BRANDI
RECHTSANWÄLTE

BRANDI-DATENSCHUTZRECHTSTAG ZUM THEMA „DATENSCHUTZVORFÄLLE“

English version

Einleitung

Am 15.09.2022 war Herr Carl Christoph Möller zu Gast bei BRANDI in Bielefeld. Herr Möller betreut im Rahmen seiner Tätigkeit als Syndikusanwalt und Referent für Datenschutz & Datensicherheit bei der Verbraucherzentrale NRW insbesondere außergerichtliche und gerichtliche Verfahren der Verbraucherzentrale in datenschutzrechtlichen Fragen. Im Rahmen des diesjährigen Datenschutzrechtstags zu dem Thema „Datenschutzvorfälle – Beteiligte, Konsequenzen und Absicherung“ gab er im Gespräch mit Rechtsanwälten von BRANDI, darunter Herr Dr. Sebastian Meyer, Herr Dr. Christoph Rempe, Herr Dr. Daniel Wittig und Herr Dr. Christoph Worms, einen spannenden Einblick in verschiedene datenschutzrechtliche Themen, aktuelle Verfahren und die tägliche Arbeit der Verbraucherzentrale.

Im Rahmen der Veranstaltung wurden Fragestellungen rund um die Thematik „Datenschutzvorfälle“ aus verschiedenen Perspektiven beleuchtet. Im ersten Teil diskutierten die Teilnehmer unter anderem über den Begriff des Datenschutzvorfalls, die Geltendmachung und den Missbrauch von Betroffenenrechten, Schadensersatzansprüche sowie verfahrensrechtliche Aspekte. Zum Einstieg referierte Herr Möller zum Thema „Rechtsdurchsetzung als Verbraucherverband im Datenschutz – Update Verbandsklagemöglichkeiten und Fallbeispiel Cookies“. Im zweiten Teil wurden im Anschluss an den Impulsvortrag „Europaweit einheitliche Sanktionierung?“ von Herrn Dr. Daniel Wittig das Vorgehen bei Datenschutzvorfällen, die Maßstäbe für die Bemessung von Bußgeldern, die Rolle der Aufsichtsbehörden und die Zusammenarbeit von Unternehmen und Aufsichtsbehörden thematisiert.

Die wesentlichen Inhalte unseres Datenschutzrechtstags haben wir für Sie nachfolgend aufbereitet.

Datenschutzvorfälle – Rechte und Pflichten der Beteiligten

Der erste Teil der Veranstaltung widmete sich vor allem den Fragen, was unter einem Datenschutzvorfall zu verstehen ist und welche Rechte und Pflichten sich für die Beteiligten ergeben.

Begriff des Datenschutzvorfalls

Hinsichtlich der Frage, was überhaupt unter einem Datenschutzvorfall zu verstehen ist, erläuterte Herr Dr. Meyer zunächst, dass die DSGVO den Begriff des Datenschutzvorfalls an sich nicht kenne, sondern vielmehr von der Verletzung des Schutzes personenbezogener Daten spreche. Im Kern gehe es darum, dass eine nicht ordnungsgemäße Verarbeitung personenbezogener Daten stattfinde. Hierunter fielen entsprechend der Begriffsdefinition der DSGVO vor allem der Verlust, die nicht ordnungsgemäße Nutzung sowie die unbefugte Offenlegung personenbezogener Daten. Differenziert werden könne in der Praxis in der Regel weiter zwischen einmaligen Vorkommnissen, die zu einer unrechtmäßigen Datenverarbeitung geführt haben – etwa die einmalige Fehlversendung einer E-Mail an einen falschen Verteiler –, und der systematischen Nichteinhaltung datenschutzrechtlicher Vorschriften – etwa das bewusste Nichtergreifen von Absicherungsmaßnahmen.

