BRANDI
RECHTSANWÄLTE

Dezember 2022

Liebe Leserinnen, liebe Leser,

ein bewegendes Jahr neigt sich dem Ende zu. Warum wir vor Silvester schon einmal auf das Jahresende schauen und was das Finanzamt mit Silvester und einer höheren Schenkungssteuer bei Immobilienschenkungen zu tun hat, erläutern die Kollegen unter anderem aus unserer Kompetenzgruppe Vermögensplanung, Vermögensnachfolge und Erbrecht. Spannend ist auch das Thema der sogenannten „lenkenden Ausschlagung“ der Erbschaft und wie Sie bei Geldvermächtnissen Unklarheiten vermeiden können.

Das Team IT & Datenschutz schaut auf spannende Themen wie Intranetplattformen und wie Sie diese rechtssicher gestalten können, was Sie auch bei KI-basierter Software im Recruiting Prozess beachten sollten und dass die Veröffentlichung der EVB-IT Cloud einen Meilenstein für die Beschaffung von Cloud-Lösungen für die öffentliche Hand darstellt.

Unsere Kolleginnen und Kollegen aus dem Wirtschafts- und Steuerstrafrecht schauen unter anderem darauf, dass Einziehungsanordnungen, die Unternehmensgewinne abschöpfen, genauestens geprüft werden sollten, da sie oftmals in verfahrensrechtlicher Hinsicht angreifbar sind.

Besonders freuen wir uns, dass das gesamte BRANDI Team in diesem Jahr eine besondere Idee für Weihnachtsgeschenke hatte und wir wieder viele neue Gesichter im BRANDI Team begrüßen dürfen.

Wir wünschen Ihnen eine besinnliche Weihnachtszeit, ein gesundes und friedliches neues Jahr.

Ihr BRANDI Team

NEUES AUS DEM BRANDI TEAM

Sigrid Laves
ist mit sämtlichen originären und derivativen Dienstleistungen im Wertpapier- und Kapitalmarktrecht, Stiftungsmanagement und Testamentsvollstreckung durch Sparkassen und Verbraucherstreitbeilegungsangelegenheiten vertraut. Die Stiftungsrechtsreform 2023 mit der Vereinheitlichung des Stiftungsrechts im Bürgerlichen Gesetzbuch stellt 2022/2023 dabei einen der Schwerpunkte ihrer Tätigkeit dar.

Seit Juli 2022 verstärkt Frau Laves das BRANDI Team in Hannover und bringt dort ihre Expertise im Bankrecht ein.

Teoman Karaboga
studierte Rechtswissenschaften an der Universität Bielefeld mit dem Schwerpunk „Unternehmens- und Wirtschaftsrecht". Sein Referendariat absolvierte er am Landgericht Bielefeld.

Herr Karaboga ist seit November 2022 als Rechtsanwalt tätig und verstärkt das Dezernat Gesellschaftsrecht/M&A an unserem Gütersloher Standort insbesondere bei der Beratung und Verhandlung von Unternehmenstransaktionen, einschließlich der rechtlichen Due Diligence. Darüber hinaus berät Herr Karaboga Mandanten bei der Gründung von Gesellschaften und begleitet sie bei gesellschaftsrechtlichen Streitigkeiten.

Christian Koerdt
studierte an der Universität Halle-Wittenberg mit dem Schwerpunkt Praxis der Strafverteidigung.

Seine Stationen während des Referendariats absolvierte er u. a. beim Bundeskartellamt und bei BRANDI in Detmold.

Herr Koerdt ist seit November an unserem Standort in Detmold im Bereich Wirtschafts- und Unternehmensrecht tätig.

Dr. Philipp Hahn
ist Rechtsanwalt, Fachanwalt für Familienrecht, Fachanwalt für Erbrecht und Notar. Er studierte an der Universität Bielefeld mit Schwerpunkt im Familienrecht und Erbrecht, war dort anschließend als wissenschaftlicher Mitarbeiter tätig und schloss nach dem Referendariat die Promotion zu einem erbrechtlichen Thema mit verfassungsrechtlichen Bezügen bei Herrn Prof. Dr. Gerhard Otte ab.

Herr Dr. Hahn ist seit 2013 als Rechtsanwalt tätig und verstärkt seit Dezember 2022 unseren Bielefelder Standort im Familienrecht, Erbrecht und Notariat.

Dr. Robert Lepsien
ist jetzt zusätzlich als Fachanwalt für Erbrecht an unserem Standort in Minden für Sie tätig.

Dr. Oliver Knodel
steht Ihnen neben seiner Tätigkeit als Rechtsanwalt und Notar an unserem Standort in Bielefeld nun auch als zertifizierter Stiftungsberater (DSA) zur Verfügung.

FRAGEN AN RÜDIGER HITZ

WARUM BRANDI?

Frei nach Pep Guardiola: BRANDI oder nichts.

WAS TREIBT MICH AN?

Der Kampf um die Freiheit.

In kaum einem anderen Rechtsgebiet sind die Konsequenzen für das zukünftige Leben eines Menschen, aber auch für den Fortbestand eines Unternehmens, so einschneidend wie im Straf- und Bußgeldrecht. Schon der bloße Vorwurf, eine Straftat begangen zu haben, kann zu tiefgreifenden Auswirkungen führen: Zukunftspläne werden vereitelt und Karrierewege werden versperrt. Um drohende Reputationsschäden zu verhindern und den angelasteten Vorwürfen entgegenzutreten, verlangt Strafverteidigung eine passgenaue individualisierte Verteidigungsstrategie.

Jeden Tag treibt mich dabei die Aufgabe an, den Staat und den vermeintlichen Täter auf Augenhöhe zu bringen, die erarbeiteten Verteidigungsziele konsequent zu verfolgen und mich aktiv für die Rechte unserer Mandanten einzusetzen.

AUSSER DEM JOB GIBT ES NOCH?

… Familie, Sport und Reisen. Am besten kombiniert. Zusammen mit meiner Frau und unseren beiden Jungs verbringen wir den Winterurlaub gerne in Österreich beim Skifahren. In den Sommerferien ist Nordamerika unser bevorzugtes Reiseziel. Als geborener Bremer darf ein Besuch im Weserstadion und an der Nordsee einmal im Jahr nicht fehlen.

An den Wochenenden versuche ich mit Freunden gekonnt zu leiden und mit dem Rennrad oder dem Gravelbike eine Runde zu drehen.

Ehrenamtlich engagiere ich mich in der Ausschussarbeit der Bundessteuerberaterkammer.

Rüdiger Hitz
Rechtsanwalt und Steuerberater
Fachanwalt für Steuerrecht
Fachanwalt für Strafrecht
Zertifizierter Berater für Steuerstrafrecht (DAA)
ruediger.hitz@brandi.net

HIGHLIGHTS AUS MEINER HEIMAT?

Entgegen anderslautender Behauptungen gibt es in Hannover einiges zu entdecken. Der Rote Faden ist auf das Straßenpflaster gemalt und bietet eine einfache Möglichkeit, auch ohne Fremdenführer die Stadt schnell und bequem zu erkunden. Der Zoo – ein Muss für Jung und Alt, das kleine Fest im großen Garten, der Feuerwerkswettbewerb, die Herrenhäuser Gärten, das Maschseefest und vieles mehr lassen es in Hannover nie langweilig werden. Daneben verfügt Hannover mit der Eilenriede über einen der größten Wälder (rund 640 Hektar) mitten im Herzen einer Großstadt.

Wir sehen uns in Hannover.

Dr. Sebastian Meyer, LL.M.

Google Fonts und rechtsmissbräuchliche Schadensersatzforderungen

Das Landgericht München hat einem Betroffenen einen Betrag in Höhe von 100,00 EUR zugesprochen, weil das beklagte Unternehmen für seine Homepage frei verfügbare Schriften von Google nicht auf dem eigenen Server hinterlegt hatte, sondern die Schriften direkt bei Seitenaufruf über die Server von Google nachgeladen wurden (LG München, Urt. v. 20.01.2022, Az. 3 O 17493/20, GRUR-RS 2022, 612 – Google Fonts). Auf diese Weise erhielt Google bei jedem Seitenaufruf eines Nutzers zwangsläufig dessen IP-Adresse, weil diese zur Auslieferung der nachgeladenen Inhalte erforderlich war. Das Zivilgericht hat hierin einen Datenschutzverstoß gesehen, der es rechtfertigt, dem Betroffenen einen Schadensersatzanspruch zuzusprechen.

Der Ausgangspunkt, die Einstufung des Vorgehens als Datenschutzverstoß, für die Herleitung des Schadensersatzanspruchs ist nicht zu beanstanden. Die Bereitstellung der Schriftarten von Google wäre für das verklagte Unternehmen auch auf dem eigenen Server rechtlich zulässig und technisch möglich gewesen. Google weist in dem Kontext selbst darauf hin, dass alle Schriftarten unter Open Source Lizenzen veröffentlicht sind und frei genutzt werden können. Die von dem Unternehmen gewählte Umsetzung des Abrufs über Google war daher unnötig und führt insoweit zu einer überflüssigen Offenlegung der IP-Adresse gegenüber Google.

Wenn unter Berücksichtigung der vorstehenden Erwägungen von einem Datenschutzverstoß auszugehen ist, dann stellt sich zwangsläufig die Frage der möglichen Rechtsfolgen. Aus dem Deliktsrecht kann zunächst ein Unterlassungsanspruch hergeleitet werden, wenn von einem Eingriff in das allgemeine Persönlichkeitsrecht auszugehen ist, wozu grundsätzlich auch das Recht auf informationelle Selbstbestimmung gehört. Eigenständige Unterlassungsansprüche werden unmittelbar durch die datenschutzrechtlichen Bestimmungen dagegen nicht gewährt. Für einen zusätzlichen Anspruch auf Schadensersatz ergibt sich dagegen eine Anspruchskonkurrenz zwischen § 823 BGB und Art. 82 DSGVO. Nach dem nationalen Schadensersatzrecht kommt es immer auf ein Verschulden an, außerdem ist ein Ersatz für immaterielle Schäden unter dem Gesichtspunkt des Schmerzensgeldes nur in sehr engen Grenzen denkbar. Der datenschutzrechtliche Schadensersatzanspruch ist dagegen bewusst an geringere Voraussetzungen geknüpft und sieht ausdrücklich auch den Ersatz von immateriellen Schäden vor. Bisher noch nicht gerichtlich geklärt ist allerdings die Frage, ob besondere Anforderungen an die Beeinträchtigung des Betroffenen zu stellen sind, bevor ein immaterieller Schadensersatz verlangt werden kann. Der Umgang mit Ansprüchen auf immateriellen Schadensersatz liegt im Rahmen mehrerer Vorlageverfahren beim EuGH, mit einer kurzfristigen Entscheidung und Klärung ist aber nicht zu rechnen (OGH Österreich, Beschl. v. 15.04.2021, Az. 6 Ob 35/21x, ZD 2021, 631; BAG, Beschl. v. 26.08.2021, Az. 8 AZR 253/20, ZD 2022, 56; LG Saarbrücken, Beschl. v. 22.11.2021, Az. 5 O 151/19, RDV 2022, 107).

