BRANDI
RECHTSANWÄLTE

BRANDI - DATENSCHUTZRECHTSTAG ZUM THEMA

„SICHERHEIT BEGINNT MIT DATENSCHUTZ“

English version

Am 24. Mai 2024 waren Herr Dr. Thilo Weichert, ehemaliger Leiter der Datenschutzaufsichtsbehörde in Schleswig-Holstein (ULD), und Prof. Dr. Eckhard Koch, Vizepräsident für Forschung, Entwicklung und Transfer an der FHDW Paderborn, zu Gast bei BRANDI. Im Rahmen des diesjährigen Datenschutzrechtstags zum Thema „Sicherheit beginnt mit Datenschutz“ gaben unsere Gäste im Gespräch mit Juristinnen und Juristen von BRANDI, darunter Dr. Sebastian Meyer, Dr. Christoph Rempe, Johanna Schmale, Dr. Carina Thull und Dr. Daniel Wittig, einen spannenden Einblick in verschiedene datenschutzrechtliche und IT-sicherheitsrechtliche Themen, aktuelle Verfahren und ihre tägliche Arbeit.

Betroffenenrechte und Konsequenzen bei Datenschutzverstößen

Der erste Teil der Veranstaltung widmete sich vor allem Fragestellungen aus dem Bereich „Betroffenenrechte und Konsequenzen bei Datenschutzverstößen“.

Herr Dr. Weichert gab in seinem Impulsvortrag dem Titel des ersten Teils entsprechend einen Überblick über die in der DSGVO vorgesehen Betroffenenrechte und Sanktionsmöglichkeiten. Dabei ging er vor allem auf die Transparenzansprüche und Handlungsmöglichkeiten der Aufsichtsbehörden ein. Er wies unter anderem auf die Wichtigkeit einer transparenten Information der von der Datenverarbeitung betroffenen Personen hin und merkte an, dass es insoweit in der Praxis häufig noch Verbesserungsbedarf gebe. Man bewege sich bei der Bereitstellung der datenschutzrechtlichen Informationen im Spannungsverhältnis zwischen den Erfordernissen einer ausführlichen Information einerseits und der leichten Verständlichkeit andererseits. Weiter führte er aus, dass das Recht auf Auskunft das zentrale Grundrecht der Betroffenen sei. Konkreter setzte er sich mit dem Anspruch auf Negativauskunft, der Zweckfreiheit und dem Umfang des Auskunftsanspruchs auseinander. Er machte außerdem deutlich, dass die Identitätsprüfung in der Praxis besonders wichtig, aber häufig schwierig sei, da es in Deutschland an funktionierenden Prüfungsverfahren fehle. Als weiteren Punkt griff Herr Dr. Weichert den Anspruch auf Schadensersatz nach Art. 82 DSGVO heraus und stellte die vom EuGH ausgearbeiteten Anforderungen dar. Mit Blick auf die Sanktionsmöglichkeiten machte er deutlich, dass nicht nur die Aufsichtsbehörden, sondern zum Beispiel auch Wettbewerber oder die Verbraucherzentrale gegen Verstöße vorgehen können. Er wies zudem darauf hin, dass eine Sanktionierung auch durch eine Warnung der Aufsichtsbehörde vor einem Unternehmen bzw. einem konkreten Dienst erfolgen könne und dies aus seiner Sicht angesichts verschiedener Schwierigkeiten bei der Verhängung und Durchsetzung von Bußgeldern in der Praxis teilweise vorzugswürdig sei.

