilligungen und der Analyse des Nutzerverhaltens sowie des internationalen Datentransfers. Frau Dr. Laura Schulte und Herr Dr. Christoph Rempe von BRANDI stellten Herrn Dr. Brink Fragen zu diesen Themen, die zu einem großen Teil vorab von unseren Mandantinnen und Mandanten an uns herangetragen wurden. Die wesentlichen Aspekte aus dem Gespräch, von dem Mitschnitte auch auf unserem YouTube-Kanal abgerufen werden können, haben wir in dem folgenden Beitrag aufbereitet.

Dr. Christoph Rempe, Dr. Laura Schulte und Dr. Stefan Brink (von links nach rechts) haben sich auf dem IT- und Datenschutztag zu verschiedenen datenschutzrechtlichen Themen ausgetauscht. Moderiert wurde das Gespräch von Dr. Christoph Worms (rechts).

Rechtliche Fragestellungen zu dem Einsatz von Cookies

Cookies sind kleine Textdateien, die in Online-Anwendungen zum Einsatz kommen und auf dem Endgerät des Nutzers gespeichert werden. Sie können nicht nur bestimmte Voreinstellungen verfügbar machen und die Nutzung einer Online-Anwendung ermöglichen, sondern darüber hinaus weitere Daten erfassen, die zum Beispiel dem Tracking und der Analyse des Nutzerverhaltens dienen. Hierzu hat der BGH in einem Urteil vom 28.05.2020 (Az. I ZR 7/16) entschieden, dass für das Setzen von Cookies zu Zwecken der Werbung oder Marktforschung die aktive Einwilligung des Nutzers einzuholen ist. Über rechtliche Fragestellungen im Zusammenhang mit dem Einsatz von Cookies, insbesondere über datenschutzrechtliche Informationspflichten, haben wir uns mit Herrn Dr. Brink unterhalten.

Umfang der datenschutzrechtlichen Informationspflichten

Hinsichtlich des Umfangs der datenschutzrechtlichen Informationspflichten beschrieb Herr Dr. Brink ein Spannungsverhältnis: Einerseits müsse man den Nutzer vollumfänglich über die Datenverarbeitung informieren, andererseits könnten sehr umfangreiche Informationen und insbesondere sehr technische Erklärungen einen Nutzer überfordern und der Informiertheit sogar entgegenwirken.

Die Lösung hierfür sei eine Abschichtung der Datenschutzinformation. Zwar sei es erforderlich, dem Betroffenen vollständige Informationen zu erteilen. Diese müssten aber möglicherweise nicht für alle Betroffenen sofort sichtbar sein. In vielen Fällen reiche es aus, zunächst Grundinformationen zur Verfügung zu stellen und erst auf einer zweiten Ebene interessierte Nutzer mit zusätzlichen Informationen zu versorgen. Dies könne etwa so umgesetzt werden, dass die Grundinformationen einen weiterführenden Hinweis auf die zusätzlichen Informationsmöglichkeiten, zum Beispiel über ausgelegte Informationsblätter oder auf der verlinkten Homepage, enthalten. Die weiterführenden Informationen könnten dann etwa detaillierte Informationen zu jedem Cookie, unter anderem zu dessen Zweck und der Speicherdauer, enthalten. Eine solche Abschichtung der Information sei auch in anderen Bereichen möglich, zum Beispiel bei der Videoüberwachung.

Herr Dr. Brink wies darauf hin, dass es sehr konkrete Vorgaben zu dem jeweiligen Umfang der Grundinformationen und der weiterführenden Hinweise weder in der DSGVO noch von den Datenschutzaufsichtsbehörden und dem Europäischen Datenschutzausschuss (EDSA) gebe. Der Verantwortliche habe somit einen Gestaltungsspielraum. Am Ende müsse jedoch in jedem Fall eine vollständige Information vorliegen, damit eine betroffene Person differenziert entscheiden könne, in welchen Bereichen sie mit dem Setzen von Cookies einverstanden ist und in welchen nicht.

Einholung von Einwilligungen in das Setzen von Cookies
Im Zusammenhang mit der Einholung von Einwilligungen in das Setzen von Cookies betonte Herr Dr. Brink die Informiertheit und die Freiwilligkeit der Einwilligung. Das sogenannte „Nudging", durch das der Nutzer dazu bewegt werden soll, seine Einwilligung abzugeben, kollidiere mit der Freiwilligkeit. Als Beispiele hierfür nannte Herr Dr. Brink das Hervorheben des „Zustimmen-Buttons" durch farbliche Gestaltungen oder die Größe des Buttons sowie das „Verstecken" der Ablehnmöglichkeit oder der Einstellungen hinter langen oder irreführenden Klickwegen.

