BRANDI-DATENSCHUTZRECHTSTAG ZUM THEMA „DATENSCHUTZ IN DER CLOUD UND CYBERSICHERHEIT“

English version

Einleitung

Am 12. Mai 2023 war Herr Prof. Dr. Alexander Roßnagel, hessischer Beauftragter für Datenschutz und Informationsfreiheit (HBDI), zu Gast bei BRANDI in Bielefeld. Zuvor war er als Seniorprofessor für Öffentliches Recht, mit dem Schwerpunkt Recht der Technik und des Umweltschutzes, an der Universität Kassel tätig. Im Rahmen des diesjährigen Datenschutzrechtstags zum Thema „Datenschutz in der Cloud und Cybersicherheit“ gab er im Gespräch mit Rechtsanwältinnen und Rechtsanwälten von BRANDI, darunter Dr. Sebastian Meyer, Dr. Christoph Rempe, Dr. Laura Schulte, Dr. Christoph Worms und Dr. Daniel Wittig, einen spannenden Einblick in verschiedene datenschutzrechtliche Themen, aktuelle Verfahren und die tägliche Arbeit der Hessischen Datenschutzaufsichtsbehörde sowie der Datenschutzkonferenz (DSK).

Im Rahmen der Veranstaltung wurden Fragestellungen rund um die Nutzung von Cloud-Diensten sowie Cybersicherheit beleuchtet. Im ersten Teil diskutierten die Teilnehmer unter anderem über rechtliche Vor- und Nachteile von On-Premise-Lösungen und cloudbasierten Anwendungen, den Einsatz von Microsoft 365 sowie Aspekte der Vertragsverhandlungen mit den Anbietern von Cloud-Lösungen und die Absicherung von Drittstaatentransfers, darunter die Konsequenzen der Schrems-II-Rechtsprechung und den aktuellen Stand des neuen Angemessenheitsbeschlusses für die USA. Zum Einstieg referierte Herr Prof. Roßnagel zum Thema „Datenschutz in der Cloud“. Im zweiten Teil wurden im Anschluss an den Impulsvortrag „Haftungsrisiko Cybervorfälle“ von Frau Dr. Schulte die rechtliche Absicherung von Cybervorfällen, versicherungsrechtliche sowie strafrechtliche Aspekte und verschiedene Strategien zum Umgang mit Cybervorfällen thematisiert. Im dritten Teil der Veranstaltung referierten angehende Juristen im Rahmen des BRANDI-Nachwuchspreises zu verschiedenen aktuellen datenschutzrechtlichen Themen.

Einsatz von Cloud-Lösungen

Der erste Teil der Veranstaltung widmete sich vor allem der Nutzung von Cloud-Diensten und den in diesem Kontext relevanten datenschutzrechtlichen Fragestellungen und Anforderungen.

