BRANDI
RECHTSANWÄLTE

JAHRESRÜCKBLICK 2021 UND AUSBLICK 2022

Informationen zum Datenschutz I Januar 2022

Einleitung

Die Ausbreitung des Corona-Virus hat im Jahr 2021 Herausforderungen mit sich gebracht, die auch von datenschutzrechtlicher Relevanz sind. Unter anderem haben die Kontaktnachverfolgung, die Durchführung von Corona-Selbsttests und die Einführung der 3G-Regel am Arbeitsplatz in Unternehmen zahlreiche datenschutzrechtliche Fragen aufgeworfen.

Unabhängig von der Corona-Pandemie gab es neue Entwicklungen im Datenschutzrecht auch aufgrund von Tendenzen und Vorgaben aus der Rechtsprechung, aufgrund von Gesetzgebungsverfahren und Aktivitäten der Europäischen Kommission sowie der Aufsichtsbehörden. Zu nennen sind insofern beispielsweise das Inkrafttreten des neuen Telekommunikation-Telemedien-Datenschutz-Gesetzes und die Verabschiedung der aktualisierten Standardvertragsklauseln für den internationalen Datentransfer.

Über die aktuellen Geschehnisse im Datenschutzrecht hat BRANDI sich im Jahr 2021 in zwei Veranstaltungen mit Experten des Datenschutzrechts ausgetauscht: Auf dem Datenschutzrechtstag am 07.05.2021 hat uns der rheinland-pfälzische Landesdatenschutzbeauftragte Herr Prof. Dr. Dieter Kugelmann einen Einblick in die tägliche Arbeit seiner Datenschutz-Aufsichtsbehörde gegeben und auf dem IT- und Datenschutztag am 30.09.2021 haben wir uns mit dem baden-württembergischen Landesdatenschutzbeauftragten, Herrn Dr. Stefan Brink, über verschiedene datenschutzrechtliche Themen unterhalten. Mit dem BRANDI Blog haben wir im Jahr 2021 außerdem ein weiteres Medium ins Leben gerufen, in dem wir über aktuelle rechtliche Themen berichten.

Den Jahreswechsel haben wir zum Anlass genommen, in unserem traditionellen Jahresrückblick wesentliche Datenschutzthemen aus dem Jahr 2021 noch einmal Revue passieren zu lassen. Außerdem wagen wir einen Ausblick auf Datenschutzthemen des Jahres 2022.

Schwerpunktthemen des Datenschutz-Newsletters von BRANDI

In unserem Datenschutz-Newsletter berichten wir jeden Monat über aktuelle Geschehnisse aus dem Datenschutzrecht. Zudem informieren wir vertieft über jeweils ein ausgewähltes Schwerpunktthema, zu dem wir auf wenigen Seiten die wesentlichen datenschutzrechtlichen Besonderheiten und besonders praxisrelevanten Hinweise zusammenfassen. Die Schwerpunktthemen unseres Datenschutz-Newsletters aus dem Jahr 2021 haben wir nachfolgend für Sie zusammengefasst.

Rechtsprechung

Der Europäische Gerichtshof (EuGH) hat im Juni 2021 in einer Entscheidung die Möglichkeiten zum Vorgehen nationaler Datenschutz-Aufsichtsbehörden gegen internationale Konzerne gestärkt. Er hat entschieden, dass neben der federführenden Datenschutz-Aufsichtsbehörde unter bestimmten Voraussetzungen auch eine andere nationale Datenschutz-Aufsichtsbehörde ihre Befugnis, vermeintliche Verstöße gegen die Datenschutz-Grundverordnung (DSGVO) vor einem Gericht eines Mitgliedstaates geltend zu machen, ausüben kann (EuGH, Urt. v. 15.06.2021 – Az. C-645/19, vgl. auch die zugehörige Pressemitteilung des EuGH). Grenzüberschreitende Verfahren wegen DSGVO-Verstößen dürfen damit nicht nur von den nationalen Aufsichtsbehörden eingeleitet werden, die an dem EU-Sitz des betroffenen Unternehmens ansässig sind.