Bei einer besonders extremen Beeinflussung kann eine freie Entscheidung des Nutzers gefährdet sein. Unternehmen sollten insofern auf einen fairen Umgang mit dem Nutzer und dessen Rechten achten. Insbesondere solle auch die Erteilung der Einwilligung im Vergleich zu ihrem Widerruf nicht wesentlich leichter oder wesentlich anders gestaltet werden. Ein Gestaltungsspielraum bestehe dahingehend, dass der Nutzer durchaus eine Tendenz und das Interesse des Verantwortlichen an der Datenverarbeitung spüren dürfe. Diese Tendenz dürfe jedoch keinen manipulativen Charakter haben und der Nutzer müsse selbst über die Erteilung oder Verweigerung seiner Einwilligung entscheiden können. Das Einschreiten der Aufsichtsbehörde sei diesbezüglich in der Regel immer erst dann zu erwarten, wenn es sich um eindeutige Fälle handele, in denen eine freie Entscheidung des Nutzers nicht mehr gewährleistet sei.

Cookieless Tracking
Neue technische Ansätze, wie zum Beispiel Tracking Pixel und Fingerprinting, eröffnen immer mehr Möglichkeiten, Nutzer zu identifizieren. Derartige Technologien können dem Tracking von Nutzern dienen, ohne dabei Cookies zu setzen.

Hierzu ist nach Ansicht von Herrn Dr. Brink eine differenzierte Betrachtung erforderlich. In der Regel seien die Technologien mit Cookies derart vergleichbar, dass die Einholung von Einwilligungen der Betroffenen für ihre Nutzung erforderlich sei. Aktuell sei dies jedenfalls die sicherere Lösung. Es sei jedoch nicht auszuschließen, dass die Datenverarbeitung in bestimmten Konstellationen bei einem schonenden Vorgehen auch auf das berechtigte Interesse gem. Art. 6 Abs. 1 S. 1 lit. f) DSGVO gestützt werden könne.

In diesem „Erprobungsfeld" riet Herr Dr. Brink nicht zwingend zur Zurückhaltung, sondern zu einer gut überlegten offensiven Umgangsweise mit neuen Technologien. Neue Möglichkeiten dürfen seiner Ansicht nach durchaus genutzt werden, allerdings sollten verantwortliche Unternehmen aufmerksam die Äußerungen von Aufsichtsbehörden und Gerichten verfolgen und regelmäßig ihr eigenes Risiko einschätzen. Zumindest die süddeutschen Aufsichtsbehörden hätten ohnehin einen beratenden Ansatz. Ihr Ziel sei nicht, spektakuläre Fälle oder hohe Bußgelder zu erzielen. Vielmehr würden sie die Verantwortlichen in ihrem Wunsch, die Technik weiterzuentwickeln und möglichst viel aus ihren Kundenbeziehungen herauszuholen, verstehen. Das Gespräch mit den Verantwortlichen und die gemeinsame Entwicklung von Lösungen sei zudem der beste Schutz für die Betroffenen, da auf diese Weise Projekte von Vornherein vernünftig aufgesetzt werden könnten und nicht erst im Nachhinein Betroffenenanfragen abgewickelt werden müssten.

Freiwilligkeit und Kopplung

Ein weiteres Thema, das intensiv mit Herrn Dr. Brink diskutiert wurde, war die Möglichkeit zur Erlangung von Einwilligungen der Betroffenen bei verschiedenen Online-Angeboten. Der Versand von Newslettern dient beispielsweise vielen Unternehmen zu Werbezwecken. Um mit der Werbung einen möglichst großen Personenkreis zu erreichen, kann es hilfreich sein, besondere Anreize für eine Newsletter-Anmeldung zu schaffen. Als mögliche Maßnahme ist es beispielsweise denkbar, betroffenen Personen als „Belohnung" für ihre Newsletter-Einwilligung einen Warengutschein anzubieten. Nach Art. 7 Abs. 4 DSGVO ist allerdings bei der Beurteilung, ob eine datenschutzrechtliche Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung zu tragen, ob unter anderem die Erfüllung eines Vertrags von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Es stellt sich deshalb die Frage, ob ein solches Vorgehen mit der Freiwilligkeit der Einwilligung und dem Kopplungsverbot vereinbar ist.