Der ordnungsgemäße Umgang mit Auskunftsanfragen wurde sodann angesichts der hohen praktischen Relevanz im Rahmen der sich anschließenden Diskussion noch einmal aufgegriffen. Dabei wurde zunächst herausgestellt, dass die Art der Auskunftserteilung vom Grundsatz her im Ermessen des Verantwortlichen liege. Gleichwohl müssten alle Informationen, die der Betroffene verlangt habe, herausgegeben werden, es sei denn Rechte Dritter ständen der Herausgabe entgegen. Sinnvoll sei es insoweit, den Dialog mit dem Betroffenen zu suchen. Auf diese Weise sei es auch möglich, etwaige missbräuchliche Anfragen besser zu erkennen. Anschließend wurde die praktische Umsetzung der Identitätsprüfung diskutiert. Es wurde darauf hingewiesen, dass es durchaus technische Verfahren zur Überprüfung gebe, diese jedoch bislang aufgrund ihrer Komplexität wenig verbreitet oder selbst häufig nicht datenschutzkonform seien. In der Praxis sei die Vorlage des Personalausweises oder der Abgleich der Anfrage mit bereits vorhandenen Daten des Betroffenen am sinnvollsten. Bei Personen, die dem Verantwortlichen bekannt sind, sollte an deren schon hinterlegte Kontaktinformationen geantwortet. Schwierigkeiten ergäben sich vor allem dann, wenn die Anfrage keiner konkreten Person zugeordnet werden könne. In diesem Fall könne aber ggf. eine abstrakte Erklärung zur Datenverarbeitung unter dem Hinweis, dass für eine weitergehende Auskunft nähere Informationen zur Identität des Betroffenen benötigt werden, weiterhelfen. Hinsichtlich des Umfangs des Auskunftsanspruchs wurde sodann noch einmal auf den praktischen Umgang mit diesbezüglichen Einschränkungen etwa aufgrund von Geschäftsgeheimnisses oder Rechten Dritter eingegangen. Die Problematik betreffe vor allem die Herausgabe von Kommunikation wie E-Mails. Entsprechende Unterlagen seien vom Grundsatz her bei Vorliegen der sonstigen Voraussetzungen herauszugeben. Gegebenenfalls müsse eine redaktionelle Bearbeitung in Form von Schwärzungen erfolgen. Grundsätzlich empfehle sich eine strukturierte Vorhaltung von personenbezogenen Daten, um im Herausgabefall den Aufwand zu minimieren. Schließlich wurde noch darauf eingegangen, ob bzw. wie lange die Kommunikation zu eingehenden Auskunfts- oder Löschanfragen aufbewahrt werden darf. Es wurde ausgeführt, dass eine Speicherung auf Basis des berechtigten Interesses grundsätzlich zulässig sei. Man könne sich hinsichtlich der Speicherdauer regelmäßig an der klassischen Verjährungsfrist von drei Jahren orientieren. Hinsichtlich des Anspruchs auf Löschung wurde zum Abschluss der Diskussion schließlich die Wichtigkeit eines Löschkonzepts herausgestellt. Ohne ein solches

sei es kaum möglich, zu entscheiden, welche Datensätze etwa aufgrund von Aufbewahrungspflichten weiterhin aufbewahrt werden müssen und welche Datensätze im Übrigen zu welchem Zeitpunkt zu löschen sind. Die Differenzierung zwischen unterschiedlichen Aufbewahrungsfristen und die anschließende Umsetzung der Löschung könne praktisch etwa über die Nutzung unterschiedlicher Systeme oder die entsprechende Markierung der verschiedenen Datensätze erfolgen. Problematisch sei, dass viele Softwarelösungen keine ausreichenden Funktionalitäten für eine einfache systematische Löschung vorsähen, weshalb Verantwortliche sich frühzeitig um ein anderweitiges praktisches Vorgehen, etwa die manuelle Hinterlegung von Fristen, bemühen müssten.

Datenschutz und neue Technologien

Der zweite Teil der Veranstaltung befasste sich vor allem Fragestellungen aus dem Bereich Datenschutz und neue Technologien. Behandelt wurden unter anderem die richtige Gestaltung eines Cookie-Banners, die Zulässigkeit von Pur-Abo-Modellen sowie der richtige Umgang mit Künstlicher Intelligenz.

Herr Prof. Dr. Koch referierte in seinem Impulsvortrag über den Zusammenhang von Datenschutz und Cybersicherheit. Dabei stellte er zunächst verschiedene Bedrohungen im Bereich Cybersicherheit dar und ging unter anderem auf die Gefahr von Ransomware-Angriffen, bei denen Daten des Unternehmens von den Angreifern mittels eines Schadprogramms verschlüsselt und gegen Zahlung eines Lösegelds wieder entschlüsselt werden, ein. Dabei machte er deutlich, wie wichtig eine gute Aufstellung von Unternehmen im Bereich Cybersicherheit angesichts von deutlich zunehmenden Angriffszahlen und Schadenshöhen sowie der rasanten Entwicklung neuer Schadprogramm sei. Anschließend zeigte er die historische Entwicklung und die räumliche Ausbreitung von Cybersicherheit und Datenschutz auf und vertrat die These, dass Cybersicherheit und Verschlüsselung schon sehr lange existieren und weltweit verbreitet sind, während Datenschutz eine verhältnismäßig junge Thematik ist. Zum Abschluss seines Vortrags ging er darauf ein, dass Datenschutz in den vergangenen Jahren und auch künftig ein wesentlicher Faktor für die Weiterentwicklung des Bereichs Cybersicherheit sei und beide Themen wichtige Erfolgsfaktoren für die Digitalisierung seien.