Im November 2021 kam der EuGH in einem Urteil zu dem Ergebnis, dass Inbox-Werbung einer vorherigen Einwilligung des Betroffenen bedarf (EuGH, Urt. v. 25.11.2021 – Az. C-102/20). In dem der Entscheidung zugrunde liegenden Fall wurde Werbung eingeblendet, sobald die Nutzer eines E-Mail-Dienstes ihren Posteingang öffneten, wobei sowohl die betroffenen Nutzer als auch die eingeblende-

ten Nachrichten zufällig ausgewählt wurden (sog. „Inbox advertising"). Der EuGH qualifiziert in seinem Urteil die Werbeeinblendungen als „Verwendung elektronischer Post für die Zwecke der Direktwerbung" im Sinne von Art. 13 Abs. 1 der Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG), die nur unter der Voraussetzung gestattet sei, dass der Empfänger zuvor darin eingewilligt habe.

Das Landgericht Berlin hat in erster Instanz den von der Berliner Datenschutz-Aufsichtsbehörde erlassenen Bußgeldbescheid gegen die Deutsche Wohnen SE aus formalen Gründen als unwirksam angesehen (LG Berlin, Beschl. v. 18.02.2021 – Az. 526 AR). Die Aufsichtsbehörde hatte im September 2019 ein Bußgeld über 14,5 Millionen Euro gegen das Immobilienunternehmen festgesetzt, weil Mieterdaten nicht datenschutzkonform gespeichert wurden und insbesondere keine rechtzeitige Löschung von Altdaten erfolgt ist. Nach Auffassung des Gerichts komme eine Sanktionierung allerdings nicht in Betracht, soweit dem Unternehmen kein Verschulden nach Leitungspersonen nachgewiesen werden kann. Diese Argumentation deckt sich mit der Auffassung des österreichischen Bundesverwaltungsgerichts, das bereits im Vorjahr ein Bußgeld in Höhe von 18 Millionen Euro gegen die österreichische Post aufgehoben hatte (BVwG, Erkenntnis vom 26.11.2020 – Az. W258 2227269-1/14E). Das Landgericht Bonn hat in einem anderen Fall dagegen zwar das Bußgeld gegen das Telekommunikationsunternehmen 1&1 Telecom von 9,5 Millionen Euro auf 900.000 Euro gesenkt, allerdings keine grundsätzlichen Bedenken gegen die Bußgeldpraxis des Bundesdatenschutzbeauftragten geltend gemacht (LG Bonn, Urt. v. 11.11.2020 – Az. 29 OWi 1/20). In dem Fall vor dem Landgericht Berlin hat auf Veranlassung der Berliner Aufsichtsbehörde die Staatsanwaltschaft bereits Beschwerde gegen den Beschluss des Gerichts eingelegt; in der zweiten Instanz hat das Kammergericht jetzt Fragen zur Anforderung bei der Festsetzung von Bußgeldern dem EuGH vorgelegt (KG, Beschl. v. 06.12.2021, Az. 3 Ws 250/21). Unabhängig von der endgültigen Klärung der Angelegenheit zeigt sich, dass es für beide Seiten in Bußgeldverfahren zahlreiche Unwägbarkeiten gibt. Auffällig ist weiter, dass bisher weder in Deutschland noch in den anderen Mitgliedsstaaten der EU die bisherigen Bußgeldentscheidungen bei einer gerichtlichen Überprüfung sonderlich häufig bestätigt werden.

Gesetzgebungsverfahren

Der Bundestag hat am 24.06.2021 das „Gesetz für faire Verbraucherverträge" beschlossen. Teil des Gesetzes ist eine neue Regelung für Einwilligungen in Telefonwerbung durch einen neu eingeführten § 7a in dem Gesetz gegen den unlauteren Wettbewerb (UWG). Die Regelung ist am 01.10.2021 in Kraft getreten. Nach der Vorschrift hat derjenige, der mit einem Telefonanruf gegenüber einem Verbraucher wirbt, dessen vorherige ausdrückliche Einwilligung in die Telefonwerbung zum Zeitpunkt der Erteilung in angemessener Form zu dokumentieren und aufzubewahren. Der Nachweis muss von dem Unternehmen ab Erteilung der Einwilligung für fünf Jahre aufbewahrt werden, wobei sich der Fristbeginn mit jeder Verwendung der Einwilligung erneuert.