Verbraucherzentrale und Datenschutzvorfälle

Sowohl in seinem Impulsvortrag als auch in der anschließenden Podiumsdiskussion berichtete Herr Möller, dass die Verbraucherzentrale im Rahmen ihrer täglichen Arbeit einen guten Überblick darüber erhalte, welche datenschutzrechtlichen Themen Verbraucher (und damit potentielle Betroffene) gerade beschäftigen, in welchen Bereichen es aktuell zu Datenschutzvorfällen komme und sich Verbraucher in ihren Rechten verletzt sähen. Die Sachverhalte, die von den Verbrauchern an die Verbraucherzentrale herangetragen würden, beträfen häufig die übermäßige Datenverarbeitung in Online-Shops oder im Rahmen von Kundentreueprogrammen, die werbliche Ansprache von Verbrauchern, die Nutzung von Cookies und Cookie-Bannern sowie Änderungen in Datenschutzhinweisen. Insbesondere in den Bereichen, in denen Verbraucher verstärkt Verstöße wahrnähmen, werde die Verbraucherzentrale sodann prüfend tätig. Herr Möller erklärte, dass neben Verbraucherbeschwerden zum einen die Marktbereinigung (die Aufdeckung von Fällen, in denen Unternehmen bereits höchstrichterlich geklärte Fragen nach wie vor mangelhaft umsetzen, und deren Verfolgung) und zum anderen die höchstrichterliche Klärung strittiger Grundsatzfragen die häufigsten Auslöser für von der Verbraucherzentrale initiierte Verfahren seien. Als ein in der vergangenen Zeit auch für die Verbraucherzentrale besonders relevantes Thema griff Herr Möller dabei den Umgang mit Cookies und die Gestaltung von Cookie-Bannern heraus.

Beispiel: Cookie-Nutzung

Bei Cookies handelt es sich um kleine Textdateien, die in Online-Anwendungen genutzt werden und auf den Endgeräten der Nutzer gespeichert werden. Während einige Cookies dazu dienen, bestimmte Einstellungen verfügbar zu machen und die Nutzung einer Online-Anwendung zu ermöglichen (technisch notwendige Cookies), werden andere Cookies etwa zum Tracking und zur Analyse des Nutzerverhaltens genutzt (technisch nicht notwendige Cookies). Dem EuGH folgend hat der BGH in seiner Entscheidung 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 der Nutzer eingeholt werden muss. Hierzu wer-

den von Unternehmen häufig Cookie-Banner verwendet. Diese müssen nach aktuellem Stand so gestaltet sein, dass dem Nutzer neben einer Annahmemöglichkeit auch eine leicht zugängliche Möglichkeit zur Ablehnung von Cookies zur Verfügung steht.

Auf Nachfrage aus dem Publikum, ob bei der ausschließlichen Nutzung technisch nicht notwendiger Cookies ein Cookie-Banner nicht notwendig sei, wiesen sowohl Herr Möller als auch Herr Dr. Meyer übereinstimmend darauf hin, dass grundsätzlich im Einzelfall zu prüfen sei, ob tatsächlich keinerlei einwilligungspflichtige Datenverarbeitung durch Cookies oder andere Technologien im Rahmen der Online-Anwendung erfolge. Sofern dies tatsächlich der Fall sei, sei auch ein entsprechender Mechanismus zur Einholung von Einwilligungen wie etwa ein sog. Cookie-Banner entbehrlich. Weiter sei jedoch grundsätzlich zu berücksichtigen, dass die Einhaltung der datenschutzrechtlichen Informationspflichten dennoch und unabhängig von der Notwendigkeit eines Cookie-Banners seitens der Unternehmen zu beachten sei.

Herr Dr. Meyer erläuterte darüber hinaus, dass auch die Erfassung und Verarbeitung personenbezogener Daten zur Nutzeranalyse durch andere Technologien (sog. Cookieless Tracking) einen rechtfertigungsbedürftigen Sachverhalt darstelle und es insoweit einer Rechtsgrundlage bedürfe und ggf. eine Einwilligung einzuholen sei. Zudem wies Herr Dr. Meyer darauf hin, dass es in der Praxis häufig aus taktischen Gründen sinnvoll sein könne, unabhängig von dessen Erforderlichkeit ein Cookie-Banner zu nutzen, um sich nicht etwaigen mitunter auch unberechtigten Vorwürfen von Betroffenen zum Fehlen eines Cookie-Banners und einem entsprechenden Rechtfertigungsaufwand aussetzen zu müssen.

Herr Möller berichtete zudem von der im letzten Jahr durchgeführten Cookie-Banner-Aktion der Verbraucherzentralen, im Rahmen derer 1000 Online-Auftritte von Unternehmen dahingehend überprüft wurden, ob die seitens des BGH vorgegebenen Anforderungen korrekt umgesetzt wurden. Dabei konnten 100 datenschutzrechtliche Verstöße aufgedeckt und von den Verbraucherzentralen einer außergerichtlichen oder gerichtlichen Klärung zugeführt werden.