Es ist natürlich wenig überraschend, dass nach Veröffentlichung der Entscheidung die Argumentation des LG München zur Herleitung des Schadensersatzanspruchs von interessierten Kreisen als Anleitung aufgefasst wurde, wie Schadensersatzzahlungen verlangt werden können. Es wurden in den vergangenen Monaten in großem Umfang gezielt Unternehmen gesucht, die ebenfalls für ihre Homepages Google Fonts einsetzen, ohne die verwendeten Schriftarten auf den eigenen Servern vorzuhalten. Die Entscheidung des LG München wurde dabei verkürzt so interpretiert, dass ein „allgemeines Unwohlsein“ ausreichend wäre um eine Art Entschädigung zu verlangen.

Für die rechtliche Bewertung der von den Anspruchstellern selbst oder über Rechtsanwälte (Herrn Kairis und Herrn Lenard) geltend gemachten Ansprüche ist zunächst als Ausgangspunkt festzuhalten, dass der eigentliche Datenschutzverstoß bei der dynamischen Einbindung der Schriftarten von Google zumeist nicht mit Aussicht auf Erfolg in Abrede gestellt werden kann. Die Einordnung eines Verhaltens als Datenschutzverstoß führt aber lediglich dazu, dass die verantwortliche Stelle den Verstoß abstellen muss, um sich zukünftig rechtskonform zu verhalten. Weitergehenden Ansprüchen könnte zumindest der Einwand des Rechtsmissbrauchs gem. § 242 BGB entgegenstehen. Von einem Rechtsmissbrauch kann dann ausgegangen werden, wenn eine formale Rechtsstellung ausgenutzt wird, ohne dass ein schützenswertes Eigeninteresse besteht (LG Wuppertal, Urt. v. 29.07.2021, Az. 4 O 409/20, ZD 2022, 53). Indiz für ein rechtsmissbräuchliches Verhalten ist es etwa, wenn zwischen dem Betroffenen und dem Verantwortlichen keinerlei vorangehende Beziehung besteht. Die Geltendmachung gleichartiger Unterlassungsansprüche gegen eine Vielzahl von Anspruchsgegnern deutet ebenfalls auf ein missbräuchliches Verhalten hin. Ein weiterer Anhaltspunkt kann es sein, wenn der Aufwand der Rechtsverfolgung in keinem vernünftigen Verhältnis zu dem Ergebnis steht. Bezogen auf die Einbindung der Webfonts von Google treffen alle Indizien auf die Aufforderungsschreiben der Betroffenen zu. Soweit die Zahlung von Schadensersatz verlangt wird, müsste außerdem erklärt werden, worin der konkrete Schaden des Betroffenen liegen soll. Wenn es dem Betroffenen darum geht, die Datenschutzverletzung dafür zu nutzen, um einen Schadensersatzanspruch geltend zu machen, dann ist die Datenschutzverletzung eher eine notwendige Voraussetzung, als ein echtes schadensauslösendes Ereignis. Es liegt praktisch ein Fall bewusster Selbstschädigung vor, weil es der Betroffene gerade darauf anlegt, einen Schaden zu erleiden, um diesen dann zum Anlass zu nehmen, um einen immateriellen Schadensersatz zu fordern.

Im Ergebnis ist daher festzuhalten, dass die zahlreichen „Abmahnungen“ wegen der dynamischen Einbindung von Webfonts hinsichtlich des inhaltlichen Ausgangspunkts zutreffend sind. Abgemahnte Unternehmen sollten daher zunächst die Internetseiten so anpassen, dass die verwendeten Schriftarten lokal installiert sind. Zahlungen sollten dagegen an die Abmahner bzw. „Hinweisgeber“ keinesfalls geleistet werden, um dieser Art des Vorgehens nicht weiter Vorschub zu leisten. Besonders effektiv ist eine kurze anwaltliche Antwort, in der insbesondere auf den Aspekt des Rechtsmissbrauchs hingewiesen wird. Durch die anwaltliche Antwort gibt das betroffene Unternehmen zu erkennen, juristisch beraten zu sein. Aus Sicht des Abmahners ist das Unternehmen damit kein lohnenswertes Ziel mehr für vergleichbare Aktivitäten in der Zukunft oder eine gerichtliche Klärung. Zwar lassen sich die Argumente aus der Entscheidung des LG München nicht ohne Weiteres auf andere Fälle, etwa

generell das Nachladen von Drittinhalten, übertragen, es dürfte aber dennoch mit entsprechenden Versuchen in der Zukunft zu rechnen sein. Dies gilt natürlich umso mehr, je erfolgreicher die jetzige Abmahnwelle ist. Bis jetzt sind die Abmahner leider vergleichsweise erfolgreich, weil die geforderten Beträge bewusst so niederschwellig gewählt sind, dass offensichtlich zahlreiche Unternehmen immer noch ohne rechtliche Prüfung bzw. Beratung zahlen.

Der Autor ist Rechtsanwalt und Fachanwalt für IT-Recht sowie Inhaber mehrerer Lehraufträge, unter anderem an der Universität Bielefeld. Er ist häufig als externer Datenschutzbeauftragter für Unternehmen tätig und befasst sich daher mit einer Vielzahl von datenschutzrechtlichen Abmahnungen. In der Ausgabe 6/2022 der Zeitschrift Recht der Datenverarbeitung (RDV) ist ein ausführlicher Beitrag des Autors zu rechtsmissbräuchlichen Schadensersatzforderungen im Datenschutzrecht erschienen (RDV 2022, 300).

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt und Notar mit Amtssitz in Bielefeld
Fachanwalt für Informationstechnologierecht (IT-Recht)
Datenschutzauditor
sebastian.meyer@brandi.net

Johanna Schmale

Umgang mit Löschanfragen im Falle des Widerrufs von Einwilligungen

Angesichts der Redewendung „Gelöschte Daten sind die sichersten Daten" verwundert es nicht, dass die Grundsätze der Datenminimierung und Speicherbegrenzung wesentliche Prinzipien der Datenschutz-Grundverordnung (DSGVO) sind. Bei Beachtung dieser Grundsätze müssen die Datenverarbeitung und die Möglichkeit der Identifizierung einer Person anhand gespeicherter Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Art. 5 Abs. 1 lit. c) und e) DSGVO). Bereits aus diesen Prinzipien ergibt sich die Pflicht des Verantwortlichen, personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung nicht (mehr) erforderlich sind, unaufgefordert zu löschen. Daneben räumt Art. 17 DSGVO Betroffenen ein eigenes Recht ein, in bestimmten Fällen die Löschung ihrer Daten von dem Verantwortlichen zu verlangen. Ein möglicher Grund für die Datenlöschung liegt gem. Art. 17 Abs. 1 lit. b) DSGVO vor, wenn die betroffene Person ihre Einwilligung in die Datenverarbeitung widerruft und die Datenverarbeitung nicht auf eine anderweitige Rechtsgrundlage gestützt werden kann.

Jede Verarbeitung personenbezogener Daten im Anwendungsbereich der DSGVO muss auf eine Rechtsgrundlage gestützt werden können, beispielsweise auf eine Einwilligung des Betroffenen. Eine einmal erteilte Einwilligung kann gem. Art. 7 Abs. 3 S. 1 DSGVO jederzeit mit Wirkung für die Zukunft widerrufen werden. Macht ein Betroffener von diesem Recht Gebrauch, entfällt für die Zukunft diese Rechtsgrundlage für die Datenverarbeitung. Kann die Datenverarbeitung nicht auf eine andere Rechtsgrundlage gestützt werden, sind insoweit die Voraussetzungen des Rechts auf Löschung aus Art. 17 Abs. 1 lit. b) DSGVO erfüllt. Als alternative Rechtsgrundlagen haben insbesondere die Datenverarbeitung aufgrund berechtigter Interessen (Art. 6 Abs. 1 S. 1 lit. f) DSGVO) sowie die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 S. 1 lit. c) DSGVO) praktische Relevanz. Eine rechtliche Verpflichtung zur Datenverarbeitung kann etwa vorliegen, wenn ein Unternehmen aufgrund gesetzlicher Aufbewahrungsfristen zur weiteren Speicherung der Daten verpflichtet ist. In diesen Fällen darf der Verantwortliche die Daten trotz des Widerrufs der Einwilligung weiter verarbeiten, bis die anderweitige Rechtsgrundlage entfällt. In allen anderen Fällen hat er jedoch dem Verlangen des Betroffenen nachzukommen und die Daten entsprechend unverzüglich zu löschen. Anders als im Falle des Löschbegehrens nach einem Widerspruch gem. Art. 17 Abs. 1 lit. c) Alt. 1 DSGVO hängt im Falle des Löschbegehrens nach dem Widerruf einer Einwilligung die Löschpflicht nicht davon ab, ob vorrangige berechtigte Gründe der Löschung entgegenstehen.

Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um andere Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass ein Betroffener von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat (Art. 17 Abs. 2 DSGVO). Im Zusammenhang mit dieser Regelung hat der Europäische Gerichtshof sich in einem aktuellen Urteil mit dem Umfang der Lösch- und Informationspflicht für den Fall beschäftigt, dass sich verschiedene Verantwortliche auf eine einheitliche Einwilligung stützen (EuGH, Urt. v. 27.10.2022 – Az. C-129/21).

In dem der Entscheidung zugrunde liegenden Fall hatte Telenet, ein belgischer Telefondienstanbieter, Kontaktdaten seiner Teilnehmer an Anbieter von Teilnehmerverzeichnissen, darunter der Anbieter Proximus, weitergegeben. Proximus bietet Teilnehmerverzeichnisse und Telefonauskunftsdienste an, die den Namen, die Adresse und die Telefonnummer der Teilnehmer der verschiedenen Anbieter öffentlich zugänglicher Telefondienste enthalten. Proximus leitet die Kontaktdaten auch an einen anderen Anbieter von Teilnehmerverzeichnissen weiter.

Einer der Teilnehmer forderte Proximus auf, seine Kontaktdaten in dessen und von Dritten herausgegebenen Teilnehmerverzeichnissen nicht aufzuführen. Proximus änderte daraufhin den Status des Teilnehmers dahingehend, dass dessen Kontaktdaten nicht mehr zu veröffentlichen waren. In der Folge erhielt Proximus jedoch von Telenet eine Aktualisierung der Daten des fraglichen Teilnehmers, in der die Daten als „nicht vertraulich" ausgewiesen waren. Die Daten wurden von Proximus nach einem automatisierten Verfahren dergestalt registriert, dass sie erneut in den Teilnehmerverzeichnissen erschienen.

Auf die Beschwerde des Teilnehmers hin verhängte die belgische Datenschutzbehörde gegen Proximus ein Bußgeld in Höhe von 20.000 Euro. Gegen die Entscheidung der Behörde legte Proximus beim Appellationshof Brüssel, der im weiteren Verlauf des Verfahrens dem EuGH verschiedene Fragen zur Klärung vorlegte, ein Rechtsmittel ein.