Impulsvortrag: Datenschutz in der Cloud

Herr Prof. Roßnagel wies in seinem Impulsvortrag zunächst darauf hin, dass die meisten Cloud-Anbieter nicht aus Deutschland bzw. der EU stammten und erläuterte, was es bedeute, Cloud-Computing als Auftragsverarbeitung zu verstehen. Dabei ging er auf das grundlegende Konzept der Auftragsverarbeitung sowie die sich aus Art. 28 DSGVO ergebenden Anforderungen ein. Gleichzeitig machte er deutlich, dass das Machtverhältnis zwischen Auftraggeber und Auftragnehmer in der Praxis im Falle des Cloud-Computings in der Regel gerade umgekehrt sei, weshalb es mitunter schwierig sei, die von der DSGVO vorgesehenen Erfordernisse einzuhalten und umzusetzen. Beispielhaft führte er insoweit Microsoft 365 an und ging auf die datenschutzrechtlichen Schwachstellen der seitens Microsoft zur Verfügung gestellten Vereinbarung zur Auftragsverarbeitung sowie die mangelnde Verhandlungsbereitschaft von Microsoft ein. In diesem Kontext wies er auch darauf hin, dass Cloud-Computing in der Regel mit einem internationalen Datentransfer verbunden sei und deshalb entsprechende Absicherungsmaßnahmen ergriffen werden müssten. Dabei ging er auf die Anforderungen ein, die der EuGH in seinen Schrems-Entscheidungen entwickelt hat, und berichtete über den aktuellen Stand des neuen Angemessenheitsbeschlusses der Europäischen Kommission für Datenübermittlungen in die USA („Trans-Atlantic Data Privacy Framework“). Er verwies hierbei insbesondere auf verschiedene Kritikpunkte, wie die weiterhin bestehenden Zugriffsmöglichkeiten der US-Behörden sowie die unzureichenden Beschwerdemechanismen, die auch bereits vom EDSA und vom LIBE-Ausschuss des Europäischen Parlaments formuliert wurden. Mit einem Inkrafttreten des Angemessenheitsbeschlusses sei – sofern die weiteren Verfahrensschritte erfolgreich durchlaufen werden – zudem nicht vor Ende diesen Jahres zu rechnen und es sei wahrscheinlich, dass dieser sodann zügig klageweise angegriffen werde. Abschließend wies Herr Prof. Roßnagel darauf hin, dass man sich von den zuvor dargestellten Streitigkeiten möglichst unabhängig machen sollte und sich deshalb langfristig an dem Ziel, weitestgehend digitale Souveränität zu erreichen, orientieren müsse. Außerdem berichtete er über das kürzlich entwickelte Positionspapier der DSK, innerhalb dessen Kriterien aufgezeigt werden, anhand derer künftig beurteilt werden soll, inwieweit ein souveränes Cloud-Angebot vorliegt.

Cloudbasierte Anwendungen und On-Premise-Lösungen

Die sich an den Impulsvortrag anschließende Podiumsdiskussion begann mit einem Gespräch über die rechtlichen Vor- und Nachteile von cloudbasierten Anwendungen einerseits und On-Premise-Lösungen andererseits. Herr Dr. Meyer erläuterte zunächst, dass es sich bei On-Premise-Lösungen um Softwareanwendungen handele, die auf den eigenen Systemen eines Unternehmens und souverän gesteuert und betrieben werden könnten. Dies bedeute jedoch auch, dass das jeweilige Unternehmen die Sicherheit seiner Systeme gewährleisten müsse. Demgegenüber sei bei Cloud-Diensten auch mit Blick auf die rechtliche Bewertung zwischen verschiedenen Varianten zu differenzieren. Während eine Private Cloud etwa

nur für einen bestimmten Nutzer betrieben werde, würden andere Systeme (Public Cloud) für eine Vielzahl an Nutzern bereitgestellt. Cloud-Dienste würden zudem häufig als SaaS-Dienste angeboten. Dies habe den Vorteil, dass der jeweilige Anbieter sich um die Betreuung des Systems und dementsprechend auch um sicherheitsrelevante Aspekte und die Aktualität der Systeme kümmere. Hierauf, sowie auf die Vorteilhaftigkeit eines professionellen Sicherheitsmanagements, wies auch Herr Prof. Roßnagel bereits in seinem Vortrag hin. Problematisch sei demgegenüber, dass viele Anbieter – auch solche, die mit einer inländischen Dienstleistung werben – mitunter Drittstaaten-Subunternehmer einsetzten, wodurch komplexe Verarbeitungsketten sowie eine größere Abhängigkeit von dem jeweiligen Dienstleister entstünden. Gleichzeitig wies Herr Dr. Meyer hierbei auch auf die Expertise eines spezialisierten Dienstleisters hin, die wiederum als durchaus vorteilhaft zu bewerten sein könne.