Auskunftsanspruch und dessen Missbrauch

Ausgehend von dem Recht auf informationelle Selbstbestimmung, dem entsprechend Betroffene grundsätzlich selbst darüber entscheiden können sollen, welche personenbezogenen Daten von ihnen von welcher Stelle zu welchem Zweck verarbeitet werden dürfen, sieht das Datenschutzrecht für Personen, die von einer Verarbeitung personenbezogener Daten betroffen sind (Betroffene), umfangreiche Rechte vor. Eines der zentralen Betroffenenrechte nach dem Konzept der DSGVO ist der Auskunftsanspruch nach Art. 15 DSGVO.

Herr Dr. Meyer erläuterte zunächst, dass der Auskunftsanspruch insbesondere dazu diene, herausfinden zu können, welche Daten über die eigene Person von dem jeweiligen Verantwortlichen verarbeitet würden, und die Rechtmäßigkeit des Datenverarbeitungsprozesses zu überprüfen. In der Praxis werde der Auskunftsanspruch laut Herrn Dr. Meyer und Herrn Dr. Rempe jedoch oftmals geltend gemacht, um die eigene Unzufriedenheit über ein sonstiges Verhalten des Unternehmens zum Ausdruck zu bringen oder die Geltendmachung anderer Ansprüche (insbesondere Schadensersatzansprüche) vorzubereiten. Werde der Auskunftsanspruch ausschließlich auf Basis solch sachfremder Erwägungen geltend gemacht, sei dies häufig ein Indiz für dessen Missbrauch. Insbesondere auch in den Fällen, in denen der Auskunftsanspruch in der Hoffnung geltend gemacht werde, dass dieser nicht ordnungsgemäß beantwortet wird, um anschließend weitergehende Ansprüche insbesondere kommerzieller Art gegen das Unternehmen geltend zu machen, liegt aus Sicht von Herrn Dr. Meyer ein missbräuchliches Verhalten vor. Die DSGVO selbst beschäftige sich mit dem Thema Missbräuchlichkeit bei der Geltendmachung von Betroffenenrechten lediglich in Art. 12 Abs. 5 DSGVO. Hier gehe es jedoch ausschließlich um den quantitativen Exzess bei der Geltendmachung von Betroffenenrechten. Auf die Frage, inwieweit sachfremde Erwägungen die Missbräuchlichkeit eines Auskunftsanspruchs begründen können, finde sich in der DSGVO hingegen keine Antwort. Die Grenzen, wann von einem missbräuchlichen Verhalten ausgegangen werden könne, seien vielmehr noch von der höchstrichterlichen Rechtsprechung zu klären. Herr Dr. Meyer erläuterte, dass die Rechtsprechung zur Frage der Missbräuchlichkeit bislang verschiedene Indizien, wie etwa die Sinnhaftigkeit des Auskunftsverlangens an sich sowie die begründenden Ausführungen des Betroffenen im Rahmen des Auskunftsverlangens, heranziehe. Extrem ausführliche rechtliche Ausführungen sowie die Tatsache, dass es eine Vielzahl schematischer Betroffenenanfragen ohne konkreten Anlass gebe, sprächen ebenfalls für eine Missbräuchlichkeit des Vorgehens.

Vorgehen bei (unberechtigten) Auskunftsansprüchen

Herr Dr. Meyer berichtete im weiteren Verlauf der Diskussion, dass er es häufig erlebe, dass Unternehmen sich fragen, ob sie Dokumente, die vermutlich gegen sie verwendet werden sollen, im Rahmen von Auskunftsbegehren tatsächlich herausgeben müssen und wie am besten mit entsprechenden Anfragen umgegangen werden solle.

Seine praktische Empfehlung lautete, Auskunftsansprüche schon alleine deshalb ernst zu nehmen, um der Gegenseite keine weiteren Angriffspunkte zu liefern. Auskunftsbegehren seien zudem grundsätzlich zu beantworten. Gleichzeitig biete es sich an, die Interessen des Betroffenen zu hinterfragen. Stelle man fest, dass der Betroffene ausschließlich „Geld machen“ wolle, könne die verantwortliche Stelle die Anfrage relativ leicht abblocken. Sei ein Kunde über ein sonstiges Verhalten des Unternehmens verärgert, könnten der Kundenservice und eine Fokussierung auf das eigentliche Anliegen des Kunden häufig weiterhelfen.