Der EuGH entschied, dass für die Veröffentlichung von personenbezogenen Daten in einem öffentlichen Teilnehmerverzeichnis die Einwilligung des Teilnehmers erforderlich sei. Diese erstrecke sich auf jede weitere Verarbeitung der Daten durch dritte Unternehmen, die auf dem Markt für öffentlich zugängliche Telefonauskunftsdienste und Teilnehmerverzeichnisse tätig sind, sofern diese Verarbeitung denselben Zweck verfolge. Die Einwilligung setze nicht voraus, dass der Betroffene zum Zeitpunkt ihrer Erteilung die Identität aller Anbieter von Verzeichnissen, die seine personenbezogenen Daten verarbeiten werden, kenne. Die Teilnehmer müssten aber die Möglichkeit haben, die Löschung ihrer personenbezogenen Daten aus den Teilnehmerverzeichnissen zu erwirken. Der EuGH bestätigt diesbezüglich, dass ein Verantwortlicher wie Proximus geeignete technische und organisatorische Maßnahmen ergreifen müsse, um die anderen Anbieter von Teilnehmerverzeichnissen, denen er Daten geliefert habe, über den Widerruf der Einwilligung des Betroffenen zu informieren. Ein solcher Verantwortlicher müsse außerdem den Telefondienstanbieter, der ihm die personenbezogenen Daten übermittelt habe, informieren, damit dieser die zu übermittelnde Liste der personenbezogenen Daten anpasse. Wenn sich nämlich verschiedene Verantwortliche auf eine einheitliche Einwilligung des Betroffenen stützen, genüge es, dass sich der Betroffene für den Widerruf seiner Einwilligung an irgendeinen der Verantwortlichen wende. Der EuGH entschied außerdem, dass ein Verantwortlicher angemessene Maßnahmen zu treffen habe, um Suchmaschinenanbieter über den bei ihm eingegangenen Antrag des Teilnehmers eines Telefondienstanbieters auf Löschung seiner personenbezogenen Daten zu informieren.

Die Entscheidung des EuGH zeigt, dass für die Betroffenen die Ausübung ihres Rechts auf Löschung möglichst vereinfacht werden soll. Im Falle eines Löschbegehrens nach dem Widerruf einer Einwilligung haben Verantwortliche die Daten daher nicht nur bei sich selbst zu löschen, sondern unter Umständen auch weitere Verantwortliche hierüber zu informieren. Um Löschbegehren ordnungsgemäß nachzukommen, ist deshalb den verantwortlichen Stellen zu empfehlen, ein Konzept zum Umgang mit derartigen Anfragen zu erstellen, in dem vorab die praktische Vorgehensweise festgelegt wird. Angaben darüber, von wem personenbezogene Daten stammen und an wen diese weitergegeben wurden, sollten ordnungsgemäß dokumentiert werden, um den Umfang der Löschpflicht im Einzelfall mit geringem Zeitaufwand bestimmen zu können. Die entsprechende Dokumentation im Verzeichnis der Verarbeitungstätigkeiten kann hierbei hilfreich sein.

Johanna Schmale unterstützt Unternehmen bei der Einhaltung der datenschutzrechtlichen Anforderungen, unter anderem bezogen auf die Beantwortung von Betroffenenanfragen und die Erstellung von Löschkonzepten. Sie ist regelmäßig an der Prüfung und Beantwortung von Betroffenenanfragen hinsichtlich der Löschung von personenbezogenen Daten beteiligt.

Johanna Schmale
Wissenschaftliche Mitarbeiterin
johanna.schmale@brandi.net

Christina Prowald

Datenübermittlungen in die USA – Aktuelle und künftige Absicherungsmöglichkeiten

Vor allem die Zusammenarbeit mit amerikanischen Dienstleistern und Partnern ist für einen Großteil der Unternehmen trotz der mit internationalen Datentransfers einhergehenden datenschutzrechtlichen Schwierigkeiten nach wie vor von großer Relevanz. Im Rahmen der Umfrage „Datenschutz in der deutschen Wirtschaft: DSGVO & internationale Datentransfers“, die der Digitalverband Bitkom Ende September 2022 veröffentlichte, gaben fast zwei Drittel der befragten Unternehmen an, dass der Verzicht auf internationale Datenübermittlungen für sie gravierende negative Folgen hätte. Angeführt wurden hierbei vor allem Wettbewerbsnachteile, Lieferkettenprobleme sowie der Umstand, dass bestimmte Produkte und Dienstleistungen nicht mehr angeboten werden können und auch der globale Security-Support nicht mehr aufrecht erhalten werden kann. Die befragten Unternehmen machten insoweit deutlich, wie wichtig eine belastbare Rechtsgrundlage für internationale Datentransfers ist.

Während Datenübermittlungen in die USA in der Vergangenheit mehrheitlich auf das EU-US Privacy-Shield gestützt wurden, greifen nunmehr 91 % der Unternehmen zur Absicherung der Datentransfers auf den Abschluss von Standardvertragsklauseln zurück, die von der Europäischen Kommission zur Verfügung gestellt werden. Der Europäische Gerichtshof (EuGH) hatte das EU-US Privacy Shield in seinem Urteil „Schrems II“ (EuGH, Urt. v. 16.07.2020 – Az. C-311/18) im Juli 2020 für ungültig erklärt und darüber hinaus zusätzliche Anforderungen im Hinblick auf die Nutzung von Standardvertragsklauseln statuiert. Begründend führte der EuGH in seiner Entscheidung an, dass die USA nicht über ein den Standards innerhalb der EU entsprechendes Datenschutzniveau verfügen und die Grundrechte von EU-Bürgern nicht ausreichend geschützt werden; insbesondere die weitreichenden Zugriffsbefugnisse von amerikanischen Sicherheitsbehörden sowie der Mangel an wirksamen Rechtsbehelfen waren aus Sicht des EuGH problematisch. Als Reaktion auf das Urteil des EuGH veröffentlichte die EU-Kommission im Juni 2021 neue angepasste Standardvertragsklauseln, die nunmehr aus verschiedenen Klausel-Sets für die unterschiedlichen Verarbeitungssituationen bestehen.

Die neuen Standardvertragsklauseln tragen den Bedenken des EuGH Rechnung indem sie unter anderem konkrete Verhaltens-

pflichten für den Fall eines staatlichen Offenlegungsersuchens vorgeben (Klausel 15.1 und 15.2 der Standardvertragsklauseln). Weitergehenden Prüfpflichten hinsichtlich solcher Vorschriften des Drittstaates, die die Einhaltung der Standardvertragsklauseln und die Gewährleistung eines angemessenen Datenschutzniveaus konterkarieren könnten, können sich Unternehmen jedoch auch bei Abschluss der neuen Standardvertragsklauseln nicht entziehen (Klausel 14 der Standardvertragsklauseln). Um diesen Anforderungen gerecht werden zu können, bietet sich die Erstellung einer Folgenabschätzung für den internationalen Datentransfer (Transfer Impact Assessment), im Rahmen derer auch zusätzlich ergriffene Absicherungsmaßnahmen – wie etwa eine Verschlüsselung – abgebildet werden können, an.

Der Einsatz eines Dienstleisters mit amerikanischem Hintergrund kann unter bestimmten Voraussetzungen auch dadurch abgesichert werden, dass dieser ausdrücklich vertraglich zusichert, dass personenbezogene Daten nicht in Drittstaaten übermittelt, sondern ausschließlich innerhalb der EU bzw. des EWR verarbeitet werden (vgl. OLG Karlsruhe, Beschl. v. 07.09.2022 – Az. 15 Verg 8/22). Maßgeblich ist insoweit die Zusage, dass auch außerhalb der regelmäßigen Datenverarbeitung ein Zugriff auf die verarbeiteten Daten von außerhalb der EU bzw. des EWR nicht vorgesehen oder möglich ist. Die bloße Zusage eines europäischen Rechenzentrums oder Serverstandorts sowie der Verweis auf einen Firmensitz des Dienstleisters in der EU reichen hingegen gerade nicht aus.

Künftig könnten Datenübermittlungen in die USA auch mittels des geplanten „transatlantischen Datenschutzrahmens“ (Trans-Atlantic Data Privacy Framework“) abgesichert werden. Bereits im Frühjahr 2022 haben die Europäische Kommission und die USA eine grundsätzliche Einigung über einen solchen Rechtsrahmen, durch den insbesondere ein angemessener Schutz von in die USA übermittelten personenbezogenen Daten unter Berücksichtigung der Anforderungen des Urteils „Schrems II“ gewährleistet werden soll, erzielt. Die Regelungen sollen unter anderem strikte Vorgaben für den Zugriff von amerikanischen Sicherheitsbehörden auf Daten von Europäern sowie ein zweistufiges Rechtsbehelfssystem einschließlich eines speziellen Gerichts, mittels dessen sich EU-Bürger über vermeintlich rechtswidrige Zugriffe auf ihre Daten beschweren können, enthalten. Ein Datenzugriff soll nur noch dann zulässig sein, wenn dies zum Schutz der nationalen Sicherheit erforderlich ist. Darüber hinaus soll es strenge Vorgaben hinsichtlich der Verarbeitung von aus der EU übermittelten Daten, eine Verpflichtung zur Selbstzertifizierung mit Blick auf die vorgegebenen Grundsätze sowie verschiedene Überwachungs- und Überprüfungsmechanismen geben.

Am 7. Oktober 2022 hat US-Präsident Joe Biden nunmehr ein Dekret unterzeichnet, das auf amerikanischer Seite die rechtliche Grundlage für den transatlantischen Datenschutzrahmen schafft und die im März 2022 im Rahmen der Grundsatzvereinbarung angekündigten Verpflichtungen umsetzt. Im nächsten Schritt wird die Europäische Kommission einen Entwurf für einen Angemessenheitsbeschluss ausarbeiten und das Annahmeverfahren einleiten. Dabei erfolgt eine Überprüfung der vorgesehenen Maßnahmen unter Einbeziehung des Europäischen Datenschutzausschusses (EDSA), eines Ausschusses, der sich aus Vertretern der EU-Mitgliedstaaten zusammensetzt, und des Europäischen Parlaments. Erst nach Einholung aller Stellungnahmen wird die Europäische Kommission endgültig über einen Angemessenheitsbeschluss entscheiden. Ob es tatsächlich zu einem solchen Beschluss für die USA kommen und wie sich der EuGH zum geplanten Trans-Atlantic Data Privacy Framework positionieren wird, bleibt abzuwarten.

Bis dahin sollten Unternehmen in einem ersten Schritt überprüfen, ob sie direkt oder indirekt mit Anbietern aus den USA sowie Dienstleistern, bei denen eine Datenübermittlung in die USA erfolgt, zusammenarbeiten. Ist dies der Fall, empfiehlt es sich, die neuen Standardvertragsklauseln einzubeziehen, gegebenenfalls zusätzliche Absicherungsmaßnahmen zu ergreifen und sich im Rahmen der Vereinbarung zur Auftragsverarbeitung zumindest im Innenverhältnis haftungsrechtlich abzusichern. Es bietet sich zudem an, die ergriffenen Maßnahmen zur Absicherung der Datentransfers zu dokumentieren, um eine Auseinandersetzung mit dem Datenschutzniveau des Drittlandes i. S. v. Klausel 14 der Standardvertragsklauseln nachweisen zu können. Gerne unterstützten wir Sie bei der datenschutzkonformen Ausgestaltung der Prozesse.

Die Autorin unterstützt Unternehmen regelmäßig bei der Ausgestaltung und Absicherung der Zusammenarbeit mit (Drittstaaten-) Dienstleistern; sie hat gemeinsam mit Frau Dr. Schulte zudem auch den Fachbeitrag „Die neuen Standardvertragsklauseln – rechtskonforme Ausgestaltung internationaler Datentransfers?“ veröffentlicht (in: K&R 2021, S. 554-560).