Anschließend wurde auf die Frage eingegangen, inwieweit souveräne Cloud-Modelle auch auf die Bedürfnisse von Unternehmen zugeschnitten seien. Dabei wurde erläutert, dass entsprechende Modelle auch im privaten Bereich sinnvoll Anwendung finden könnten. Im Bereich von Videokonferenzdiensten könne etwa auf Open-Source-Lösungen (z.B. Big Blue Button) zurückgegriffen oder Modelle genutzt werden, bei denen ein Dienstleister zwischengeschaltet werde, der etwa einen Dienst wie Zoom auf seinen eigenen (innereuropäischen) Servern betreibt und den Zugriff des Dienstes auf die Daten kontrolliert. Außerdem gäbe es derzeit Bestrebungen großer Anbieter wie Microsoft oder Google, gemeinsam mit europäischen Anbietern, alternative Anwendungen zur Verfügung zu stellen, die den datenschutzrechtlichen Anforderungen an eine souveräne Cloud gerecht werden sollen. Künftig könne die Auswahl datenschutzkonformer und souveräner Cloud-Lösungen zudem durch entsprechende Zertifizierungen erleichtert werden. Entsprechende Möglichkeiten würden derzeit erarbeitet.

Relevante Aspekte beim Einsatz von Cloud-Lösungen
Herr Dr. Rempe erläuterte im weiteren Verlauf der Diskussion, welche Aspekte in Bezug auf den datenschutzkonformen Einsatz von Cloud-Lösungen und im Rahmen der Verhandlungen mit dem jeweiligen Anbieter besonders relevant sind. Dabei ging er unter anderem auf den Punkt ein, dass es unter datenschutzrechtlichen sowie unter haftungsrechtlichen Gesichtspunkten durchaus empfehlenswert sei, einen Dienstleister zwischenzuschalten. Zudem sollten Unternehmen die jeweiligen Vertrags- und Nutzungsbedingungen sowie die datenschutzrechtlichen Vereinbarungen in jedem Fall prüfen, kritisch hinterfragen und auf die Einbeziehung von (zusätzlichen) Maßnahmen zur Absicherung achten. Insbesondere sollte in diesem Kontext auch darauf geachtet werden, welche Subunternehmer vom jeweiligen Anbieter eingesetzt würden, da auch viele europäische Dienstleister auf Subdienstleister aus Drittstaaten zurückgriffen. Außerdem sollten Unternehmen von ihren vereinbarten Rechten, wie etwa Kontrollmöglichkeiten, Gebrauch machen und bei Bedarf durchaus auch Überprüfungen vornehmen.

Nutzung von Microsoft 365
Im weiteren Verlauf der Diskussion wurde hinsichtlich der Nutzung von Microsoft 365 erläutert, dass die DSK in der Vergangenheit verschiedene datenschutzrechtlich problematische Punkte herausgearbeitet und aufgezeigt habe. Diese seien sodann in zahlreichen Gesprächen mit Microsoft erörtert worden. Die Anpassungen, die Microsoft anschließend in seiner Vereinbarung zur Auftragsverarbeitung vorgenommen hat, hätten jedoch keine wesentlichen datenschutzrechtlichen Verbesserungen gebracht. Auch unter Verwendung des zuletzt erarbeiteten Ergänzungspapiers sei es nicht möglich, die Vorgaben der DSGVO einzuhalten, sodass ein datenschutzkonformer Einsatz nicht möglich sei. Besonders kritisch sei insoweit, dass Microsoft die Daten der Nutzer zu eigenen Zwecken verwenden dürfe, ohne dass klar sei, welche dies seien und was konkret mit den Daten passiere.

Weiter berichtete Herr Prof. Roßnagel, dass derzeit keine systematischen Überprüfungen hinsichtlich des Einsatzes geplant seien, sondern man Unternehmen beim datenschutzkonformen Einsatz von Cloud-Diensten unterstützen wolle. Dies bedeute jedoch nicht, dass verantwortliche Unternehmen nicht mit einer Prüfung im Einzelfall konfrontiert werden könnten. Eine solche müsse etwa dann vorgenommen werden, wenn Bürger Beschwerde bei einer der Datenschutzaufsichtsbehörden einreichten. In entsprechenden Fällen könnten gegebenenfalls auch Sanktionen verhängt werden, soweit Unternehmen auf das Vorbringen der Behörden nicht eingingen.