Grundsätzlich wies Herr Dr. Meyer darauf hin, dass bei der Beantwortung des Auskunftsbegehrens darauf geachtet werden sollte, nicht den Eindruck zu erwecken, man habe alle vorliegenden Informationen geliefert, soweit man nicht ausschließen könne, dass noch weitere Daten im Unternehmen vorhanden seien. Seine Empfehlung lautete insofern, darzulegen, welche Systeme man durchsucht und welche Daten man gefunden habe. Gleichzeitig biete es sich an, darauf aufmerksam zu machen, dass möglicherweise noch mehr Daten gespeichert seien, und gezielt nachzufragen, welche Daten für den Betroffenen von besonderem Interesse seien, um bei Bedarf weitergehende Auskünfte erteilen zu können. Auf diese Weise könnten berechtigte Anliegen häufig befriedet und missbräuchliche Begehren abgewehrt werden. Würden die Motive erforscht und anschließend entsprechend gehandelt, ließe sich laut Herrn Dr. Meyer ein Großteil der gerichtlichen Verfahren vermeiden.

Herr Dr. Meyer verwies auch auf die Rolle des von Unternehmen zu bestellenden Datenschutzbeauftragten. Dieser sei zum einen in das Unternehmen eingegliedert und für dieses beratend tätig, zum anderen aber auch dafür zuständig, die Interessen der Betroffenen zu wahren. Der Datenschutzbeauftragte sei nach der Grundidee der DSGVO erster Ansprechpartner für die Betroffenen und könne bei etwaigen Vorfällen kontaktiert werden.

Beispiel: Google Fonts
Als Beispiel für einen möglichen Rechtsmissbrauch führte Herr Dr. Wittig die Reaktionen auf eine Entscheidung des Landgerichts München an. Das Gericht entschied zu Beginn diesen Jahres, dass es angemessen sein kann, einem Nutzer einen immateriellen Schadensersatz zuzusprechen, wenn es im Rahmen der Nutzung von Google Fonts durch das dynamische Nachladen der Schriftarten zu einem Abfluss von Nutzerdaten in die USA kommt (LG München, Urt. v. 20.01.2022, Az. 3 O 17493/20). Google sieht grundsätzlich zwei verschiedene Möglichkeiten vor, wie Google Fonts auf einer Seite eingebunden werden können. Entweder können Google Fonts direkt auf dem Server des Seitenbetreibers hinterlegt werden oder es muss für jeden Nutzer ein separater Abruf von den Servern bei Google erfolgen. Bei der letztgenannten Alternative ist es erforderlich, gegenüber Google zumindest die IP-Adresse des Nutzers offenzulegen, was bei der ersten Variante vermieden werden kann. Das Gericht entschied vor diesem Hintergrund, dass das dynamische Nachladen von Inhalten bei Google für die Einbeziehung von Google Fonts unnötig und damit auch datenschutzwidrig ist, weil es eine gleichwertige Alternative gibt, die ohne eine entsprechende Datenübermittlung auskommt. Die Entscheidung des Landgerichts hat dazu geführt, dass es im Nachgang zu einer regelrechten „Abmahnwelle" kam, im Rahmen derer gezielt nach Verstößen bei der Einbindung von Google Fonts gesucht wurde und Schadensersatzansprüche gegen Unternehmen geltend gemacht wurden.

Herr Dr. Meyer betonte diesbezüglich zunächst, dass die Entscheidung des LG München grundsätzlich korrekt sei. Jede Datenverarbeitung erfordere das Vorliegen einer Rechtsgrundlage. In Anbetracht der alternativen, datenschutzkonformen Einbindungsmöglichkeit könne die in Rede stehende Datenübermittlung an Google nicht auf das Vorliegen eines überwiegenden berechtigten Interesses gestützt werden. Man könne in dem der Entscheidung zugrunde liegenden Fall auch keinen Rechtsmissbrauch erkennen und es sei zumindest diskussionsfähig, dass der Betroffene bei entsprechender persönlicher Einstellung in Bezug auf seine Privatsphäre tatsächlich einen Schaden erlitten habe.

Er verwies jedoch auch darauf, dass die Entscheidung in der Folge falsch verstanden und ein Geschäftsmodell entwickelt wurde, das nicht der datenschutzrechtlichen Zielsetzung entspricht. Inzwischen suche man gezielt nach Seiten, auf denen die Schriftarten nach wie vor fehlerhaft eingebunden werden, um anschließend Schadensersatzansprüche gegen die jeweiligen Unternehmen geltend zu machen. Soweit ein vermeintlich Betroffener im Rahmen seiner Anfrage ausschließlich einen Schadensersatzanspruch geltend mache, ein Unterlassungsanspruch hingegen keinerlei Erwähnung finde, könne insoweit relativ sicher von einem missbräuchlichen Begehren ausgegangen werden. Auch dann, wenn der Schaden vom Betroffenen durch die gezielte Suche nach einem Verstoß provoziert worden sei und man den Verstoß gar „mit Freude festgestellt habe", bleibt aus Sicht von Herrn Dr. Meyer kein Raum für einen Schadensersatzanspruch. In diesen Fällen sei der provozierte Schaden vielmehr lediglich notwendige Voraussetzung für den Schadensersatzanspruch.