Christina Prowald
Wissenschaftliche Mitarbeiterin
christina.prowald@brandi.net

Cristin Rösener

Datenschutzkonforme Nutzung von WhatsApp bei unternehmensinterner Nutzung

Der Messenger-Dienst WhatsApp von Meta erfreut sich weiterhin großer Beliebtheit als einfaches und schnelles Kommunikationsmittel in Unternehmen. Es gibt daher weiterhin eine Tendenz, dass Arbeitgeber gerne die interne Nutzung erlauben würden, aber teilweise datenschutzrechtliche Bedenken haben. Tatsächlich birgt WhatsApp auch ein hohes datenschutzrechtliches Risiko, da es relativ schwer ist, die Nutzung von WhatsApp zugleich datenschutzkonform und praktikabel zu gestalten.

Bei der Nutzung von WhatsApp zu betrieblichen Zwecken greift die datenschutzrechtliche Privilegierung der persönlichen Nutzung gem. Art. 3 Abs. 2 lit. c) DSGVO nicht ein. Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO für die betriebliche Nutzung ist vielmehr der Arbeitgeber, der auch dafür zu sorgen hat, dass die

sich auf dem Mobilgerät des Arbeitnehmers befindlichen personenbezogenen Daten datenschutzkonform verarbeitet werden. WhatsApp erfasst von den Nutzern personenbezogene Daten, wie Name und Telefonnummer und greift darüber hinaus automatisch auf alle Kontaktdaten des Mobilgerätes zu. Wenn auf dem Mobilgerät zugleich Mail-Programme installiert und synchronisiert sind, dann kann WhatsApp häufig hierdurch auf umfangreiche Kontaktdaten zugreifen und zwar einschließlich der Kontakte ohne eigene WhatsApp-Nutzung. Zwar wirbt WhatsApp mit einer Ende-zu-Ende-Verschlüsselung der Inhalte, dennoch können aber zumindest die Metadaten zu dem Kommunikationsverhalten von Meta ausgewertet werden. Problematisch ist insbesondere die Tatsache, dass die Daten möglicherweise an die WhatsApp-Server in den USA, also in ein Drittland übermittelt werden. Aufgrund dieses Drittlandbezuges ist es besonders wichtig, dass der Arbeitgeber als verantwortliche Stelle für eine angemessene Absicherung sorgt. In der Entscheidung „Schrems II" hat der Europäische Gerichtshof (EuGH) das EU-US-Privacy Shield zum Datenaustausch mit den USA für unwirksam erklärt mit der Folge, dass für die USA verlässlich kein hinreichendes Datenschutzniveau mehr garantiert werden kann (EuGH, Urt. v. 16.07.2020, Az. C-311/18, NJW 2020, 2613). Der EuGH hat dies vor allem damit begründet, dass US-Sicherheitsbehörden Zugriff auf durch US-Unternehmen gespeicherte Daten nehmen könnten.

Personenbezogene Daten dürfen aber nur aufgrund einer Rechtsgrundlage verarbeitet oder übermittelt werden, wobei bei einem Drittlandbezug zusätzliche Anforderungen erfüllt werden müssen. In der Regel liegt eine vertragliche Regelung im Unternehmen mit den einzelnen Arbeitnehmern als Rechtsgrundlage zur Nutzung von WhatsApp nicht vor. Die Rechtfertigung über eine Interessenabwägung gem. Art. 6 Abs. 1 lit. f) DSGVO scheidet im Regelfall aus, weil der konkrete Umfang der Nutzung auch von WhatsApp selbst nur schwer gerechtfertigt werden kann. Es ist insbesondere zu berücksichtigen, dass alle Kontakte selbst einen WhatsApp-Account besitzen und sie demnach mit der Auswertung ihrer Daten rechnen müssen. Im Rahmen einer Sorgerechtsstreitigkeit hat das AG Bad Hersfeld bereits vor fünf Jahren entschieden, dass, wer durch die Nutzung von WhatsApp die andauernde Datenweitergabe zulässt, ohne zuvor von den Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, gegenüber diesen Personen eine deliktische Handlung begeht und von den betroffenen Personen kostenpflichtig abgemahnt werden kann (AG Bad Hersfeld, Urt. v. 20.03.2017, Az. F 111/17, ZD 2017, 435 (451)). Der Nutzer von WhatsApp müsste demnach theoretisch von jedem seiner Kontakte auf seinem Mobilgerät die Einwilligung für die Datenübermittlung einholen. Praktisch ist diese Umsetzung für die unternehmensinterne Nutzung allerdings kaum realistisch. Für einen datenschutzkonformen Einsatz von WhatsApp kommt aber möglicherweise eine technische Umsetzung in Betracht, bei der die Datenweitergabe der Kontaktdaten an WhatsApp unterbunden wird. Da WhatsApp unmittelbar nach Aktivierung und Erst-Installation auf dem Mobilgerät automatisch das vollständige Adressbuch des Nutzers ausliest, muss der Zugriff spätestens mit der Installation technisch untersagt werden. Da WhatsApp in regelmäßigen Abschnitten auf die Kontaktdaten zugreift, muss auch anschließend sichergestellt sein, dass der Zugriff deaktiviert ist. Zu beachten ist, dass dadurch ein gewisser Komfort des Kommunikationsmittels verloren geht. Unter anderem ist das aktive Anschreiben der Kontakte aus dem Adressbuch nicht mehr möglich, so dass die Kommunikation durch den Partner initiiert werden muss. Technisch anspruchsvoller ist die Verwaltung mehrerer Adressbücher, bei denen nur die Daten aus einem Adressbuch mit WhatsApp synchronisiert werden. Durch derartige technische Maßnahmen und ein Mobile-Device-Management können Datenschutzverstöße verhindert und das Haftungsrisiko gesenkt werden.

Eine Nutzung von WhatsApp im Unternehmen zur internen Kommunikation ist dennoch nicht zu empfehlen. Eine datenschutzkonforme Nutzung ist bislang nur möglich, wenn die Datenweitergabe an WhatsApp ausgeschlossen wird. Dies hat jedoch zur Folge, dass gerade der Nutzungskomfort des Messenger-Dienstes erheblich eingeschränkt wird. Des Weiteren bedarf nach den Nutzungsbedingungen von WhatsApp eine nicht-private Nutzung eigentlich einer Genehmigung, jedenfalls soweit nicht explizit WhatsApp for Business genutzt wird. Eine Alternative könnten aber andere Messaging-Dienste sein, die nicht über zentrale Server eines kommerziellen Unternehmens wie Meta abgewickelt werden. Teilweise gibt es auch Anbieter für Intranet-Lösungen, über die ebenfalls eine schnelle und sichere Kommunikation möglich ist.

Die datenschutzkonforme Nutzung von WhatsApp innerhalb eines Unternehmens bleibt dagegen immer zumindest mit datenschutzrechtlichen Restrisiken verbunden, die sorgfältig geprüft werden sollten. Wenn in Kenntnis der Risiken eine Entscheidung für WhatsApp getroffen wird, sollte dies zumindest klar geregelt werden, auch bezogen auf die Rahmenbedingungen.

Cristin Rösener ist Wirtschaftsjuristin und unterstützt das Datenschutz-Team von BRANDI bei rechtlichen Fragestellungen, unter anderem auch zum Einsatz von WhatsApp in Unternehmen.

Hendrik Verst

Datenschutz im Intranet

Viele Unternehmen nutzen Intranet-Portale in ihrem Arbeitsalltag. Intranet-Anwendungen eignen sich besonders für den unternehmensinternen Informationsaustausch. Dieser interne Informationsaustausch ist gerade bei einer verstärkten Verlagerung von Arbeitstätigkeiten ins Home Office oder für Unternehmen mit unterschiedlichen Standorten von besonderer Wichtigkeit.

Neben der reinen Verteilung von internen Unternehmensinformationen gibt es vermehrt auch Anbieter, die Intranet-Anwendungen mit verschiedenen Interaktions-Funktionen – vergleichbar mit denjenigen der gängigen Social-Media-Plattformen – anbieten. Findet eine solche interaktive Kommunikation zwischen den Mitarbeitern statt, wird das Angebot teilweise auch als „Social Intranet" bezeichnet.

Da Intranet-Portale der internen Kommunikation sowie Informationsverteilung dienen und somit „lediglich" Daten der Mitarbeiter involviert sind, werden die datenschutzrechtlichen Vorgaben in diesem Zusammenhang teilweise nicht besonders intensiv geprüft. Es darf jedoch nicht außer Acht gelassen werden, dass die DSGVO und insbesondere auch das BDSG für personenbezogene Daten der Mitarbeiter einen besonderen Schutz statuieren. Beim Mitarbeiterdatenschutz gilt, wie im gesamten Datenschutzrecht, der Grundsatz des Verbots mit Erlaubnisvor-

behalt. Eine Datenverarbeitung ist grundsätzlich untersagt, außer sie ist aufgrund einer Rechtsgrundlage ausdrücklich erlaubt. Erforderlich ist daher auch bei internen Angeboten immer eine Prüfung, auf welcher rechtlichen Grundlage die Datenverarbeitung stattfinden soll. Wird das Intranet-Portal von einem Dienstleister zur Verfügung gestellt, sollte zur datenschutzrechtlichen Absicherung eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO abgeschlossen werden.

1. Technische Ausgestaltung des Intranets

Bei der technischen Ausgestaltung des Intranets sollten grundsätzlich dieselben Maßgaben beachtet werden wie bei einer üblichen Internetseite. Auf dem Portal sind dementsprechend gem. Art. 13 DSGVO Datenschutzhinweise zu hinterlegen, die die Nutzer über die auf dem Portal stattfindende Datenverarbeitung informieren. Ein Impressum kann dagegen entbehrlich sein, wenn das Intranet außerhalb des Unternehmens gar nicht erreichbar ist und demnach keine Außenwirkung entfaltet (Ott in Gersdorf/Paal, BeckOK Informations- und Medienrecht, § 5 TMG Rn. 9).

Die Datenübertragung sollte wie bei einer Internetseite grundsätzlich verschlüsselt erfolgen, idealerweise über eine TLS-Verschlüsselung. Werden auf der Seite Cookies oder anderweitige Technologien zur Analyse des Nutzerverhaltens eingesetzt, sollte auch hier – wie auf Internetseiten – die aktive Einwilligung der Nutzer nach Art. 6 Abs. 1 lit. a) DSGVO eingeholt werden.

2. Datenverarbeitung im Zusammenhang mit der Nutzung des Intranets

Ist das Intranet so gestaltet, dass die wesentlichen internen Informationen durch die Mitarbeiter auch ohne vorherige Registrierung einsehbar sind, ist eine ausdrückliche Einwilligung der Nutzer nicht erforderlich. Die dazugehörige Datenverarbeitung, etwa die Erfassung technischer Daten bei dem Besuch des Intranets über den Arbeits-PC, kann sodann auf die berechtigten Interessen des Unternehmens an einer bestmöglichen Informationsübermittlung und einer strukturierten Kommunikation im Unternehmen erfolgen.