Neuer Angemessenheitsbeschluss für die USA
Nach Einschätzung von Herrn Dr. Meyer wird der neue Angemessenheitsbeschluss, zumindest aus technischer Sicht, nicht zu mehr Rechtssicherheit führen, da die Datenübermittlungen nicht unmittelbar sicherer werden. Aus der risikobasierten Perspektive stelle sich die Frage, inwieweit der neue Beschluss belastbar sei oder erneut von der Rechtsprechung für unwirksam erklärt werde. Herr Dr. Meyer vermutet insoweit, dass der EuGH sich erneut auf die mangelnde Angemessenheit des Datenschutzniveaus in den USA berufen und auf seine vorherigen Entscheidungen verweisen wird. Man werde sich zudem die Frage stellen müssen, inwieweit man sich überhaupt auf einen solchen Angemessenheitsbeschluss verlassen darf, wenn dieser bereits mehrfach für unwirksam erklärt und grundlegende Probleme nicht gelöst wurden. Es ergebe sich außerdem die Frage, welche Relevanz ein neuer Angemessenheitsbeschluss überhaupt habe. Er mache Datenübermittlungen in die USA zwar einfacher. Gleichwohl würde derzeit – ohne Angemessenheitsbeschluss – in vielen Fällen jedoch auch nicht auf den Einsatz von amerikanischen Dienstleistern verzichtet. Man versuche entsprechende Datenübermittlungen vielmehr unter Einbeziehung von Standardvertragsklauseln und zusätzlichen Maßnahmen abzusichern. Künftig sei insoweit ein doppelter Ansatz denkbar, um sich für den Fall abzusichern, dass der neue Angemessenheitsbeschluss ebenfalls keinen Bestand hat.

Mit Blick auf den Einsatz von Microsoft 365 empfahl Herr Dr. Meyer auch unter Berücksichtigung des Umstands, dass der neue Angemessenheitsbeschluss vermutlich keinen echten Durchbruch bedeuten wird, von den Optionen und Konfigurationsmöglichkeiten, die derzeit von Microsoft angeboten werden, Gebrauch zu machen und sich hierdurch, soweit derzeit möglich, abzusichern. Es biete sich an im Vorfeld der Nutzung entsprechender Produkte eine umfassende Risikoabwägung für den konkreten Fall und unter Berücksichtigung der möglichen Alternativen vorzunehmen und diese zu dokumentieren.

Cybervorfälle

In dem zweiten Teil der Veranstaltung ging es um Fragestellungen rund um Cybervorfälle – Verantwortlichkeit und Haftung, rechtliche Absicherung, versicherungsrechtliche und strafrechtliche Aspekte sowie Strategien zum Umgang mit Cybervorfällen.

Impulsvortrag: Haftungsrisiko Cybervorfälle
Frau Dr. Schulte stellte in ihrem Vortrag zunächst die relevanten Gefahren im Bereich Cybersicherheit vor und ging dabei insbesondere auf die Bedrohung durch Ransomware ein. Hierbei handelt es sich um Angriffe, bei denen die Daten des Unternehmens von den Angreifern mittels eines Schadprogramms verschlüsselt und gegen Zahlung eines Lösegelds wieder entschlüsselt werden. Sie verwies darauf, dass sowohl die Anzahl der Angriffe als auch die Höhe des