Öffentlich-rechtliche Perspektive auf Datenschutzvorfälle – Bußgeldverfahren

In dem zweiten Teil der Veranstaltung ging es um die öffentlich-rechtliche Perspektive auf Datenschutzvorfälle, wobei insbesondere auch über Bußgeldverfahren und die Rolle der Aufsichtsbehörden gesprochen wurde.

Europaweit einheitliche Sanktionierung
Dr. Daniel Wittig wies in seinem Impulsvortrag zunächst auf den hohen Bußgeldrahmen der DSGVO hin, nach dem für Datenschutzverstöße generell ein Bußgeld von bis zu 20 Mio. Euro oder 4 Prozent des weltweit erzielten Jahresumsatzes eines Unternehmens verhängt werden kann. Nachdem die Datenschutzaufsichtsbehörden nach Inkrafttreten der DSGVO am 25.05.2018 zunächst zurückhaltend mit der Verhängung von Bußgeldern waren, ist mittlerweile ein Anstieg der Häufigkeit und Höhe der Sanktionen zu verzeichnen.

Zur Berechnung der Bußgelder enthält die DSGVO keine klare Vorgabe. Sie sollen gem. Art. 83 Abs. 1 DSGVO allerdings „wirksam, verhältnismäßig und abschreckend" sein. Um die Transparenz bei der Bemessung von Bußgeldern zu erhöhen und ein einheitliches Vorgehen der verschiedenen Aufsichtsbehörden sicherzustellen, hat die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, im Oktober 2019 ein Konzept zur Bußgeldbemessung in Verfahren gegen Unternehmen veröffentlicht, das auf Sachverhalte innerhalb von Deutschland anwendbar war. Das Konzept der DSK wird nun abgelöst durch die neuen Leitlinien zur Berechnung von Bußgeldern unter der DSGVO, die der Europäische Datenschutzausschuss (EDSA), ein Zusammenschluss aus Vertretern der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten, am 12.05.2022 veröffentlicht hat. Die Leitlinien sollen die Berechnung von Bußgeldern europaweit harmonisieren, da sie auch auf grenzüberschreitende Fälle in der Europäischen Union anwendbar sind. Ähnlich wie nach dem Konzept der DSK wird die Höhe eines Bußgeldes nach den neuen Leitlinien in fünf Schritten ermittelt, die Herr Dr. Wittig in seinem Vortrag erläuterte. Einzelheiten zu der Bußgeldberechnung nach den Leitlinien des EDSA haben wir in dem Schwerpunktthema unseres Datenschutz-Newsletters im September 2022 ausführlich dargestellt.

Herr Dr. Wittig betonte in seinem Vortrag, dass die neuen Leitlinien durchaus mit Problemen behaftet seien. So sei es problematisch, dass der Umsatz eines Unternehmens prägend für die Bußgeldhöhe sei, obwohl die DSGVO selbst nur auf tatbezogene Kriterien und gerade nicht auf den Umsatz abstelle und der EuGH für das Kartellrecht bereits festgestellt habe, dass dem Umsatz keine übermäßige Bedeutung bei der Sanktionsbestimmung zugemessen werden dürfe. Es sei außerdem keine Milderung für einen Erstverstoß vorgesehen und bei der Einordnung in Schweregrade und der Festlegung von Strafenkatalogen bestehe weiterhin ein großer Ermessensspielraum der Behörden.

Als Fazit hielt Herr Dr. Wittig fest, dass die Leitlinien zwar einen wichtigen Baustein zur einheitlichen Anwendung der DSGVO darstellen und mehr Flexibilität als das Konzept der DSK ermöglichen, jedoch kein Bußgeldrechner sind. Eine Bewertung und Überarbeitung der Leitlinien ist auch durch den EDSA selbst vorgesehen.