Müssen sich die Mitarbeiter hingegen zwingend registrieren, um Informationen einsehen zu können, ist zu unterscheiden, ob die Registrierung mit den geschäftlichen Kontaktdaten der Mitarbeiter erfolgt oder ob die privaten Kontaktdaten, wie die private E-Mail-Adresse, hierzu verwendet werden. Werden lediglich geschäftliche Daten abgefragt, kann argumentiert werden, dass die Datenverarbeitung nach § 26 BDSG zur Durchführung des Arbeitsverhältnisses erforderlich ist, bzw. dass die Datenverarbeitung dem berechtigten Interesse an einer bestmöglichen Informationsübermittlung und einer strukturierten Kommunikation nach Art. 6 Abs. 1 lit. f) DSGVO dient.

Werden bei der Registrierung jedoch zusätzliche persönliche Daten abgefragt, muss zuvor zwingend eine ausdrückliche Einwilligung der Mitarbeiter eingeholt werden. Die datenschutzrechtlichen Vorgaben sehen im Rahmen eines Beschäftigungsverhältnisses erhöhte Anforderungen an die Freiwilligkeit der Einwilligung vor, da das Arbeitsverhältnis von einem besonderen Über- und Unterordnungsverhältnis von Arbeitgeber und Arbeitnehmer gekennzeichnet ist. Für die Freiwilligkeit im Beschäftigungsverhältnis kommt es entscheidend darauf an, ob den Arbeitnehmer im Falle der Verweigerung der Einwilligung negative Folgen treffen. Es sollte in diesem Zusammenhang sichergestellt werden, dass im Falle der Abfrage persönlicher Kontaktdaten notwendige interne Informationen auch ohne Registrierung zum Intranet zugänglich gemacht werden. Hierzu könnte es sich insbesondere anbieten, wichtige Informationen weiterhin auf einem zentralen „Schwarzen Brett" zu veröffentlichen und dies den Mitarbeitern vor der Registrierung auch transparent mitzuteilen.

3. Nutzungsrichtlinien

Die Art und Weise der Intranet-Nutzung kann den Mitarbeitern durch eine Nutzungsrichtlinie vorgegeben werden.

Sofern die Mitarbeiter im Intranet auch miteinander interagieren und kommunizieren können, sollte die Kommunikation beispielsweise lediglich unter Klarnamen erfolgen und das Teilen strafbarer Inhalte oder die Nutzung einer beleidigenden Sprache untersagt werden. Es sollte weiterhin klargestellt werden, dass sensible Informationen wie Geschäfts- oder Betriebsgeheimnisse nicht geteilt werden dürfen. Die Mitarbeiter sind anzuhalten, auch bei der Nutzung der Plattform das Datengeheimnis zu wahren. Hilfreich ist schließlich der Hinweis, dass die Kommunikation grundsätzlich dienstlichen Zwecken dienen und die Nutzung des Intranets auf einen Umfang begrenzt soll sein, der die Arbeitsleistung nicht beeinträchtigt.

4. Fazit

Mit den Anbietern von Intranet-Plattformen sollte eine Vereinbarung zur Auftragsverarbeitung abgeschlossen werden. Beim Intranet sind grundsätzlich dieselben technischen und gestalterischen Vorgaben zu beachten, wie bei üblichen Internetauftritten, abgesehen von dem Erfordernis eines Impressums.

Sofern die Mitarbeiter im Rahmen der Registrierung persönliche Daten angeben müssen, sollte dies lediglich mit freiwilliger Einwilligung geschehen. Für die Freiwilligkeit ist dabei wichtig, dass die wichtigsten internen Informationen auch ohne Registrierung zum Intranet einsehbar sind. Die wesentlichen Eckpunkte der Nutzung des Intranets können zusätzlich durch eine Richtlinie vorgegeben werden, sodass stets eine rechtskonforme und respektvolle Kommunikation der Mitarbeiter untereinander stattfindet und dass die Nutzung des Portals zu keiner Beeinträchtigung der vertraglich geschuldeten Arbeitsleistung führt.

Der Autor berät Mandanten regelmäßig zu der Nutzung von Intranet-Portalen. Er begleitet sie ebenfalls bei den nötigen Vorkehrungen, wie dem Abschluss von Auftragsverarbeitungsvereinbarungen oder der Erstellung von Nutzungsrichtlinien.

Hendrik Verst
Wissenschaftlicher Mitarbeiter
hendrik.verst@brandi.net

Eva Ritterswürden

Bußgelder: Persönliches Verschulden als Voraussetzung für einen Bußgeldbescheid?

Seit Inkrafttreten der DSGVO haben die Datenschutzbehörden der EU-Mitgliedstaaten bereits sehr hohe Bußgelder gegen zahlreiche Unternehmen aufgrund von Datenschutzverstößen verhängt. Die irische Behörde hat beispielsweise im September 2022 ein Bußgeld in Höhe von 405 Mio. Euro gegen Meta Platforms wegen der rechtswidrigen Veröffentlichung personenbezogener Daten Minderjähriger bei Instagram verhängt. Die deutschen Aufsichtsbehörden verhängen ebenfalls vermehrt Bußgelder aufgrund von Datenschutzverstößen. Zuletzt hat insoweit etwa die Landesbeauftragte für den Datenschutz in Niedersachen ein Bußgeld in Höhe von 900.000 Euro gegen ein Kreditinstitut verhängt, weil umfangreiche Kundenprofile ohne ausreichende Rechtsgrundlage erstellt und genutzt wurden. Nicht in allen Fällen kann im Unternehmen jedoch eine konkrete Person identifiziert werden, die sich nachweislich fehlerhaft verhalten hat. In solchen Konstellationen stellt sich die Frage, ob das Unternehmen selbst Adressat eines Bußgeldbescheides sein kann, ohne dass der Verschuldensvorwurf ein bestimmtes Organ trifft. Eine juristische Person kann naturgemäß unmittelbar keine Ordnungswidrigkeit begehen, es bedarf stets der Handlung einer natürlichen Person. Nach deutschem Recht erfolgt eine Haftung des Unternehmens dann alleine über Fragen der Zurechnung. Zentrale Zurechnungsnorm für die Haftung des Unternehmens ist § 30 OWiG.

Nach einem Vorlagebeschluss durch das Kammergericht in Berlin (Beschl. v. 06.12.2021 – 3 Ws 250/21) muss sich jetzt der EuGH mit der Frage befassen, inwieweit es für die Verhängung von Bußgeldern erforderlich ist, dass ein Datenschutzverstoß durch konkrete Mitarbeiter vorliegt und nachgewiesen werden kann. Ursprünglich wurde im Oktober 2019 gegen die Deutsche Wohnen SE ein Bußgeld in Höhe von 14,5 Millionen Euro verhängt. Aufgrund „gravierender Mängel“ wurde der Bußgeldbescheid vom LG Berlin aufgehoben (Beschl. v. 18.02.2021 – 212 Js-OWi 1/20) und das Verfahren wurde eingestellt. Die Staatsanwaltschaft ging gegen die Entscheidung des LG Berlin vor, woraufhin das Kammergericht Berlin in zweiter Instanz mit dem Fall befasst wurde, das sich zur Klärung an den EuGH wandte.

Unter Berücksichtigung des Wortlauts der DSGVO ergibt sich aus Art. 83 DSGVO die Haftung des „Verantwortlichen“ für jegliche Verstöße gegen die Verordnung. Verantwortlicher ist in den meisten Fällen ein Unternehmen, welches bei Formulierung der DSGVO auch bekannt war. Die DSGVO ließe sich daher so auslegen, dass nach europäischem Recht juristische Personen sehr wohl direkte Adressaten eines Bußgeldbescheides sein und unmittelbar haften können (Funktionsträgerprinzip). Hier würde sich deutlich eine Diskrepanz zwischen dem europäischen Datenschutzrecht und dem deutschen Ordnungswidrigkeitenrecht ergeben. Da einzelne Mitgliedstaaten keine abweichenden Vorgaben treffen dürfen, stellt sich die Frage, ob aufgrund der Vorgaben der DSGVO zwingend auch europaweit eine Harmonisierung der Sanktionierungspraxis erfolgen muss. Würde der EuGH sich für eine unmittelbare Haftung von Unternehmen entscheiden, dürfte mit einem weiteren Anstieg der Bußgeldbescheide aufgrund von Datenschutzverstößen in Deutschland auszugehen sein. Je nach Gesellschaftsform des Unternehmens käme zudem oftmals eine persönliche Haftung von Leitungsorganen in Betracht. Der EuGH müsste als Folgefrage entscheiden, ob ein schuldhaftes Verhalten generell erforderlich ist oder ob ein objektiver Verstoß gegen die DSGVO für einen Bußgeldbescheid ausreichend wäre. Im deutschen Recht käme der Rechtsanwender hier auf eine eindeutige Antwort; Unternehmen haften nach dem in § 30 OWiG verankerten Rechtsträgerprinzip nur, wenn ihre Organe vorsätzlich oder fahrlässig gehandelt haben. Mit Blick in die DSGVO ist diese Auslegung der Verordnung durch den EuGH allerdings eher unwahrscheinlich. Es bestehen in der Verordnung keine Anhaltspunkte, dass ein Verstoß tatsächlich schuldhaft sein muss.

Für die Praxis wird die Entscheidung des EuGH einen erheblichen Einfluss darauf haben, wie gewissenhaft zukünftig datenschutzrechtliche Standardthemen und generell Compliance-Maßnahmen in Unternehmen behandelt werden. Kommt es auf einen rein objektiven Datenschutzvorfall ohne jeglichen Personenbezug an, wird die potentielle Zahl an Bußgeldverfahren massiv steigen. Um dem vorzubeugen, ist eine intensive Sensibilisierung aller Mitarbeiter für den Bereich Datenschutz des Unternehmens erforderlich. Die sorgfältige und regelmäßige Pflege von datenschutzrechtlichen Dokumentationen wird aufgrund der Rechenschaftspflicht der DSGVO ein noch größeres Thema als bislang darstellen. Um Bußgelder möglichst gering zu halten oder gar ein Verfahren zu verhindern, muss bewiesen werden, jedenfalls das Bestmögliche getan zu haben, einen Datenschutzvorfall zu verhindern. Je intensiver und ernster das Thema Datenschutz im Unternehmen behandelt wird und je besser die Bemühungen dokumentiert sind, desto eher wird die Aufsichtsbehörde im Rahmen ihres Ermessens davon absehen, abschreckend hohe Bußgelder festzusetzen. Welche Maßnahmen im Einzelfall geboten sind, ist dabei regelmäßig eine Frage des Einzelfalls und sollte nach entsprechender Beratung individuell festgelegt werden.

Die Autorin berät regelmäßig Mandanten im Umgang mit datenschutzrechtlichen Fragen und betreut auch die regelmäßige Pflege der datenschutzrechtlichen Dokumentation in Unternehmen, um das Datenschutzniveau konstant zu halten bzw. zu verbessern und Datenschutzvorfällen vorzubeugen.

Eva Ritterswürden
Wissenschaftliche Mitarbeiterin
eva.ritterswuerden@brandi.net

WEIHNACHTSGESCHENKE EINMAL ANDERS

Wir freuen uns sehr, dass das gesamte BRANDI Team seine Weihnachtsgeschenke in Form von Geldspenden Kindern in drei regionalen Organisationen gespendet hat.
Wir sagen danke an das gesamte BRANDI Team.

DAS SIND DIE VEREINE:

KARLSSON E. V.