geforderten Lösegelds stetig zunähmen. Daneben könnten die Angriffe mitunter aber auch zu Betriebsunterbrechungen, dem Verlust von Geschäftsgeheimnissen, einem Reputationsverlust sowie Bußgeldern führen. Anschließend wies sie auf verschiedene, in diesem Kontext relevante Vorschriften hin, mittels derer Unternehmen zur IT-Sicherheit verpflichtet und Cybervorfälle verhindert werden sollen. Diese ergäben sich vor allem aus dem Datenschutzrecht sowie unmittelbar aus dem IT-Sicherheitsrecht, aber auch aus dem allgemeinen Zivilrecht oder vertraglichen Vereinbarungen. Sie machte dabei deutlich, dass die rechtlichen Verpflichtungen nicht nur von der Geschäftsleitung eines Unternehmens oder dem IT-Sicherheitsbeauftragten, sondern auch von den einzelnen Mitarbeitern einzuhalten seien. Gleiches gelte für Dienstleister, die von Unternehmen eingesetzt würden. Als Ausblick verwies Frau Dr. Schulte auf die Regelungen der NIS II-Richtlinie, die künftig von Unternehmen aus bestimmten Sektoren – etwa im Gesundheitsbereich und der Daseinsvorsorge – im Bereich IT-Sicherheit zu berücksichtigen sein werden. Die Richtlinie lege dabei einen gefahrenübergreifenden und risikobasierten Ansatz zu Grunde und sehe vor allem intensivierte Meldeverpflichtungen bei Cybervorfällen vergleichbar dem Datenschutzrecht vor. Zudem sehe die NIS-Richtlinie, wie auch die DSGVO, im Vergleich zu den jeweiligen Vorgängerregelungen einen deutlich erhöhten Bußgeldrahmen vor.

Strafrechtliche Relevanz

Impulse zur strafrechtlichen Perspektive wurden innerhalb der sich anschließenden Diskussion von Herrn Weber-Blank, Fachanwalt für Steuer- und Strafrecht bei BRANDI in Hannover eingebracht. Herr Weber-Blank berichtete zu Beginn über die zunehmende strafrechtliche Relevanz von IT-bezogenen Sachverhalten und die Problematik, dass dieser Bereich nach seiner Wahrnehmung von den Strafverfolgungsbehörden nicht ausreichend beherrscht werde. Er ging dabei auf das Beispiel der Fake-Shops ein und berichtete aus der Praxis, dass die Strafverfolgung mitunter sehr langwierig sei und häufig wenig erfolgreich verlaufe. Problematisch seien insoweit unter anderem die Zuständigkeit sowie fehlendes Know-How der Behörden, die Komplexität der Sachverhalte sowie die schwierige Nachverfolgbarkeit. Vor diesem Hintergrund verwies er darauf, wie wichtig es sei, die IT-Systeme des eigenen Unternehmens im Vorfeld gegen Cyberangriffe abzusichern.

Im weiteren Verlauf der Diskussion wurde zudem thematisiert, inwieweit die Zahlung des Lösegelds bei einem Ransomwareangriff auch strafrechtliche Konsequenzen haben kann. Herr Weber-Blank erläuterte, dass eine Zahlung – dem Bereich Geldwäsche vergleichbar – mitunter auch strafrechtlich relevant sein könne und empfahl, die Thematik im Bedarfsfall vorab rechtlich und insbesondere auch unter dem Aspekt der Geldwäsche zu prüfen.

Juristische Absicherungsmöglichkeiten

Herr Dr. Meyer berichtete im Anschluss darüber, inwieweit es möglich ist, sich im Bereich Cybervorfälle juristisch, etwa vertraglich, abzusichern. Dabei machte er eingangs deutlich, dass man von einer solchen juristischen Absicherung nicht zu viel erwarten dürfe, da sie in der Regel keine echte Absicherung gegen entsprechende Vorfälle darstelle, sondern lediglich erreicht werden könne, dass der Schaden sich nicht bei dem eigenen Unternehmen, sondern bei jemand anderem – etwa dem Dienstleister – realisiere. Hierzu sei ein gut gestalteter Vertrag erforderlich, der zum einen Verantwortlichkeiten des jeweiligen Dienstleisters in Bezug auf die IT-Sicherheit konkret benennt und zum anderen Fragen zum Haftungsrahmen und zur Versicherung im Interesse des Unternehmens regelt. Unter Berücksichtigung dieser Problematik wurde auch darauf hingewiesen, dass der Fokus insoweit verstärkt auf präventive Maßnahmen gelegt werden sollte.