Rolle und Position der Datenschutzaufsichtsbehörden
Die sich an den Impulsvortrag anschließende Podiumsdiskussion begann mit einem Gespräch über die Rolle und Position der Datenschutzaufsichtsbehörden. Herr Dr. Worms stellte hierzu die verschiedenen Aufgaben und Befugnisse der Behörden aus der DSGVO dar. Er wies etwa darauf hin, dass die Behörden Datenschutzverstöße aufnehmen, indem ihr gegenüber bestimmte Meldepflichten erfüllt werden. Daneben hätten sie eine Aufklärungs- und Beratungsfunktion und würden darauf hinwirken, dass Verstöße bei den verantwortlichen Unternehmen abgestellt werden. Sie hätten die Möglichkeit, Bescheide und Beschlüsse gegenüber verantwortlichen Stellen, mithin Verwaltungsakte, zu erlassen, gegen die sich Verantwortliche vor den Verwaltungsgerichten zur Wehr setzen könnten. Letztlich seien die Aufsichtsbehörden aber auch zuständig für die Ahndung von Verstößen durch die Verhängung von Bußgeldern. Nach der Wahrnehmung von Herrn Dr. Worms würden die

Aufsichtsbehörden diesbezüglich zumeist mit Augenmaß agieren, wobei jedoch Unterschiede zwischen den einzelnen Behörden festzustellen seien.

Missbräuchliche Geltendmachung von Betroffenenrechten
Auch im Hinblick auf die öffentlich-rechtliche Perspektive auf Datenschutzvorfälle im zweiten Teil der Veranstaltung kamen die Teilnehmer auf die missbräuchliche Geltendmachung von Betroffenenrechten zu sprechen. Zu der Frage, wann Betroffenenrechte rechtsmissbräuchlich geltend gemacht würden, wies Herr Dr. Worms darauf hin, dass es diesbezüglich Unterschiede in der Rechtsprechung gebe. Während der Einwand des Rechtsmissbrauchs in der arbeitsgerichtlichen Rechtsprechung eher zurückgewiesen werde, hätten einige Zivilgerichte bereits Fälle des Rechtsmissbrauchs bejaht. Aus dem verwaltungsgerichtlichen Bereich gebe es insofern noch keine Rechtsprechung.

Für das Informationsfreiheitsrecht, einen ähnlichen Bereich, wies Herr Dr. Worms darauf hin, dass mittlerweile bereits vor dem Bundesverwaltungsgericht abschließend geklärt sei, dass der Einwand des Rechtsmissbrauchs nur in besonderen Ausnahmefällen bei völlig zu missbilligenden, evidenten Motiven erhoben werden könne. Insofern erläuterte er, dass der Bereich des datenschutzrechtlichen Auskunftsrechts ebenso unabhängig von Motiven und Zwecken sei und dass nach den bisherigen Hinweisen der Verwaltungsgerichte diese ähnlicher Ansicht seien und einen Rechtsmissbrauch ebenfalls grundsätzlich verneinen würden.

Herr Dr. Rempe wandte ein, dass der Einwand des Rechtsmissbrauchs aus dem Übermaßverbot und dem Verhältnismäßigkeitsgrundsatz im Europarecht hergeleitet werde und dass der Zweck des Auskunftsrechts nach den Erwägungsgründen der DSGVO gerade sei, festzustellen, ob jemand in seinen Persönlichkeitsrechten betroffen sei.

Herr Dr. Meyer äußerte hierzu nochmals, dass das Auskunftsrecht den Betroffenen in die Lage versetzen solle, über die Rechtmäßigkeit der Verarbeitung seiner personenbezogenen Daten zu entscheiden. Eine rechtsmissbräuchliche Geltendmachung des Auskunftsrechts sei nach seiner Ansicht daher möglich. In der Praxis sei es die Aufgabe der verantwortlichen Stelle, den Rechtsmissbrauch nachzuweisen. Bei dem Sammeln von Indizien helfe auch ein Austausch mit anderen Verantwortlichen, um herauszufinden, ob diese von derselben Auskunftsanfrage betroffen sind. Aus der Sicht von Herrn Dr. Meyer sei es jedoch wünschenswert, dass auch die Aufsichtsbehörden Anfragen, die evident querulatorisch seien, deutlicher zurückweisen. Grundsätzlich sei es aber zu begrüßen, dass von den Behörden jede Anfrage eines Bürgers zunächst ernst genommen werde und losgelöst von den Motiven über sie entschieden werde.

Herr Möller berichtete, dass viele Anfragen, die die Verbraucherzentrale erreichen, darin begründet seien, dass für die Verbraucher unklar sei, woher ein Unternehmen ihre Daten erhalten habe, wie ihre Daten verarbeitet würden und an wen die Daten weitergegeben würden. Er äußerte deshalb Vorsicht bei der vorschnellen Annahme eines Rechtsmissbrauchs, ein solcher sei in der Regel nicht gegeben. Dies folge aus der zentralen Rolle des Auskunftsanspruchs in der DSGVO, der die Geltendmachung von weiteren Rechten häufig erst ermögliche.