Der Verein hat sich seinen Namensgeber zum Vorbild genommen. Ihm ist es ein großes Anliegen, Kindern, die an den Rand der Gesellschaft gerückt sind, eine Freude zu machen. Sie sollen erfahren, dass sie besonders sind – genau wie jedes andere Kind auch. Außerdem will der Verein den betroffenen Kindern und ihren Familien »ein guter Freund« sein. Bei ihm finden sie Vertrauen, Hilfe, Rat – und nicht zu vergessen: auch ganz viel Spaß.

Denn es ist eine besondere Herzensangelegenheit, Kinder ein Stück vom Rand in die »Mitte« der Gesellschaft zu holen. Die Philosophie des Vereins hat unser BRANDI Team überzeugt.

https://karlsson-ev.de

DAS SOS-KINDERDORF LIPPE

setzt sich seit über 50 Jahren für die Belange von Kindern und Jugendlichen, jungen Erwachsenen sowie deren Familien ein. Im Jahr 2016 wurden die beiden Einrichtungen SOS-Kinderdorf Lippe und SOS-Kinderdorf Detmold zum „SOS-Kinderdorf Lippe“ zusammengeführt. Aufgabe der entstandenen Verbundeinrichtung ist es, Kindern, Jugendlichen, jungen Erwachsenen und ihren Familien mit unterschiedlichen Problemstellungen ein differenziertes Hilfs- und Unterstützungsangebot anzubieten.

https://www.sos-kinderdorf.de

DAS KINDER-UND JUGENDHEIM LIMMER

Die Einrichtung reagiert auf gesellschaftlich veränderte Bedingungen der Kinder, Jugendlichen, jungen Erwachsenen und deren Familien durch ein differenziertes pädagogisches Angebot. Die Atmosphäre des Kinderheims kann als familiär, zugewandt und beschützend beschrieben werden und stellt die Grundlage für die Anforderungen an eine moderne und aktuelle Jugendhilfeeinrichtung dar.

https://www.kinderheim-limmer.de

Dr. Laura Schulte

Datenschutzrechtliche Herausforderungen für den Einsatz von KI-basierter Software im Recruiting-Prozess

Die Gewinnung neuer Talente stellt sich für viele Unternehmen als Herausforderung dar. Dies liegt nicht nur am vielfach beklagten Fachkräftemangel, sondern teilweise auch an bisweilen komplexen Informationsverwaltungsvorgängen im Bewerbungsprozess selbst. Schließlich werden für viele Unternehmen die sog. Soft Skills von Mitarbeitenden zunehmend wichtiger. Wie sollen diese aber im Auswahlprozess valide und dennoch mit vertretbarem Aufwand eingeschätzt werden?

Angesichts dieser Ausgangslage fragen sich viele Unternehmen, ob ihre Personalbeschaffungsprozesse durch KI-basierte Softwareanwendungen effektiviert werden können. Angestrebt wird hierbei neben einer allgemeinen Zeit- und Kostenersparnis auch die Verbesserung der eigentlichen Auswahlentscheidung. Bereits heute können sämtliche Phasen des Recruiting-Prozesses – zumindest theoretisch – durch KI-basierte Software unterstützt werden. So existieren beispielsweise Produkte, die Stellenprofile automatisch generieren, Karrierenetzwerke auf der Suche nach passenden Kandidatinnen auswerten, Stellenanzeigen generieren und veröffentlichen, Chatbots, die Jobinterviews führen und Anwendungen, die eine Vorauswahl im Hinblick auf eingehende Bewerbungen treffen können. Diese Produkte stammen nicht nur von US-amerikanischen Anbietern, sondern auch von nationalen Unternehmen. Unabhängig von der Herkunft der Produkte stellen sich allerdings die Fragen, ob diese den geltenden datenschutzrechtlichen Anforderungen gerecht werden und was bei ihrer Anwendung zu berücksichtigen ist.

Rechtmäßigkeitsgrundsatz

Jede (teilweise) automatisierte Verarbeitung personenbezogener Daten bedarf einer Rechtfertigung – unabhängig davon, ob insoweit künstliche Intelligenz zum Zuge kommt. Die Erfüllung dieser grundlegenden datenschutzrechtlichen Anforderungen stellt bereits viele Arbeitgeber vor allem in Bewerbungsprozessen vor Herausforderungen. In der Praxis werden hier vielfach zwei Rechtfertigungsgründe relevant: Die Einwilligung der Bewerber und die Erforderlichkeit der Datenverarbeitung für die Begründung des Beschäftigtenverhältnisses.

Die Einholung wirksamer Einwilligungen von Jobkandidatinnen stellt sich allerdings als äußerst schwierig dar. Denn eine Einwilligung kann nur dann legitimierende Wirkung entfalten, wenn diese – neben weiteren Voraussetzungen – freiwillig erteilt wird. Möchte eine Jobkandidatin eine Position in einem Unternehmen unbedingt erhalten und macht das Unternehmen die Einstellungsentscheidung beispielsweise von dem Ergebnis einer KI-basierten Stimmanalyse im Rahmen eines Jobinterviews abhängig, wird die Bewerberin keine echte Wahl haben im Hinblick auf die Erteilung ihrer Einwilligung in die Verarbeitung ihrer Daten durch Software. Die Drucksituation, in der sich Bewerber befinden, wird vielfach die Freiwilligkeit ihrer Einwilligungen ausschließen. Etwas anders kann regelmäßig nur dann gelten, wenn den Bewerbern eine echte Alternative offensteht, die sich nicht negativ auf ihre Einstellungschancen auswirkt. Sollte das Unternehmen allerdings wirklich eine Alternative zu der Datenverarbeitung durch die KI-basierte Software einrichten, könnten gerade die erhofften Effektivitätseffekte gemindert werden und es stellt sich außerdem die Frage nach der Vergleichbarkeit der Datengrundlage für die Einstellungsentscheidung.

Weiterhin könnten Datenverarbeitungsprozesse im Kontext von Bewerbungsverfahren gesetzlich gerechtfertigt sein, wenn diese für die Begründung eines Beschäftigtenverhältnisses erforderlich sind. Ob die Datenverarbeitung im Rahmen einer KI-basierten Anwendung erforderlich ist, ist im Rahmen einer dreischrittigen Prüfung zu ermitteln. Zunächst müsste die Datenverarbeitung geeignet sein, den Zweck des Arbeitgebers zu erfüllen. Der Zweck besteht vorliegend in der Effektivierung des Bewerbungsverfahrens bzw. der Ermittlung des am besten geeigneten Kandidaten für eine offene Position. Die Förderungen dieser Zwecke durch das Software-Tool müsste empirisch belegt sein. Einige bereits auf dem Markt befindlichen KI-basierten Softwareprodukte sind in der Vergangenheit allerdings als fehleranfällig negativ aufgefallen. Auch gilt es auf dieser Prüfungsstufe bereits etwaige Diskriminierungseffekte der Softwareprodukte zu adressieren.

In einem zweiten Schritt müsste die Datenverarbeitung durch das Softwareprodukt erforderlich sein. Erforderlich meint in diesem Kontext, dass kein gleich geeignetes, aber gleichzeitig den Bewerber weniger belastendes Mittel im Verhältnis zur KI-basierten Datenverarbeitung besteht. Insoweit müsste der Arbeitgeber nachweisen, dass beispielsweise eine KI-basierte Stimmenanalyse effektiver und für den Bewerber weniger belastend ist als etwa die Durchführung eines Assessment-Centers bzw. einer nicht-automatisierten psychologischen Untersuchung. Hier könnte grundsätzlich damit argumentiert werden, dass auch den Bewerbern selbst eine etwaige Zeitersparnis zugutekommt und diese ggf. eine automatische Analyse ihrer Eignung für die ausgeschriebene Stelle weniger belastend finden, als eine nicht-automatisierte psychologische Bewertung. Insgesamt sollte das insoweit bestehende Rechtfertigungserfordernis jedenfalls nicht unterschätzt werden und es darf angenommen werden, dass bei einer etwaigen gerichtlich bzw. aufsichtsbehördlichen Überprüfung des Einsatzes eines KI-basierten Software-Tools dieser Prüfungsschritt besondere Aufmerksamkeit erfährt.

Auf einer dritten und letzten Ebene dürfte der mit der Datenverarbeitung einhergehende Eingriff in die Rechte der Bewerber (Stichwort: informationelle Selbstbestimmung) nicht außer Verhältnis stehen zu dem mit der Datenverarbeitung durch den Arbeitgeber verfolgten Zwecken. Bei der Prüfung dieser Ebene kommt es insbesondere darauf an, welchen Umfang die konkret in Rede stehende Datenverarbeitung aufweist und welchen Eindruck diese auf die Bewerber macht. Wenn die Bewerber diese als besonders belastend empfinden (dürfen) und mit dem Einsatz des Software-Tools auch keine Zeit- und Kostenersparnis für die Bewerber verbunden ist, dürfte eine Interessenabwägung vielfach zu Lasten der Abreitgeber ausfallen, was im Ergebnis bedeutet, dass die Datenverarbeitung im Rahmen des Tools nicht durch Zwecke des Beschäftigtenverhältnisses gerechtfertigt werden kann.

(Keine) automatisierte Einzelentscheidung

Im Datenschutzrecht gilt der Grundsatz, dass automatisierte Einzelentscheidungen grundsätzlich verboten sind. Hierdurch soll verhindert werden, dass Menschen mit rechtlich relevanten Entscheidungen konfrontiert werden, die ausschließlich durch eine Maschine bzw. eine KI-basierte Software getroffen werden.

Aufgrund dieser Wertentscheidung ist es damit verhältnismäßig eindeutig ausgeschlossen, dass die Entscheidung über den Abschluss eines Arbeitsvertrages ausschließlich durch eine KI-basierte Software getroffen wird. Demgegenüber kann es wohl zulässig sein, wenn eine KI-basierte Software eine Vorauswahl von Bewerbern trifft, die wiederum zu einem Bewerbungsgespräch eingeladen werden. Voraussetzung hierfür dürfte allerdings sein, dass aufgrund der großen Masse an eingehenden Bewerbungen die Durchführung des Bewerbungsverfahrens dem Arbeitgeber ansonsten schlicht nicht möglich bzw. zumutbar wäre. Hier können der Sache nach einige Parallelen zu den rechtlichen Anforderungen an das algorithmusbasierte Kredit-Scoring gezogen werden. Allerdings ist auch im Zusammenhang mit diesem datenschutzrechtlichen Grundsatz die besondere Schutzwürdigkeit von Bewerbern aufgrund einer vermuteten wirtschaftlichen Abhängigkeit zu berücksichtigen.

Schließlich müsste der Arbeitgeber im Hinblick auf eine KI-basierte Vorauswahl von Bewerbern besondere Schutzmaßnahmen treffen, insbesondere im Hinblick auf die Verarbeitung besonders schutzwürdiger Informationen, wie z. B. Gesundheitsdaten und religiöse Überzeugungen, die regelmäßig Gegenstand von Bewerbungsunterlagen sein können. Als Richtlinie lässt sich formulieren, dass je eher eine KI-basierte Software lediglich die Auswahlentscheidung des Arbeitgebers vorbereitet, davon ausgegangen werden kann, dass diese auch keine ausschließliche automatisierte Einzelentscheidung im Sinne des Datenschutzrechts trifft.