Im Rahmen der sich anschließenden Diskussion erfolgte zunächst ein Austausch über die Entwicklung der Anforderungen im Bereich Cookies und die datenschutzkonforme Gestaltung von Cookie-Bannern. Dabei wurde unter anderem auf das Erfordernis einer Einwilligung unter der E-Privacy-Richtlinie, die Entwicklung der Tracking-Möglichkeiten, die gescheiterte Einführung von Personal-Information-Management-Systems (PIMS) zur zentralen Einwilligungsabfrage sowie die Zulässigkeit von Pur-Abo-Modellen eingegangen. In diesem Kontext wurde auch eine aktuelle Entscheidung des EDSA diskutiert, nach der das Verfahren „pay or okay“ nur in begrenztem Umfang für zulässig erachtet wurde. Insoweit seien zeitnah weitere Entwicklung bei den Aufsichtsbehörden und in der Rechtsprechung zu erwarten. Die datenschutzkonforme Gestaltung eines Cookie-Banners erfordere nach aktuellem Stand insbesondere die transparente Darstellung der Auswahlmöglichkeiten „Zustimmen“ und „Ablehnen“ auf der ersten Seite des Cookie-Banners. Außerdem sei es wichtig, dem Nutzer die für seine Entscheidung erforderlichen Informationen zur Verfügung zu stellen. Dabei könnten die weiterführenden Informationen auch in die Datenschutzerklärung ausgelagert werden, solange die für die Entscheidung wesentlichen Punkte im Cookie-Banner selbst zentral bereitgestellt werden. Der Cookie-Banner müsse außerdem an das jeweilige Endgerät, auf dem die Anzeige erfolgen soll, angepasst werden. Künftig könnten sich die Anforderungen noch verschärfen, soweit mittels Cookies auch besonders sensible Datenkategorien i.S.v. Art. 9 DSGVO verarbeitet werden sollen.

Das Thema Cybersicherheit wurde sodann mit Blick auf die nach Art. 32 DSGVO verpflichtend zu ergreifenden technischen und organisatorischen Maßnahmen noch einmal aufgegriffen. Es sei insoweit vor allem wichtig, dass Unternehmen über ein Zugriffsberechtigungskonzept verfügen, um steuern zu können, wer in welchem Umfang auf die Daten zugreift. Daneben sollte zusätzlich protokolliert und auch kontrolliert werden, wer tatsächlich auf die Daten zugegriffen hat. Außerdem sei es sinnvoll, Daten verschlüsselt auf den vom Unternehmen genutzten (externen) Systemen wie Servern oder Clouds abzulegen. Wichtig sei zudem, Mitarbeiter für einen rechtskonformen Umgang mit Daten zu sensibilisieren etwa durch Schulungsmaßnahmen oder Richtlinien zur IT-Sicherheit.

BRANDI-Nachwuchsrunde

Im Rahmen der BRANDI-Nachwuchsrunde wurden zum Abschluss der Veranstaltung aktuelle datenschutzrechtliche Themen im Rahmen von Kurzvorträgen von angehenden Juristinnen und Juristen präsentiert.