Zum 01.12.2021 ist das neue Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft getreten. Das TTDSG enthält insbesondere Regelungen zum Datenschutz bei Telekommunikationsdiensten sowie Telemedien und führt die bislang im Telekommunikationsgesetz und im Telemediengesetz getrennt normierten Datenschutzbestimmungen in einem Gesetz zusammen. Mit dem neuen § 25 TTDSG hat der Gesetzgeber die Anforderungen der E-Privacy-Richtlinie sowie der Rechtsprechung des EuGH und des Bundesgerichtshofs (BGH) zur Nutzung von Cookies beziehungsweise diesen vergleichbaren Technologien in einer nationalen Regelung umgesetzt.

Aktivitäten der Europäischen Kommission

Nachdem der EuGH in seiner Entscheidung Schrems II (EuGH, Urt. v. 16.07.2020 – Az. C-311/18) das EU-US-Privacy-Shield-Abkommen für ungültig erklärt und die weitere Nutzung von Standardvertragsklauseln unter die Bedingung gestellt hatte, dass unter bestimmten Umständen zusätzliche Schutzmaßnahmen etabliert werden, war die Rechtsunsicherheit im Hinblick auf die rechtliche Absicherung internationaler Datentransfers verhältnismäßig hoch. Von dem EuGH wurde insbesondere das Fehlen wirksamer Rechtsschutzmöglichkeiten in Anbetracht der weitreichenden Zugriffsbefugnisse von Behörden auf in Drittstaaten übermittelte Daten kritisiert. In Anbetracht dessen hat die Europäische Kommission am 04.06.2021 aktualisierte Standardvertragsklauseln verabschiedet, die als geeignete Garantien zur Einhaltung europäischer Datenschutzstandards dienen sollen. Die neuen Standardvertragsklauseln enthalten Verbesserungen und zusätzliche Sicherheiten. Gleichwohl können sie nicht alle Problempunkte hinsichtlich bestehender Konflikte mit den Rechtsordnungen von Drittstaaten vollständig beheben, weshalb Unternehmen auch weiterhin das Datenschutzniveau bei Datenübermittlungen im Einzelfall prüfen sollten. Wie sich der EuGH zu der Frage, ob die neuen Klauseln ein ausreichendes Datenschutzniveau gewährleisten können, positionieren wird, bleibt abzuwarten.

Für die Datenübermittlung in das Vereinigte Königreich hat die EU-Kommission am 28.06.2021 einen Angemessenheitsbeschluss erlassen, der zunächst bis zum 27.06.2025 befristet ist. Aufgrund des Brexit-Abkommens zwischen der EU und dem Vereinigten Königreich vom 31.12.2020 galt das Vereinigte Königreich trotz seines Austritts aus der EU für einen Übergangszeitraum bis zum 30.06.2021 bei der Übermittlung personenbezogener Daten nicht als Drittstaat im Sinne der DSGVO. Um eine Regelung für die Zeit nach dem Übergangszeitraum zu finden, hatte die Europäische Kommission im Februar 2021 einen Entwurf eines Angemessenheitsbeschlusses für die Übermittlung personenbezogener Daten in das Vereinigte Königreich veröffentlicht. Im April 2021 hat der Europäische Datenschutzausschuss (EDSA) eine Stellungnahme hierzu veröffentlicht, in der er zwar viele Aspekte des Datenschutzniveaus im Vereinigten Königreich als gleichwertig mit dem Datenschutzniveau in der EU identifiziert, aber auch Herausforderungen erkannt hat.

Aktivitäten von Aufsichtsbehörden

Die Datenschutz-Aufsichtsbehörden wurden im Jahr 2021 bezogen auf verschiedene datenschutzrechtliche Themen tätig. Unter anderem wurden Bußgelder aufgrund von Datenschutzverstößen verhängt und Stellungnahmen zu ausgewählten Themen veröffentlicht.