Transparenz

Soweit Unternehmen KI-basierte Software in ihre Recruiting-Prozesse einbinden wollen und hierbei auch personenbezogene Daten verarbeitet werden, müssen die transparenzrechtlichen Vorgaben des Datenschutzrechts gewahrt werden. Im Ergebnis muss den Bewerbern hinreichend transparent kommuniziert werden, welche ihrer Daten, auf welche Weise und mit welchen Konsequenzen für sie durch die KI-basierte Software verarbeitet werden. Dies setzt wiederum voraus, dass Unternehmen selbst über ein grundlegendes Verständnis der von ihnen eingesetzten KI-basierten Software verfügen. Anbieter entsprechender Softwareprodukte werden demgegenüber tendenziell nur höchst ungern die Mechanismen bzw. Algorithmen, auf denen ihre Softwareprodukte basieren, ihren Kunden gegenüber offenlegen. Schließlich handelt es sich bei diesen um eines ihrer zentralsten Geschäfts-Assists und werden diese regelmäßig Fragen nach der Funktionslogik ihrer Softwareprodukte mit dem Verweis auf ihr Geschäftsgeheimnis weitgehend unbeantwortet lassen. Im Ergebnis sollte vor der Lizenzierung von KI-basierten Softwareprodukten mit deren Anbietern diskutiert und auch vertraglich abgesichert werden, wie datenschutzrechtliche Informationspflichten erfüllt werden können.

KI-Verordnung

Im April 2022 hat die Europäische Kommission den Entwurf einer KI-Verordnung veröffentlicht. Nach diesem Entwurf werden KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl von Bewerbern verwendet werden sollen, etwa für die Bekanntmachung freier Stellen, das Filtern von Bewerbungen und das Bewerten von Bewerbern in Vorstellungsgesprächen, als sog. Hochrisiko-KI kategorisiert. Mit dieser Kategorisierung als Hochrisiko-KI sollen künftig sowohl für die Betreiber entsprechender KI-Systeme als auch für den Einsatz derselben durch Unternehmen erhöhte rechtliche Anforderungen einhergehen. Zu diesen Anforderungen zählt nach dem derzeitigen Stand des Entwurfs etwa, dass die Trainingsdaten, mit denen die KI arbeitet, bestimmte Qualitätsanforderungen erfüllen müssen. Außerdem sollen solche KI-Systeme regelmäßig getestet werden. Darüber hinaus müssen die Betreiber von Hochrisiko-KI-Systemen verschiedene Protokollierungs- und Transparenzpflichten erfüllen. Auch wenn die konkrete Ausgestaltung der rechtlichen Vorgaben für den Einsatz von KI-basierten Softwaresystemen in Recruiting-Prozessen aufgrund des derzeitigen Standes des Gesetzgebungsverfahrens noch nicht abschließend beurteilt werden kann, ist davon auszugehen, dass die KI-Verordnung künftig mehr Rechtssicherheit schaffen wird für den Einsatz KI-basierter Software. Andererseits ist zu vermuten, dass die neue Regulierung einen Wettbewerbsnachteil für europäische Unternehmen im Verhältnis zur internationalen Konkurrenz begründen kann.

Fazit

Im Ergebnis kommt es bei der datenschutzrechtlichen Bewertung von KI-basierten Softwareanwendungen, die im Recruiting-Prozess Anwendung finden sollen, auf den Einzelfall an, eine pauschale Bewertung ist hier also nicht möglich. Jedenfalls setzt die datenschutzrechtliche Bewertung des jeweiligen Softwareprodukts ein grundsätzliches Verständnis der Funktionsweise desselben voraus. Allgemein ist außerdem darauf zu achten, dass Diskriminierungseffekte, die mit der KI einhergehen können, adressiert werden. Weiterhin ist kritisch zu hinterfragen, ob der Einsatz der KI tatsächlich datenschutzrechtlich gerechtfertigt werden kann und auch für die betroffenen Bewerber hinreichend transparent ausgestaltet ist. Auswahlentscheidungen dürften durch KI-basierte Anwendungen lediglich vorbereitet, nicht aber final getroffen werden. Schließlich sind die Entwicklungen auf europäischer Ebene im Hinblick auf die KI-Verordnung zu beobachten.

Dr. Laura Schulte
Rechtsanwältin
laura.schulte@brandi.net

Dr. Daniel Wittig

Zuwachs in der EVB-IT Familie – die EVB-IT Cloud sind da

Cloud-Lösungen prägen immer mehr das Leistungsangebot von IT-Unternehmen und sind unverzichtbarer Bestandteil der fortschreitenden Digitalisierung unserer Gesellschaft. Dies gilt auch für die öffentliche Hand. Diese sehnte daher bereits lange die Erstellung und Veröffentlichung der EVB-IT Cloud herbei.

Am 01.03.2022 war es nunmehr soweit. Die EVB-IT Cloud wurden auf der Homepage des CIO des Bundes zur Verfügung gestellt. So wurde ein wichtiger Meilenstein für IT-Beschaffungen der öffentlichen Hand erreicht.

Hintergrund

Bei der Beschaffung von IT-Leistungen durch die öffentliche Hand gehören die EVB-IT Verträge zum Standardrepertoire. Diese haben sich als Musterunterlagen in zahlreichen IT-Beschaffungen seit nunmehr über 20 Jahren bewährt. Die EVB-IT Vertragsmuster werden dabei von der Arbeitsgruppe EVB-IT, welche vom Bundesministerium des Inneren und für Heimat (BMI) geleitet wird, und dem Bitkom e. V., als Vertreter der IT-Wirtschaft, verhandelt. Sie stellen somit deutschlandweit etablierte Musterverträge dar, die auf breiter Basis anerkannt werden. Auch wenn sie teilweise als Kompromiss zu betrachten sind, gewährleisten sie in der IT-Beschaffung die Einhaltung einer Mindestqualität von vertraglichen Inhalten, die die öffentliche Hand absichert, aber auch die Bieter zu schätzen wissen. Große Teile der öffentlichen Hand sind sogar zur Verwendung der EVB-IT verpflichtet (z. B. gemäß Ziff. 4.3 der Verwaltungsvorschrift zu § 55 BHO).

In den letzten Jahren haben sich Cloud-Lösungen in der Privatwirtschaft weitgehend fest etabliert, wohingegen im öffentlichen Sektor eine gewisse Zurückhaltung zu beobachten war. Auch im öffentlichen Sektor erkannte man zwar die mannigfaltigen Vorteile von Cloud-Lösungen (wie z. B. Flexibilität, Skalierbarkeit von Ressourcen und Services, Zugriff auf fremde Rechenleistungen und Speicherplätze, geringere Kosten etc.), gleichzeitig wurde aber auch stets ein Kontroll- und Zugriffsverlust bezüglich der Daten befürchtet und Vorbehalte wegen Datenschutz und IT-Sicherheit geschürt. Hinzu kam, dass viele Beschaffer der öffentlichen Hand kaum Erfahrung mit Cloud-Lösungen vorweisen konnten, gleichzeitig aber eine hohe Expertise bei deren Bezug erforderlich ist. Ohne die Möglichkeit auf Vorlagen zurückgreifen zu können, wurde die Beschaffung von IT-Leistungen der öffentlichen Hand erschwert und verzögert. Oftmals erfolgte die Beschaffung von Cloud-Lösungen durch eine umfangreiche und komplexe Umgestaltung und Erweiterung des EVB-IT Systemvertrages. Auch wir haben diese für viele unserer Mandanten vorgenommen. Andere Beschaffer wiederum verließen sich leichtfertig auf die Angebote oder Vorlagen der Bieter. Dieses Problem soll nun durch Veröffentlichung der EVB-IT Cloud gelöst bzw. vereinfacht werden.

EVB-IT Cloud

Die nun veröffentlichten EVB-IT Cloud gehören zu den EVB-IT Basisdokumenten. Wie bereits die zahlreichen anderen EVB-IT Vertragsmuster bestehen diese im Wesentlichen aus dem EVB-IT Cloud Vertrag sowie den zugehörigen EVB-IT Cloud AGB, in denen die wesentlichen Vertragsklauseln enthalten sind. Inhaltlich erfassen die EVB-IT Cloud insbesondere die Beschaffung von Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) sowie Managed Cloud Service (MCS) Leistungen.

In Abweichung zu den übrigen Vertragsmustern wurden mit den EVB-IT Cloudmustern zwei weitere Vorlagen zur optionalen Verwendung zur Verfügung gestellt. Dies sind zum einen der „EVB-IT Cloud Kriterienkatalog für Cloudleistungen“ (im Folgenden: Kriterienkatalog) und zum anderen die „EVB-IT Cloud Anlage auftragnehmerseitige AGB“ (im Folgenden: Anlage Anbieter AGB). Diese beiden Anlagen sind aus den anderen EVB-IT Verträgen nicht bekannt, weswegen der Fokus dieses Artikels auf diesen beiden Anlagen liegen soll.

Verwendet man als Beschaffer lediglich die bekannten Bestandteile, das Vertragsmuster und die EVB-IT Cloud AGB, so sind bereits schon die Mindeststandards für die Beschaffung von IT-Leistungen geregelt, wie Mindeststandards in der IT-Sicherheit, Art und Umfang der Leistungen, Vorgaben des Datenschutzes, Leistungsort, Reporting, Störungsbeseitigung und Exit Management.

Da aber nicht alle Cloud-Leistungen sowie Anforderungen an diese gleich sind, bietet der Kriterienkatalog die Möglichkeit von den standardisierten EVB-IT Cloud AGB abzuweichen und so detailliertere und differenziertere Vorgaben für die konkrete Leistung einzuführen. So kann man den Besonderheiten des Einzelfalles Rechnung tragen. Gleichzeitig ist in diesem Zusammenhang zu erwähnen, dass die Anwendung des Kriterienkatalogs eine hohe Expertise bezüglich Cloud-Leistungen erfordert.

Die wohl überraschendste Neuerung im EVB-IT Kosmos bildet hingegen die Anlage der Anbieter AGB. Auch diese kann optional einbezogen werden. Die Zurverfügungstellung dieser Anlage ist zwar eine Neuerung im EVB-IT Kosmos, war mit Hinblick auf den hohen Standardisierungsgrad von Cloud-Lösungen jedoch sinnvoll und geboten. Oftmals werden Bieter aufgrund des hohen Standardisierungsgrads nicht sämtliche Standards der EVB-IT Cloud einhalten können oder wollen. Die Verwendung der Anlage kann somit dazu beitragen, dass die öffentliche Hand überhaupt Angebote in der jeweiligen Beschaffung erhält. Gleichzeitig ermöglicht es die Verwendung der Anlage Anbieter AGB die vergaberechtlich vorgeschriebene Vergleichbarkeit der Angebote sicherzustellen, da der Beschaffer im Vorfeld Aspekte festlegt, in denen eine vorrangige Geltung der Bieter AGB in Betracht kommt. Hervorzuheben ist, dass die vorrangige Geltung der Bieter AGB stets nur in einzelnen, möglichst wenigen Punkten zur Anwendung kommen sollte, um nicht den Mindeststandard, den die Verwendung der EVB-IT Cloud sicherstellen soll, vollständig zu unterlaufen. Dies dürfte gerade unerfahrenen Beschaffern schwerfallen. Gerade hier können wir Sie aber in Zukunft unterstützen.