Auch Herr Prof. Roßnagel bekräftigte, wie wichtig das Ergreifen präventiver Absicherungsmaßnahmen sei. Er wies zudem auf das generelle Problem hin, dass die IT-Systeme bei einem Cybervorfall – konkret einem Ransomwareangriff – regelmäßig von einer Schadsoftware befallen sind und diese Problematik unabhängig von einer juristischen Absicherung oder der Zahlung eines Lösegelds fortbestehe. Die insoweit einzige Lösung sei es, die Systeme neu aufzusetzen.

Neben der Frage, inwieweit Haftungsfragen auf einen Dienstleister verlagert werden können, wurde im Rahmen der Diskussion weiter auf das Thema Geschäftsführerhaftung eingegangen. Eben jene könne sich sowohl strafrechtlich als auch zivilrechtlich auswirken. Es reiche von Seiten der Geschäftsführung insofern nicht aus, einmalig einen IT-Sicherheitsbeauftragten zu benennen. Die Geschäftsführung müsse sich vielmehr kontinuierlich mit dem Thema auseinandersetzen und die Prozesse im Blick behalten. Parallelen könnten an dieser Stelle auch zum VW-Abgasskandal gezogen werden, im Rahmen dessen auch die Geschäftsführung in Bezug auf Haftungsfragen verstärkt in den Fokus gerückt wurde.

Cyberversicherungen

Im weiteren Verlauf der Diskussion stellte sich zudem die Frage nach den Vorteilen einer Cyberversicherung und den bei deren Abschluss zu berücksichtigenden Aspekten. Unabhängig von den konkreten Versicherungsbedingungen sei es mitunter nicht einfach, überhaupt eine solche Versicherung zu attraktiven und tragbaren Konditionen zu bekommen. Die Anforderungen der Versicherungen seien insoweit sehr hoch und Unternehmen müssten häufig nachweisen, dass sie aus IT-rechtlicher Sicht gut aufgestellt seien. Sinnvoll sei es deshalb, vorbereitet zu sein und vorab etwa die eigenen Absicherungsmaßnahmen aufzulisten und einen Notfallplan zu erstellen. Was schließlich ein attraktives Produkt sei, richte sich nach den jeweiligen Bedürfnissen des Unternehmens im Einzelfall. Herr Dr. Meyer wies ebenfalls darauf hin, dass zwei Aspekte im Rahmen des Abschlusses einer Cyberversicherung besonders relevant seien – zum einen der spätere Versicherungsschutz an sich, zum anderen aber insbesondere auch die vorherige Auseinandersetzung mit der eigenen IT-Infrastruktur und den bereits getroffenen oder noch erforderlichen Absicherungsmaßnahmen.

Cyber-Kompetenz-Zentren

Herr Prof. Roßnagel wies noch darauf hin, dass es in Hessen ein Cyber-Kompetenz-Zentrum gebe, an das sich Unternehmen im Falle eines Cyberangriffs wenden könnten. Dieses würde sodann beratend tätig und könnte auch Kontakte zu IT-Spezialisten herstellen. Herr Dr. Meyer merkte an, dass es entsprechende Zentren auch in anderen Bundesländern gebe, machte jedoch gleichzeitig darauf aufmerksam, dass entsprechende Einrichtungen aber natürlich nur während ihrer Öffnungszeiten behilflich sein könnten. Komme es etwa am Freitagnachmittag oder am Wochenende zu einem Vorfall, könne auf solche Hilfsangebote in der Regel nicht zurückgegriffen werden. Weiter machte Herr Dr. Meyer in diesem Rahmen deutlich, wie wichtig der Zeitfaktor bei Cyberangriffen sei und es deshalb wichtig sei, auf entsprechende Vorfälle vorbereitet zu sein. Hierzu sei es hilfreich, Notfallpläne und Abläufe im Vorfeld zu üben.

Meldepflichten und Bußgelder

Im Rahmen der Diskussion wurde weiter darauf hingewiesen, dass bei Cybervorfällen gegebenenfalls auch die datenschutzrechtlichen Meldepflichten aus Art. 33 und 34 DSGVO zu berücksichtigen seien. Neben den in der DSGVO vorgesehenen Pflichten gebe es auch weitere Meldepflichten im Bereich des IT-Sicherheitsrecht, die ebenfalls in den Blick zu nehmen seien. Weiter müsse sich zeitnah mit der Frage auseinandergesetzt werden, inwieweit eine Kunden-

information auch unabhängig von gesetzlichen Meldepflichten sinnvoll sein kann – auch um weitere Schäden zu verhindern.