Bußgelder

Die irische Datenschutz-Aufsichtsbehörde DPC hat im September 2021 gegen die zum Facebook-Konzern gehörende WhatsApp Ireland Ltd. ein Bußgeld in Höhe von 225 Millionen Euro verhängt, weil betroffene Personen nicht transparent genug über die Datenverarbeitung durch WhatsApp informiert wurden. Die irische Aufsichtsbehörde hatte das Verfahren bereits 2018 eingeleitet und wollte eigentlich ein moderates Bußgeld verhängen. Mehrere andere europäische Aufsichtsbehörden hatten förmlich Bedenken gegen das Vorgehen geäußert. Nachdem keine Einigung erzielt werden konnte, hat der europäische Datenschutzausschuss EDPB verbindlich vorgegeben, dass von einem größeren Umfang an Datenschutzverletzungen ausgegangen werden müsse und die Sanktionen deutlich strenger ausfallen müssen. Die irische Aufsichtsbehörde hat sich letztlich diesen Vorgaben gebeugt. Es wird erwartet, dass sich Facebook und WhatsApp gegen die Entscheidung gerichtlich zur Wehr setzen werden.

Die norwegische Datenschutzbehörde Datatilsynet hat im Dezember 2021 ein Bußgeld in Höhe von umgerechnet ungefähr 6,5 Millionen Euro gegen die Grindr LLC verhängt. Dem Unternehmen, das die Dating- und Social-Networking-App Grindr betreibt, wird vorgeworfen, Nutzerdaten mit Dritten geteilt zu haben, ohne dass für diese Datenverarbeitung die erforderlichen Einwilligungen bestanden. Zudem habe Grindr die Nutzer nicht in ausreichender Weise über die Datenverarbeitung informiert. Grindr kann gegen die Entscheidung innerhalb von drei Wochen Einspruch erheben.

Die Landesbeauftragte für den Datenschutz Niedersachsen (LfD) hat gegenüber der notebooksbilliger.de AG ein Bußgeld in Höhe von 10,4 Millionen Euro ausgesprochen. Dem Unternehmen wird vorgeworfen, über mindestens zwei Jahre seine Mitarbeiter mit Videokameras überwacht zu haben, ohne dass dafür eine ausreichende Rechtsgrundlage bestand. Unter anderem aufgrund der hohen schutzwürdigen Interessen der Betroffenen in Bereichen, die typischerweise für eine längere Aufenthaltsdauer bestimmt sind, und aufgrund der Tatsache, dass die Videoüberwachung zeitlich unbegrenzt und nicht auf konkrete Beschäftigte zur Aufklärung von Straftaten beschränkt war, sei die Videoüberwachung nach Auffassung des Gerichts in dem konkreten Fall nicht verhältnismäßig gewesen. Die notebooksbilliger.de AG hat sich in einer Pressemitteilung zu dem Bußgeldbescheid geäußert und die Bußgeldhöhe als unverhältnismäßig kritisiert. Sie hat Einspruch gegen den Bußgeldbescheid eingelegt.

Der Energieversorger Vattenfall Europe Sales GmbH veröffentlichte am 24.09.2021 eine Pressemitteilung, wonach gegen das Unternehmen ein Bußgeld in Höhe von 900.000 Euro vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) verhängt worden sei. Zwischen August 2018 und Dezember 2019 glich das Unternehmen anhand seiner Kundendatei Daten potenzieller Neukunden mit bereits beim Unternehmen vorhandenen älteren Kundendaten ab, um preisbewusste Verbraucher, die häufiger ihren Energieversorger wechselten, um etwaige Boni zu erhalten, auszusortieren und abzulehnen. Von der Aufsichtsbehörde wurde gerügt, dass der Energieversorger die Betroffenen nicht entsprechend der Anforderungen der Art. 13 und 14 DSGVO über den internen Datenabgleich im Zusammenhang mit Vertragsanfragen für Sonderangebote ausreichend transparent informiert habe. Vattenfall akzeptierte das Bußgeld.

Stellungnahmen

Die Aufsichtsbehörden äußerten sich in verschiedenen Stellungnahmen zu datenschutzrechtlichen Themen.