Vorgehen bei Datenschutzvorfällen
Ein weiteres Thema der Diskussion war, wie verantwortliche Stellen idealerweise bei einem Datenschutzvorfall vorgehen sollten. Herr Dr. Worms empfahl Verantwortlichen insofern zunächst, die Frist für die Meldung eines Datenschutzvorfalls bei der Aufsichtsbehörde zu beachten, die gem. Art. 33 Abs. 1 DSGVO innerhalb von 72 Stunden ab Kenntnis des Vorfalls zu erfolgen hat. Kenntnis meine in diesem Zusammenhang nicht, dass der Vorfall bereits abschließend untersucht sein müsse, sondern es werde auf den Zeitpunkt abgestellt, ab dem die Möglichkeit bestehe, dass es zu Persönlichkeitsrechtsverletzungen gekommen sei. Die Frist könne auch über ein Wochenende ablaufen. Wichtig sei für Unternehmen insofern auch, die eigene Rolle zu klären. Um herauszufinden, wen die Meldeverpflichtung treffe, müsse vor allem geklärt werden, ob das Unternehmen allein oder mit einem anderen Unternehmen gemeinsam für die Datenverarbeitung verantwortlich oder Auftragsverarbeiter sei.

Herr Dr. Meyer wies darauf hin, dass es zur Einhaltung der knappen Meldefrist zwingend erforderlich sei, ein Konzept für das Vorgehen bei Datenschutzvorfällen zu erstellen, um beispielsweise interne Informationsketten vorab festzulegen. Zu beachten sei außerdem, dass nicht jeder Datenschutzverstoß meldepflichtig sei, sondern dass sich die Meldepflicht nach dem Vorliegen eines Risikos beziehungsweise, bei der Benachrichtigungspflicht gegenüber Betroffenen, eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen richte. Hierbei seien die Eintrittswahrscheinlichkeit und die möglichen Auswirkungen für die Betroffenen zu berücksichtigen. Die Einschätzung ist insofern aufgrund einer Prognose abzugeben. Herr Dr. Worms wies hierzu darauf hin, dass eine einst vertretbare Prognose, die sich im Nachhinein jedoch als unzutreffend herausstelle, nicht zwingend einen Datenschutzverstoß bedeute.

Herr Dr. Meyer ergänzte, dass es in den Meldeportalen der Aufsichtsbehörden die Funktion gebe, einen Vorfall, der lediglich zu einem geringen Risiko führe und daher nicht meldepflichtig sei, zu speichern und zu dokumentieren. Falls der Vorfall zu einem späteren Zeitpunkt zu einer anderen Risikobewertung und damit zu einer Meldepflicht führe, könne das Dokument als Nachweis dienen, dass vorher eine andere Bewertung hinsichtlich der Schwere des Verstoßes vorgenommen wurde.

Bei der Meldung von Datenschutzvorfällen sei außerdem zu berücksichtigen, dass bei den Behörden eine große Anzahl an Meldungen eingehe und die dortigen Mitarbeiter in der Regel wenig Zeit für die Bearbeitung hätten. Für die Praxis empfahl Herr Dr. Meyer daher, der Aufsichtsbehörde möglichst alle relevanten Informationen direkt zuzusenden, sofern dies innerhalb der Frist möglich sei. Von der Möglichkeit der vorläufigen Meldung und der anschließenden Nachreichung von Informationen sollte nur dann Gebrauch gemacht werden, wenn die Meldefrist ansonsten nicht eingehalten werden könne.

Herr Dr. Meyer wies darauf hin, dass auch die Einbeziehung der Aufsichtsbehörde in die Frage, ob ein Verstoß meldepflichtig sei, eine mögliche Vorgehensweise darstelle. In diesem Fall solle die verantwortliche Stelle jedoch bereit sein, die am Ende vorgeschlagenen Maßnahmen der Aufsichtsbehörde auch umzusetzen.

Zusammenarbeit der Verbraucherzentrale mit den Aufsichtsbehörden
Herr Möller berichtete in diesem Zusammenhang über die Zusammenarbeit der Verbraucherzentrale mit den Aufsichtsbehörden. Es erfolge insofern etwa regelmäßig eine Abstimmung mit der Datenschutzaufsichtsbehörde in Nordrhein-Westfalen. Herr Möller begrüßte, dass die Aufsichtsbehörden mittlerweile mit eigenen Positionen an die Öffentlichkeit treten, da die Stellungnahmen und Beschlüsse auch für die Verbraucherzentrale relevant seien. Es sei jedoch wünschenswert, dass diese Rechtspositionen auch gegenüber Unternehmen stärker durchgesetzt werden. Dies könne bei-

spielsweise durch Verwaltungsakte sowie durch eine etwaige gerichtliche Bestätigung dieser geschehen, was erheblich zur Rechtssicherheit beitragen würde.