Hinsichtlich der Verhängung von Bußgeldern im Kontext von Cybervorfällen machte Herr Prof. Roßnagel deutlich, dass es wichtig sei, nach Art. 33 und 34 DSGVO relevante Vorfälle rechtzeitig zu melden und Betroffene zu informieren, da ansonsten Bußgelder wegen unterlassener Meldung bzw. Information drohten. Wegen der Meldung an sich würden Unternehmen unter Berücksichtigung des nemo-tenetur-Grundsatz hingegen nicht bebußt. Allerdings bliebe es nicht aus, dass das Unternehmen durch die Meldung in Erinnerung bliebe und gegebenenfalls Sicherheitsmaßnahmen im Nachgang überprüft würden. Herr Dr. Meyer wies in diesem Rahmen auch darauf hin, dass es sinnvoll sei, einen entsprechenden Vorfall zum Anlass zu nehmen, die unternehmensseitig ergriffenen Absicherungsmaßnahmen einer generellen Prüfung zu unterziehen.

BRANDI-Nachwuchspreis

Im Rahmen des BRANDI-Nachwuchspreises wurden zum Abschluss der Veranstaltung aktuelle datenschutzrechtliche Themen im Rahmen von Kurzvorträgen von angehenden Juristen präsentiert.

Nutzer-Tracking, Cookie-Banner und Einwilligungsverwaltung

Frau Christina Prowald berichtete zunächst über den Einsatz von Tools zum Nutzer-Tracking und die datenschutzrechtlichen Anforderungen der verschiedenen Rechtsquellen sowie der Rechtsprechung, die bei der Nutzung einzuhalten sind. Wie für jede andere Datenverarbeitung sei insbesondere das Vorliegen einer belastbaren Rechtsgrundlage erforderlich. Außerdem müssten den Nutzern umfangreiche datenschutzrechtliche Informationen zur Verfügung gestellt werden, damit diese über die Verarbeitung ihrer personenbezogenen Daten in informierter Weise entscheiden und von ihren Rechten Gebrauch machen könnten. Für die Nutzung von Cookies sei geklärt, dass grundsätzlich eine aktive Nutzereinwilligung eingeholt werden müsse. Sofern andere Technologien verwendet würden, sei zu prüfen, inwieweit ebenfalls die Zustimmung des Nutzers in die jeweilige Datenverarbeitung erforderlich sei oder der Prozess gegebenenfalls auf eine andere Rechtsgrundlage gestützt werden könne. Neben einer den rechtlichen Anforderungen entsprechenden Ausgestaltung des Cookie-Banners sei außerdem darauf zu achten, dass die Nutzerentscheidung auch im Übrigen technisch korrekt umgesetzt werde. Frau Prowald ging darüber hinaus auf die neue Vorschrift des § 26 TTDSG, die Regelungen für Dienste zur Einwilligungsverwaltung enthält und der Cookie-Banner-Müdigkeit vieler Nutzer begegnen soll, sowie die geplante Einwilligungsverwaltung-Verordnung ein. Sie stellte dabei Vorteile sowie problematische Aspekte der neuen Regelungen dar und warf verschiedene datenschutzrechtliche Fragen zur Umsetzung entsprechender Dienste auf.