Der HmbBfDI hat auf seiner Internetseite einen Vermerk veröffentlicht, in dem er sich mit der Abdingbarkeit von technischen und organisatorischen Maßnahmen beschäftigt. Es geht dabei um die Frage, ob betroffene Personen bezüglich ihrer personenbezogenen Daten in ein niedrigeres als das rechtlich geforderte Schutzniveau einwilligen können. Die Datenschutz-Aufsichtsbehörde kommt zu dem Ergebnis, dass Verantwortliche und Auftragsverarbeiter die nach Art. 32 DSGVO erforderlichen Maßnahmen zwingend umzusetzen und vorzuhalten haben. Betroffene Personen könnten aber in die Herabsetzung dieses Schutzniveaus bezogen auf ihre eigenen Daten im Einzelfall einwilligen.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) hat zu Fragen und Maßnahmen von Arbeitgebern zum Schutz vor Corona-Infektionen und in diesem Zusammenhang zu der Erhebung von Gesundheitsdaten durch den Arbeitgeber eine Einschätzung auf ihrer Homepage veröffentlicht. Darin erläutert die LDI NRW, dass Informationen über die Gesundheit von Beschäftigten oder Bewerbern einem besonderen Schutz unterliegen, deren Verarbeitung im Arbeitsverhältnis in einem engen gesetzlichen Rahmen erlaubt ist. Sie gibt Hinweise für verschiedene Fallkonstellationen im Zusammenhang mit der Corona-Pandemie, unter anderem zu der Frage, wie 3G-Kontrollen am Arbeitsplatz datenschutzkonform durchgeführt werden können.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat sich in einer Stellungnahme vom 14.09.2021 zu der Vereinbarkeit der Telefax-Nutzung mit der DSGVO geäußert. Seiner Ansicht nach könne die Übermittlung von personenbezogenen Daten per Telefax insbesondere dann gegen die DSGVO verstoßen, wenn es sich um besonders schutzbedürftige Daten handele. Der Faxversand weise vergleichbare Risiken auf, wie diese auch bei dem unverschlüsselten Versand von E-Mail-Nachrichten gegeben seien. Der hessische Landesdatenschutzbeauftragte empfiehlt daher, besonders schutzwürdige personenbezogene Daten grundsätzlich nicht per Telefax zu übertragen, wenn keine zusätzlichen Schutzmaßnahmen bei den Versendern und Empfängern, etwa Verschlüsselungstechnologien, implementiert seien. Lediglich in Ausnahmefällen könne auch die Versendung besonders schutzbedürftiger personenbezogener Daten mittels Fax rechtmäßig sein.

In ähnlicher Weise hat sich am 14.05.2021 die Landesdatenschutzbeauftragte in Bremen in einer Stellungnahme geäußert. Insbesondere für die Übertragung besonderer Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DSGVO sei ihrer Ansicht nach die Nutzung von Fax-Diensten unzulässig.

Besondere Herausforderungen aufgrund der Corona-Pandemie

Zur Erleichterung der Abfrage von Kontaktdaten zur Nachverfolgung von Infektionsketten gibt es verschiedene softwaregestützte Lösungen, wobei im Jahr 2021 neben der Corona Warn-App die App luca in vielen Bereichen zum Einsatz kam und auch weiterhin zum Einsatz kommt. Dies ist jedenfalls mit entsprechenden freiwilligen Einwilligungen der Betroffenen möglich. Darüber hinaus müssen Unternehmen unter anderem die betroffenen Personen transparent über die Datenverarbeitung informieren.

Da regelmäßig nicht alle Mitarbeiter eines Unternehmens die Möglichkeit haben, im Homeoffice zu arbeiten, wurde im Jahr 2021 zur Eindämmung des Corona-Virus verstärkt auf Testmöglichkeiten gesetzt. Aufgrund einer Änderung der SARS-CoV-2-Arbeitsschutzverordnung (SARS-CoV-2-ArbSchV) vom 21.04.2021 müssen Unternehmen ihren Beschäftigten grundsätzlich zwei Corona-Tests pro Woche anbieten. Corona-Testergebnisse unterliegen als sensible Gesundheitsdaten einem besonders hohen Schutz. Bei der Durchführung von Corona-Selbsttests in Unternehmen sollten daher die datenschutzrechtlichen Bestimmungen eingehalten werden und sollte insbesondere der Grundsatz der Datenminimierung beachtet werden.

Am 24.11.2021 ist das „Gesetz zur Änderung des Infektionsschutzgesetzes und anderer Gesetze“ in Kraft getreten. Mit diesem Gesetzesvorhaben wurde unter anderem die 3G-Regel am Arbeitsplatz eingeführt. Hiernach dürfen lediglich solche Beschäftigte Arbeitsstätten, in denen physische Kontakte nicht ausgeschlossen werden können, betreten, die geimpft, genesen oder getestet sind. Arbeitgeber sind verpflichtet, die Einhaltung der 3G-Regel am Arbeitsplatz täglich zu überwachen und regelmäßig zu dokumentieren. Die Erfüllung dieser Kontroll- und Dokumentationspflichten setzt die Verarbeitung personenbezogener Daten voraus. Das Infektionsschutzgesetz sieht insofern eine ausdrückliche Ermächtigung zur Datenverarbeitung vor. Es müssen jedoch technische und organisatorische Maßnahmen zum Schutz dieser Daten zur Anwendung kommen.