Herr Dr. Brink hält dabei das Schaffen von positiven Anreizen auch in Bereichen, die von dem ursprünglichen Datenverarbeitungsprozess entkoppelt sind, für vertretbar. Für seine Aufsichtsbehörde komme das Kopplungsverbot immer nur dann zum Tragen, wenn offenkundige Nachteile für den Betroffenen zu sehen seien. Wenn der Betroffene lediglich positive Anreize bekomme und dadurch überzeugt werde, sei dies kein Angriff auf seine Selbstbestimmungsfreiheit und kein Fall von Art. 7 Abs. 4 DSGVO. Wichtig sei jedoch, dass die entsprechenden Einwilligungen auch in diesen Fällen entsprechend der Anforderungen der DSGVO eingeholt werden und die Betroffenen ihre Einwilligungen jederzeit widerrufen können.

Analyse des Nutzerverhaltens

Unternehmen, die einen Onlineshop betreiben, gewinnen regelmäßig eine Vielzahl an Daten von ihren Kunden. Zur Verbesserung der eigenen Leistungen und Marketingmaßnahmen besteht in den Unternehmen regelmäßig der Wunsch, diese Daten zu analysieren, um weitere Informationen über die Interessen und Kaufgewohnheiten der Kunden zu erhalten.

Frau Dr. Laura Schulte im Gespräch mit Herrn Dr. Stefan Brink.

Rechtsgrundlage für die Datenverarbeitung
Herr Dr. Brink schloss es nicht grundsätzlich aus, die Datenverarbeitung zu internen Analysezwecken über das berechtigte Interesse gem. Art. 6 Abs. 1 S. 1 lit. f) DSGVO zu rechtfertigen. In Bereichen, in denen die schutzwürdigen Belange der betroffenen Kunden offensichtlich schwerwiegend seien, halte er jedoch in der Regel die Einwilligung für die bessere und sichere Rechtfertigungsmöglichkeit. Dies könne zum Beispiel der Fall sein, wenn sensible Daten betroffen seien und der Verarbeiter die Daten nicht nur selbst für eigene Zwecke nutze, sondern dabei Dienstleister einsetze oder Dritten den Zugriff auf die Daten ermögliche.

Die Aufsichtsbehörden würden in diesen Fällen auf eine gute und faire Argumentation der verantwortlichen Stellen im Einzelfall Wert legen. Verantwortliche sollten sich die Interessenkollision vor Augen führen und ernsthaft mit den schutzwürdigen Belangen der

Betroffenen umgehen. Dazu gehört nach Ansicht von Herrn Dr. Brink, dass Verantwortliche nachvollziehbar darlegen, warum sie in einem konkreten Fall zu dem Ergebnis kommen, dass das berechtigte Interesse die schutzwürdigen Belange des Betroffenen überwiegt. Dieser Abwägungsvorgang solle sorgfältig dokumentiert werden. Mit einer entsprechenden guten Argumentation und Dokumentation könne die Berufung auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO somit durchaus möglich sein.

Personalisierte Werbung für registrierte Kunden

Über registrierte Nutzer mit einem eigenen Kundenkonto in einem Onlineshop liegen Unternehmen regelmäßig besonders viele Informationen vor. Basierend auf bereits gekauften Produkten und dem Verhalten der Nutzer ist es denkbar, den betroffenen Kunden personalisierte Werbung anzuzeigen. Wir haben Herrn Dr. Brink gefragt, wie er ein solches Vorgehen im Hinblick auf das Erfordernis von datenschutzrechtlichen Einwilligungen beurteilt.

Herr Dr. Brink wies darauf hin, dass sich die Einholung von Einwilligungen bei einer vernünftigen Konzeption von personalisierter Werbung regelmäßig einfach umsetzen lasse. Durch die Einholung der Einwilligung seien Unternehmen auf der sicheren Seite und könnten sich Folgefragen ersparen.

In den Fällen, in denen keine Einwilligung der Nutzer vorliegt oder Unternehmen etwa wegen des Aufwands keine Einwilligung einholen wollen, sei zu differenzieren. Eine Rechtfertigung über das berechtigte Interesse gem. Art. 6 Abs. 1 S. 1 lit. f) DSGVO komme eher in den Fällen in Betracht, in denen die Datenverarbeitung überschaubar und für den Betroffenen nicht überraschend sei. In Situationen, in denen der Betroffene überrascht werde und seine Erwartungen übergangen würden, wenn sich zum Beispiel die Analyse auf für den Betroffenen nicht vorhersehbare Bereiche beziehe oder es sich um Gesundheitsdaten handele, seien die schutzwürdigen Belange des Betroffenen in der Regel höher anzusetzen. In diesen Fällen sei die Einholung von informierten Einwilligungen erforderlich.