Vollstreckungspraxis der Aufsichtsbehörden
Im Zusammenhang mit der Durchsetzung der Positionen der Aufsichtsbehörden wurde die Diskussion auf die Vollstreckungspraxis der Aufsichtsbehörden gelenkt. Herr Dr. Meyer wies insofern darauf hin, dass bisher eher die drohenden Bußgelder als Anreiz gesehen wurden, Anordnungen der Aufsichtsbehörden umzusetzen.

Nach Ansicht von Herrn Dr. Worms sei der Grund dafür ein vollstreckungsrechtliches Problem, da zwar eigentlich das allgemeine Vollstreckungsrecht zur Verfügung stehe, die Bescheide aber nicht aus sich heraus vollziehbar seien. Bei einer Verwaltungsvollstreckung sei vorliegend nur ein Zwangsgeld als Maßnahme denkbar, das jedoch im Vergleich zu einem Bußgeld geringer bemessen und daher weniger wirksam, wenn auch mit anderer Zweckrichtung, sei.

Herr Dr. Meyer sah es als Schwachpunkt, dass einerseits die Aufsichtsbehörden zu Beratungszwecken hinzugezogen werden können und andererseits Bußgeldverfahren möglich seien, jedoch die Mitte zwischen diesen beiden Möglichkeiten noch ausgefüllt werden müsse. Es sei wünschenswert, Themen auch unabhängig von Sanktionen einer Klärung zuzuführen.

Vorgehen von verantwortlichen Stellen hinsichtlich möglicher Sanktionen
Um sich gegen Sanktionen zu wehren, empfahl Herr Dr. Worms, bereits vor dem Erlass des Bußgeldbescheids die Möglichkeit der Anhörung wahrzunehmen, um die eigene Position einzubringen. Gegen einen Bescheid könne eine verantwortliche Stelle gerichtlich vorgehen, wobei bis zu einer Entscheidung in zweiter oder dritter Instanz mit einem gewissen Zeitaufwand zu rechnen sei.

Hinsichtlich der Verhängung von Sanktionen wies Herr Dr. Meyer darauf hin, dass es aufgrund des hohen Bußgeldrahmens für Unternehmen schwierig sei, Bußgelder einzukalkulieren und sie bei dem eigenen Handeln „in Kauf zu nehmen“. Wenn auch die neuen Leitlinien des EDSA zu einer Verbesserung der Bußgeldberechnung geführt hätten, gebe es doch regelmäßig Zweifel an der Verhältnismäßigkeit der Bußgelder, was auf die Schwachpunkte des Bußgeldkonzepts, insbesondere auf die große Bedeutung der Umsätze eines Unternehmens, zurückzuführen sei. Es sei insofern abzuwarten, wie die Gerichte über Bußgelder entscheiden werden, die zukünftig anhand der neuen Leitlinien berechnet werden. Zumindest bisher seien die Aufsichtsbehörden nicht oder zumindest nicht überwiegend erfolgreich in der gerichtlichen Verteidigung ihrer Bußgelder gewesen.

Fazit

Auf unserem Datenschutzrechtstag haben die Teilnehmer der Veranstaltung zu verschiedenen datenschutzrechtlichen Fragestellungen rund um das Thema „Datenschutzvorfälle – Beteiligte, Konsequenzen und Absicherung –“ Stellung bezogen und dabei deutlich gemacht, dass einerseits verantwortliche Stellen durch geeignete Maßnahmen die Risiken eines Vorfalls minimieren sowie die Abläufe für den Ernstfall im Vorfeld optimieren können und dass andererseits durch die Leitlinien des EDSA zur Bußgeldbemessung und verschiedene Stellungnahmen der Aufsichtsbehörden teilweise bereits mehr Rechtssicherheit im Hinblick auf mögliche Sanktionierungen geschaffen werden konnte. Für einige Themen bleibt dagegen jedoch eine zukünftige Klärung abzuwarten. Dies betrifft insbesondere die Überarbeitung beziehungsweise gerichtliche Überprüfung der Bußgeldberechnung sowie die stärkere Positionierung und Durchsetzung dieser Positionen durch die Aufsichtsbehörden.

Christina Prowald/Johanna Schmale

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 890
F +49 521 96535 - 113
M christina.prowald@brandi.net

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