Zu den datenschutzrechtlichen Herausforderungen der Corona-Pandemie haben sich auch die Datenschutz-Aufsichtsbehörden geäußert. Die Konferenz der Datenschutz-Aufsichtsbehörden des Bundes und der Länder (DSK) hat eine Stellungnahme zur Kontaktverfolgung in Zeiten der Corona-Pandemie sowie eine Orientierungshilfe zum Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurant- und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19 veröffentlicht. Aufgrund der Digitalisierung und der in Zeiten der Pandemie stark eingeschränkten Möglichkeiten von Präsenzprüfungen hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg eine Handreichung für Hochschulen veröffentlicht, die Hinweise dazu enthält, wie Online-Prüfungen unter Beachtung der datenschutzrechtlichen Anforderungen durchgeführt werden können.

Ausblick 2022

Verschiedene Datenschutzthemen aus dem Vorjahr werden auch im Jahr 2022 weiterhin eine Rolle spielen. Dies betrifft unter anderem die datenschutzrechtlichen Herausforderungen der Corona-Pandemie. Außerdem ist mit neuen Themen zu rechnen.

In dem Koalitionsvertrag 2021 – 2025 zwischen SPD, Bündnis 90/Die Grünen und FDP sind unter anderem Regelungen mit datenschutzrechtlicher Relevanz enthalten. Zur besseren Durchsetzung und Kohärenz des Datenschutzes planen die Ampel-Parteien, die europäische Zusammenarbeit zu verstärken und die DSK im Bundesdatenschutzgesetz zu institutionalisieren und ihr rechtlich verbindliche Beschlüsse zu ermöglichen. Geplant sind zudem unter anderem Regelungen zum Beschäftigtendatenschutz, die Förderung von Anonymisierungstechniken und die Einführung der Strafbarkeit rechtswidriger De-Anonymisierung. Die Koalition will sich außerdem für eine schnelle Verabschiedung einer „ambitionierten" E-Privacy-Verordnung einsetzen.

Hinsichtlich der E-Privacy-Verordnung hat sich der Rat der EU am 10.02.2021 auf ein Verhandlungsmandat zum Verordnungsvorschlag über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation geeinigt. Die E-Privacy-Verordnung soll die Vertraulichkeit elektronischer Kommunikation stärken. Es bleibt abzuwarten, ob es in der Folgezeit zu einer Einigung über den Entwurf und einer Verabschiedung der Verordnung kommen wird und welchen endgültigen Wortlaut der Rat, das Europäische Parlament und die Europäische Kommission aushandeln werden. Mit einem Inkrafttreten der neuen Regelungen ist aber weiterhin nicht vor 2023 zu rechnen.

Im Jahr 2022 wird es für digitale Produkte und Dienstleistungen erste Zertifizierungen nach der DSGVO geben. Bisher gibt es keine akkreditierte Zertifizierungsstelle, die ein echtes DSGVO-Zertifikat ausstellen könnte; im Jahr 2022 sollen aber die ersten Stellen den Akkreditierungsprozess durchlaufen haben. Datenschutzspezifische Zertifizierungsverfahren können dem Nachweis dienen, dass bei Datenverarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern die datenschutzrechtlichen Vorgaben eingehalten werden. Die Zertifizierungsstellen werden in Deutschland von der Deutschen Akkreditierungsstelle GmbH (DAkkS) gemeinsam mit der jeweils zuständigen Datenschutzaufsichtsbehörde akkreditiert.

Über die datenschutzrechtlichen Herausforderungen und Geschehnisse, die das Jahr 2022 mit sich bringen wird, wird das Datenschutzteam von BRANDI Sie natürlich auch im neuen Jahr in seinem Datenschutz-Newsletter auf dem Laufenden halten.

Johanna Schmale

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Wissenschaftliche Mitarbeiterin

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