Tracking von Newsletter-Empfängern

Unternehmen haben regelmäßig ein Interesse daran, Informationen über die Nutzung der von ihnen versendeten Newsletter zu erhalten. Angaben darüber, ob ein Newsletter geöffnet wird und ob der Empfänger auf darin enthaltene Links klickt, können wichtige Hinweise für die Verbesserung der eigenen Marketingmaßnahmen liefern.

Für die praktische Umsetzung hat Herr Dr. Brink insofern empfohlen, die Einwilligung in den Newsletter-Empfang und die Einwilligung bezüglich der Datenverarbeitung hinsichtlich der Art und Weise der Newsletter-Nutzung gemeinsam bei der Newsletter-Anmeldung abzufragen. Auch die jeweils zu erteilenden Informationen über die Datenverarbeitung sollten seiner Ansicht nach für beide Datenverarbeitungen an dieser Stelle platziert werden. Die Einholung von Einwilligungen sei insbesondere bei einer sehr weitreichenden Profilbildung, bei sensiblen Daten und besonders neuartigen überraschenden Datenverarbeitungen erforderlich.

Aufgrund der sich ständig erweiternden technischen Möglichkeiten unterliege der Bereich der Personalisierung einem steten Wandel. Nach Ansicht von Herrn Dr. Brink sei deshalb nicht auszuschließen, dass sich auch die rechtliche Beurteilung mit der Zeit ändern könne. Wachsende Kenntnisse über Trackingmöglichkeiten im Internet und veränderte Nutzererwartungen könnten etwa dazu führen, dass Verantwortliche sich zukünftig leichter auf das berechtigte Interesse zur Rechtfertigung der Datenverarbeitung stützen könnten als aktuell. Die DSGVO sei technikoffen und versuche nicht, technischen Fortschritt zu verhindern. Damit aber die technischen Neuerungen und die damit einhergehenden Datenverarbeitungen auch von den Betroffenen verstanden werden, müsse durch eine sorgfältige Aufklärung der Betroffenen und in der Regel auch durch die Einholung von Einwilligungen nachgesteuert werden.

Internationaler Datentransfer

Als „spannendes“, aber auch „leidvolles“ Thema bezeichnete Herr Dr. Brink die Datenübermittlung in die USA. Nachdem der Europäische Gerichtshof (EuGH) in seiner Entscheidung „Schrems II“ vom 16.07.2020 (Az. C-311/18) das EU-US-Privacy-Shield für unwirksam erklärt und die Anforderungen an den Einsatz von Standardvertragsklauseln konkretisiert hat, hat die Europäische Kommission am 04.06.2021 aktualisierte Standardvertragsklauseln verabschiedet. Unternehmen stellt sich daher aktuell die Frage, ob die neuen Standardvertragsklauseln Datentransfers in die USA absichern können und worauf sie bei ihrem Einsatz zu achten haben.

Im Rahmen der Veranstaltung fand ein reger Austausch zu Datenschutzthemen statt. Hier sind Herr Dr. Daniel Wittig, Herr Dr. Sebastian Meyer, Herr Dr. Stefan Brink und Frau Christina Prowald (von links nach rechts) im Gespräch zu sehen.

Nach der Ansicht von Herrn Dr. Brink enthalten die neuen Standardvertragsklauseln gute Lösungsansätze. Diese beständen im Wesentlichen in verbesserten Informationspflichten gegenüber Betroffenen sowie der Rechtspflicht von Dienstleistern im Ausland, sich gegen behördliche Anforderungen gerichtlich zu wehren.

Die Lösungsansätze seien aber nicht für alle Fälle ausreichend. Vielmehr werde es neben den vertraglichen Grundlagen immer auch technischer und organisatorischer Maßnahmen, beispielsweise Verschlüsselungstechniken, bedürfen.