Umgang mit datenschutzrechtlichen Auskunftsanfragen

Im zweiten Vortrag ging Frau Johanna Schmale näher auf das Auskunftsrecht nach Art. 15 DSGVO ein. Dies stelle einen wichtigen Aspekt bei der Ausübung des Rechts auf informationelle Selbstbestimmung dar. Es sei insoweit erforderlich, dass Betroffene darüber informiert würden, in welchen Fällen eine Verarbeitung personenbezogener Daten stattfinde und welche Informationen zu der eigenen Person bei einer verantwortlichen Stelle vorlägen. Das Auskunftsrecht diene diesem Umstand sowie der erleichterten Geltendmachung weiterer Betroffenenrechte. Frau Schmale berichtete, dass sich der Umfang der Auskunftspflicht nach dem konkreten Verlangen des Betroffenen richte. Weiter erläuterte sie, dass verantwortlichen Stellen empfindliche Konsequenzen drohen können, sofern diese Auskunftsanfragen nicht oder nicht fristgerecht, spätestens innerhalb eines Monats, beantworteten. Für eine rechtskonforme Beantwortung seien deshalb ein koordiniertes und intern abgestimmtes Vorgehen empfehlenswert. Die erforderlichen Informationen seien den betroffenen Personen unentgeltlich sowie in präziser, transparenter, verständlicher und leicht zugänglicher Form zu übermitteln. Um zu verhindern, dass die personenbezogenen Daten der betroffenen Person an einen unbefugten Dritten herausgegeben würden, müsse vor Erteilung der Auskunft zudem die Identität des Anfragenden geprüft werden. Insbesondere in Zweifelsfällen sei es zudem sinnvoll, dass der Datenschutzbeauftragte das Unternehmen bei der Bearbeitung der Auskunftsanfrage unterstütze.

EuGH zum Schadensersatz aus der DSGVO

Herr Ingold berichtete zum Abschluss über das aktuelle Urteil des Europäischen Gerichtshofs (EuGH) zu den Anforderungen des Schadensersatzes aus der DSGVO. Im Ausgangsverfahren habe der Kläger einen Schadensersatzanspruch gegen die Österreichische Post AG geltend gemacht, weil diese Informationen über politische Präferenzen gesammelt, „Zielgruppenadressen“ definiert und dem Kläger eine bestimmte Parteiaffinität zugeschrieben habe. Hierdurch sei der Kläger verärgert und beschämt gewesen. Der OGH habe dem EuGH sodann im Rahmen eines Vorabentscheidungsverfahrens unter anderem die Fragen vorgelegt, ob ein bloßer Verstoß gegen die DSGVO ausreicht, um einen Schadensersatzanspruch zu begründen und ob es Voraussetzung für den Anspruch sei, dass eine Folge der Rechtsverletzung von zumindest einigem Gewicht vorliegt. Herr Ingold berichtete, dass es nach Auffassung des EuGH eines konkreten Schadens bedürfe. Begründend seien insbesondere der Wortlaut von Art. 82 DSGVO sowie verschiedener Erwägungsgründe und der systematische Vergleich mit dem Beschwerderecht sowie der Sanktionierung durch Geldbußen angeführt worden. Weiter habe der EuGH eine Erheblichkeitsschwelle verneint und sich insoweit ebenfalls auf den Wortlaut von Art. 82 DSGVO und EWG 146 sowie die einheitliche Auslegung des Schadensbegriffs bezogen. Die Kriterien zur Bestimmung des Umfangs des Schadensersatzes seien darüber hinaus durch die Mitgliedstaaten selbst festzulegen.

Fazit

Im Rahmen unseres Datenschutzrechtstags haben die Teilnehmer der Veranstaltung zu verschiedenen datenschutzrechtlichen Fragestellungen rund um das Thema „Datenschutz in der Cloud und Cybersicherheit“ Stellung genommen. Dabei wurde deutlich, dass der Einsatz von Cloud-Lösungen einerseits Vorteile für den Arbeitsalltag von Unternehmen mit sich bringt, aber andererseits auch verschiedene datenschutzrechtliche Probleme aufwirft, die einer näheren Betrachtung bedürfen. Mit Blick auf das Thema Cybervorfälle wurde deutlich, dass der Fokus neben der juristischen Absicherung durch entsprechende Verträge mit den einbezogenen Dienstleistern und Versicherungsgesellschaften insbesondere auch auf präventive Maßnahmen zur Abwehr entsprechender Angriffe gelegt werden sollte.

Christina Prowald

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