Frau Christina Prowald und Frau Gesche Kracht berichteten zu Beginn über das Thema „Zugriff des Arbeitgebers auf E-Mail-Accounts von Arbeitnehmern“. Dabei gingen sie zunächst auf die datenschutzrechtlichen Anforderungen ein und erläuterten insbesondere, welche Rechtsgrundlagen zur Rechtfertigung eines solchen Zugriffs je nach Fallgestaltung herangezogen werden können. Anschließend erfolgte eine Auseinandersetzung mit der Frage, ob neben den datenschutzrechtlichen Bestimmungen auch das Fernmeldegeheimnis zu beachten ist, wenn Mitarbeitern die Privatnutzung ihres E-Mail-Accounts gestattet ist oder eine solche zumindest geduldet wird. Bis zu einer abschließenden Klärung empfehle es sich, die Thematik unternehmensintern ausdrücklich zu regeln, die Privatnutzung bestenfalls zu unterbinden oder sich alternativ von den Beschränkungen des Fernmeldegeheimnisses befreien zu lassen. Zum Abschluss gingen die Vortragenden darauf ein, wie bei einem Zugriff aufgrund von vorübergehender oder dauerhafter Abwesenheit eines Mitarbeiters und aufgrund von missbräuchlichem Verhalten vorgegangen werden sollte und gaben Empfehlungen für den praktischen Umgang mit Zugriffserfordernissen. Es empfehle sich insoweit, die Thematik bereits im Vorfeld zu regeln und Maßnahmen wie das Einstellen einer Abwesenheitsnotiz oder einer Weiterleitung oder das Abspeichern relevanten Informationen an einem zentralen Ablageort vorzugeben. Sei ein Zugriff dennoch erforderlich, sei darauf zu achten, dass die Einsichtnahme nur im erforderlichen Umfang durch sensibilisierte Mitarbeiter nach dem „Mehr-Augen-Prinzip“ vorgenommen und diese auch protokolliert wird. Eine vorherige Bewertung durch den Datenschutzbeauftragten sei grundsätzlich empfehlenswert.

Im zweiten Vortrag berichtete Frau Carolina Vortkamp über die Entscheidung des BGH zum Recht auf eine Datenkopie nach Art. 15 Abs. 3 DSGVO. Nach einer kurzen Einführung in den Sachverhalt und den Verfahrensgang ging sie dabei vor allem auf die Entscheidungsgründe des BGH ein. Dieser sei der Auffassung, dass ein personenbezogenes Datum dann vorliege, wenn eine irgendwie geartete Information über eine Person gegeben sei. Dies sei anzunehmen, wenn die Information eine Verknüpfung mit einer konkreten Person aufgrund des Inhalts, des Zwecks oder der Auswirkung der Information aufweise. Schreiben der betroffenen Person an den Verantwortlichen seien insoweit ihrem gesamten Inhalt nach als personenbezogene Daten einzustufen, da eigene Äußerungen bzw. Schreiben grundsätzlich eine Verknüpfung zur Person des Äußernden aufweisen würden. In der Folge bestehe ein Anspruch auf Überlassung einer Kopie des gesamten Dokuments. Bei Unterlagen, die nicht von dem Betroffenen selbst stammen, seien hingegen nur die darin wirklich enthaltenen personenbezogenen Daten vom Auskunftsanspruch umfasst, sodass lediglich ein Anspruch auf Überlassung einer Kopie der enthaltenen Daten, nicht des gesamten

Dokuments bestehe. Etwas Anderes gelte nur dann, wenn die Kontextualisierung erforderlich sei, um die Datenverarbeitung nachvollziehen und von seinen Rechten Gebrauch machen zu können.

Herr Hendrik Verst berichtete zum Abschluss über die Nutzung von Microsoft 365 im Unternehmen. Er führte aus, dass aus datenschutzrechtlicher Sicht zusätzlich zur Lizenzvereinbarung eine Vereinbarung zur Auftragsverarbeitung abgeschlossen werden müsse. Problematisch sei insoweit, dass aufgrund der Marktmacht von Microsoft kein Verhandlungsspielraum gegeben sei und in der Folge der Standardvertrag von Microsoft abgeschlossen werden müsse. Seitens der Aufsichtsbehörden würden insoweit vor allem die intransparente Darstellung der erfolgenden Datenverarbeitungen, der verarbeiteten Daten und der betroffenen Personen, die unzureichende Abgrenzung der Verantwortlichkeiten und die fehlenden Weisungs- und Kontrollmöglichkeiten kritisiert. In der Praxis empfehle es sich, die jeweils aktuelle Version der Vereinbarung abzuschließen, die technischen Konfigurationsmöglichkeiten zu nutzen und den Datenabfluss an Microsoft so zu begrenzen, eine umfassende Dokumentation anzufertigen und ggf. zusätzliche Maßnahmen, etwa zur Verschlüsselung der Daten, zu ergreifen.

Nähere Informationen zum 5. BRANDI-Datenschutzrechtstag und den einzelnen Inhalten finden Sie auch auf unserer Webseite.

Christina Prowald

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

T +49 521 96535 - 980
F +49 521 96535 - 113
M christina.prowald@brandi.net