Problematisch sei der relativ theoretische Ansatz des EuGH, nach dem der Druck, bestimmte Dienstleister in Drittstaaten nicht mehr zu nutzen, von den deutschen Aufsichtsbehörden über die verantwortlichen Stellen an die US-Dienstleister weitergegeben werden solle, was wiederum die US-Regierung zu einem Abkommen mit der EU bewegen solle. Zwar würden sich einige amerikanische Anbieter bereits auf die Situation einrichten, indem sie ihre Datenverarbeitungen in den europäischen Raum verlagern. Microsoft habe etwa angekündigt, wesentliche Datenverarbeitungen bis Ende des Jahres 2022 nach Europa zu verlegen. Eine politische Einigung sei aktuell aber nicht in Sicht.

Insgesamt können somit auch die neuen Standardvertragsklauseln die rechtlichen Probleme bei dem Datentransfer in die USA nicht vollständig lösen. Es ist jedoch ein guter Ansatz, die neuen Standardvertragsklauseln spätestens nach Ablauf der Umsetzungsfrist zu verwenden. Außerdem sollten verantwortliche Stellen sich um weitere Schutzmaßnahmen, wie zum Beispiel Verschlüsselungs- oder Anonymisierungstechniken und Zusatzvereinbarungen, bemühen, um sich in der aktuell schwierigen Situation möglichst gut abzusichern, bis in der Zukunft hoffentlich eine politische Einigung auf höherer Ebene erzielt werden kann.

Brexit: Wie sicher sind Datentransfers nach Großbritannien?
Sowohl eine Äußerung der britischen Regierung, dem „Datenschutzwahnsinn“ in der EU nicht mehr ohne weiteres nachkommen und sich von der DSGVO distanzieren zu wollen, als auch der kurzfristig getroffene Angemessenheitsbeschluss zur Absicherung von Datentransfers in das Vereinigte Königreich zeigen, dass der Brexit eine gewisse datenschutzrechtliche Relevanz hat.

Nach Ansicht von Herrn Dr. Brink sei der Angemessenheitsbeschluss für Großbritannien bei realistischer Betrachtung noch stärker angreifbar und noch unsicherer als das EU-US-Privacy-Shield. Dies liege unter anderem daran, dass die von dem EuGH in seiner Entscheidung „Schrems II“ benannten Kritikpunkte, insbesondere das Auftreten der Sicherheitsbehörden in den USA, auch im Vereinigten Königreich zu verzeichnen seien, weil dort ein ähnliches Niveau der Überwachung herrsche. Es sei daher für Datenschützer und den EDSA „fast nicht begreiflich“, wie die EU-Kommission den Angemessenheitsbeschluss fällen konnte.

Da der Beschluss trotzdem gefasst wurde, dürften sich Verantwortliche auch zunächst darauf stützen. Die Chancen, dass der Beschluss von Dauer sein werde, seien aber deutlich geringer als in Bezug auf die USA, weshalb man sich nicht vollends auf ihn verlassen dürfe. Herr Dr. Stefan Brink kritisierte in diesem Zusammenhang das Verhalten der britischen Regierung, die öffentlich ihre Distanzierung von dem europäischen Datenschutz signalisiere.

Angesichts dieses Verhaltens bestehe ein hoher Druck auf die EU-Kommission, die Wirksamkeit und die Angemessenheit des Angemessenheitsbeschlusses ständig im Blick zu haben.

Die Rechtsanwender dürfen zu diesem Thema jedoch auf die Unterstützung der Aufsichtsbehörden hoffen. Herr Dr. Brink sagte hierzu, dass sich seine Aufsichtsbehörde im Rahmen eines kooperativen Ansatzes bemühe, in diesem Bereich zu unterstützen, um die Ziele des Datenschutzes letztendlich zu verwirklichen.

Fazit

Herr Dr. Brink hat auf unserem IT- und Datenschutztag ausführlich zu verschiedenen datenschutzrechtlichen Themen Stellung bezogen und dabei deutlich gemacht, dass einerseits verantwortliche Unternehmen die Vorgaben des Datenschutzrechts einhalten und sich um einen möglichst hohen Schutz personenbezogener Daten, besonders in sensiblen Bereichen, bemühen müssen, dass andererseits seine Aufsichtsbehörde den Verantwortlichen aber auch unterstützend und beratend zur Seite steht und Verständnis für die Ziele und Geschäftsmodelle von Unternehmen sowie den technischen Fortschritt hat. Es bleibt zu hoffen, dass auch in der Zukunft ein kooperatives Verhältnis zwischen den Datenschutzaufsichtsbehörden und den Anwendern bestehen bleibt, um auf diese Weise die Ziele des Datenschutzes gemeinsam zu verwirklichen.

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