Fazit und Ausblick

Die Veröffentlichung der EVB-IT Cloud kann durchaus als Meilenstein für die Beschaffung von Cloud-Leistungen für die öffentliche Hand bezeichnet und gefeiert werden. Sie stellen eine wichtige Grundlage für die Einhaltung von Mindeststandards in der Beschaffung dar. Gleichzeitig bleibt ihre Anwendung komplex, insbesondere im Vergleich zu den bisher bekannten EVB-IT Vertragsmustern. Daher bedarf es bei der Anwendung der EVB-IT Cloud großer Umsicht und einer Bewertung des jeweiligen Einzelfalles. Selbstverständlich können wir Ihnen weiterhin bei der Beschaffung von IT-Leistungen zur Seite stehen.

Dr. Daniel Wittig berät regelmäßig schwerpunktmäßig in den Rechtsbereichen des Vertriebs-, IT- und Datenschutzrechtes. Er ist am Paderborner Standort tätig, der im Übrigen einen öffentlich-rechtlichen Schwerpunkt besitzt. Somit begleitet Dr. Wittig regelmäßig auch Vergabeverfahren aus zivilrechtlicher (vertraglicher) Sicht.

Dr. Daniel Wittig
Rechtsanwalt
Datenschutzbeauftragter (TÜV ®) gemäß DSGVO und BDSG
daniel.wittig@brandi.net

Dr. Christoph Rempe

Online-Bewertungen und Meinungsfreiheit – „Versandkosten Wucher!!“

Der gute Ruf eines Unternehmens ist in Zeiten der Digitalisierung ein entscheidender Faktor, um Kunden zu gewinnen oder zu halten. Besonders wichtig sind dabei nutzergenerierte Bewertungen des Unternehmens oder der angebotenen Waren und Dienstleistungen, die anderen potentiellen Kunden als Entscheidungshilfe dienen können. Denn die Meinung anderer Kunden schafft Vertrauen. Schlechte Bewertungen führen aber umgekehrt dazu, dass Vertrauen verloren geht oder gar nicht erst entsteht und das Produkt schließlich nicht gekauft oder die Dienstleistung nicht in Anspruch genommen wird.

Es liegt daher auf der Hand, dass Unternehmen möglichst gegen negative Bewertungen juristisch vorgehen möchten. Soweit in der Bewertung falsche Tatsachenbehauptungen enthalten sind, ist dies auch möglich und die Bewertungsportale müssen nach der Rechtsprechung des Bundesgerichtshofs (BGH) auch entsprechende Verfahren etablieren, um solche Bewertungen zu löschen. Schwieriger wird es aber, wenn die Bewertung nur Meinungsäußerungen beinhaltet. Weil das Recht auf freie Meinungsäußerung grundrechtlich geschützt ist, müssen Gerichte hier abwägen und die Meinungsfreiheit des Bewertenden berücksichtigen. Nur bei sogenannten Schmähkritiken tritt das Recht auf freie Meinungsäußerung zurück. Eine Schmähkritik liegt vor, wenn die Diffamierung des Bewerteten im Vordergrund steht, insbesondere bei Formalbeleidigungen.

Die Grenzen sind fließend. So musste der BGH sich aktuell mit einer Bewertung auf der Handelsplattform ebay befassen, bei der ein Kunde einem Händler „Ware gut, Versandkosten Wucher!!“ attestiert hatte (BGH, Urteil vom 28.09.2022 – VIII ZR 319/20). Der Kunde hatte von dem Händler über die Internetplattform eBay vier Gelenkbolzenschellen für 19,26 € brutto erworben. Davon entfielen 4,90 € auf die dem Kunden in Rechnung gestellten Versandkosten. Nach Erhalt der Ware bewertete der Kunde das Geschäft in dem von eBay zur Verfügung gestellten Bewertungsprofil wie angegeben. Die ebay-AGB regeln, dass Bewertungen sachlich sein müssen und keine Schmähkritiken enthalten dürfen. Der Händler klagte daher gegen die Bewertung und verlangte deren Entfernung, verlor in erster Instanz, bekam in zweiter Instanz aber Recht. Der Kunde habe mit der Bewertung eine vertragliche Nebenpflicht verletzt und gegen die Regelung in den ebay-AGB verstoßen, da es sich um eine überspitzte Bewertung ohne Sachbezug handele.

Der BGH hat nun jedoch in seinem Urteil vom 28.09.2022 entschieden, dass die Bewertung nicht zu entfernen sei. Die Regelung in den ebay-AGB enthalte keine über die bei Werturteilen ohnehin allgemein geltende Grenze der Schmähkritik hinausgehenden strengeren vertraglichen Beschränkungen für die Zulässigkeit von Werturteilen in Bewertungskommentaren. Es fehle eine Definition dafür, wann eine Bewertung sachlich ist. Daher solle die Bewertung allein nach der Rechtsprechung zu Schmähkritiken beurteilt werden, zumal der grundrechtlich verbürgten Meinungsfreiheit des Bewertenden von vornherein ein geringeres Gewicht beigemessen würde als den Grundrechten des Verkäufers, wenn man eine Meinungsäußerung eines Käufers regelmäßig bereits dann als unzulässig einstufte, wenn sie herabsetzend formuliert sei.

Die Grenze zur Schmähkritik sei nach den Karlsruher Richtern durch die Bewertung „Versandkosten Wucher!!“ aber nicht überschritten. Wegen seiner das Grundrecht auf Meinungsfreiheit beschränkenden Wirkung sei der Begriff der Schmähkritik eng auszulegen. Auch eine überzogene, ungerechte oder gar ausfällige Kritik mache eine Äußerung für sich genommen noch nicht zur Schmähung. Hinzutreten müsse vielmehr, dass bei der Äußerung nicht mehr die Auseinandersetzung in der Sache, sondern die Diffamierung des Betroffenen im Vordergrund stehe. Das sei aber bei der streitigen Bewertung nicht der Fall, weil der Kunde sich – wenn auch in scharfer und möglicherweise überzogener Form – kritisch mit einem Teilbereich der Leistung des Händlers auseinandersetze, indem er die Höhe der Versandkosten beanstande.

Diese Entscheidung zeigt erneut, welch hohen Wert der BGH der Meinungsfreiheit beimisst, sodass auch bei sehr negativen und sogar überzogenen Kritiken die Grenze zur Schmähkritik nur dann erreicht wird, wenn eine Auseinandersetzung in der Sache gar nicht mehr erkennbar ist. Wenn ein Unternehmen daher einen Kunden wegen einer negativen Bewertung auf Entfernung in Anspruch nehmen möchte, ist daher sehr genau zu argumentieren.

Dr. Christoph Rempe
Rechtsanwalt
Fachanwalt für Informationstechnologierecht (IT-Recht)
christoph.rempe@brandi.net

Dr. Steffen Kurth, LL.M.

Risiken bei der sog. lenkenden Ausschlagung einer Erbschaft

Bei demjenigen, der – sei es aufgrund der gesetzlichen Erbfolge oder aufgrund einer letztwilligen Verfügung wie eines Testaments – Erbe wird, fällt die Erbschaft mit dem Tod des Erblassers automatisch an. In der Praxis gibt es allerdings gelegentlich den Wunsch von Erben, dass die ihnen zustehende Erbschaft eigentlich jemand anderem zufällt. Aus diesem Beweggrund erfreut sich die Ausschlagung von Erbschaften, damit diese an eine andere Person „gelenkt" werden, bislang gewisser Beliebtheit.

Konkret muss in dem Fall, in dem die Erbschaft ausgeschlagen und so zu einer anderen Person gelenkt wird, die Erbschaft formgerecht (nämlich zur Niederschrift des Nachlassgerichts oder in notariell beglaubigter Form gegenüber dem Nachlassgericht) und vor allen fristgerecht (in der Regel binnen sechs Wochen ab Kenntnis von dem Anfall des Erbes und dem Grund der Berufung) ausgeschlagen werden. Infolge der wirksamen Erbausschlagung gilt der Ausschlagende dann nicht länger als Erbe und der nächstberufenen Person fällt das Erbe zu.

Einer der wesentlichen Vorteile einer solchen lenkenden Ausschlagung ist, dass bei dem Ausschlagenden kein erbschaftsteuerpflichtiger Zwischenerwerb erfolgt. Der wesentliche Nachteil der lenkenden Ausschlagung ist dagegen, dass der Ausschlagende nicht selbst bestimmen kann, wem die ausgeschlagene Erbschaft zufällt. Vielmehr bestimmt der Erblasser selbst, notfalls das Gesetz, wem die Erbschaft infolge der Ausschlagung zuteil wird. Das birgt das Risiko, dass der Ausschlagende sich darüber täuscht, wem infolge seiner Ausschlagung die Erbschaft letztlich zufällt. In der juristischen Literatur sind die Folgen eines solchen Irrtums, wer infolge der lenkenden Ausschlagung Erbe wird, seit Langem umstritten. Höchstrichterlich geklärt ist die Frage bislang noch nicht. Allerdings liegt nun eine Entscheidung des OLG Hamm vom 21.04.2022 (Az.: 15 W 51/19) vor, die in der Praxis für wahrscheinlich mehr Klarheit sorgen wird. Das OLG Hamm stellt sich auf den Standpunkt, dass der Irrtum über die Person, der die Ausschlagung zugutekommt, grundsätzlich nicht beachtlich ist. Dies hat zur Folge, dass nach Meinung der Hammer Richter die Erbausschlagung wirksam bleibt, selbst wenn der Ausschlagende sein Ziel verfehlt, die Erbschaft durch Ausschlagung zu einer bestimmten Person zu lenken.

Es ist zu erwarten, dass der BGH diese Streitfrage in absehbarer Zeit höchstrichterlich klären wird. Für die Zwischenzeit und für den Fall, dass sich der BGH der Auffassung des OLG Hamm anschließen sollte, gibt es für die Beteiligten weiterhin andere Wege, eine Erbschaft einer bestimmten Person zuzulenken. Insbesondere wird in Zukunft voraussichtlich vermehrt Gebrauch gemacht werden von der Möglichkeit, eine Erbschaft gerade nicht auszuschlagen, sondern anzunehmen (vor allen wenn nicht eindeutig ist, wer im Falle der Ausschlagung nächst berufener Erbe wäre) und die angenommene Erbschaft dann auf die gewünschte Person mittels notariellem Vertrag zu übertragen.

Dr. Steffen Kurth, LL.M und Jessika Biskup

Unklarheiten vermeiden bei sogenannten Geldvermächtnissen

Das OLG Frankfurt a. M. musste sich in seinem aktuellen Urteil vom 05.04.2022 (Az. 10 U 200/20) mit der Anwendbarkeit einer gesetzlichen Auslegungsregel im Zusammenhang mit sogenannten (Geld-)vermächtnissen beschäftigen. Die Entscheidung verdeutlicht, welche Unklarheiten und deshalb Streitpotenziale bei der Anordnung von Vermächtnissen der vorgenannten Art lauern.

Von einem Geldvermächtnis ist die Rede, wenn eine Person nicht den gesamten Nachlass des Erblassers automatisch als Erbe erhalten soll, sondern lediglich das Recht, eine bestimmte Geldzahlung von den Erben zu verlangen.

In dem von dem OLG Frankfurt a. M. zu entscheidenden Fall errichtete die Erblasserin ein Testament, um die Verteilung ihres Vermögens nach dem Todesfall zu regeln. In ihrem Testament setzte sie zunächst eine Person zu ihrem alleinigen Erben ein, der ihren gesamten Nachlass einschließlich eventueller Verbindlichkeiten automatisch erhalten sollte. Zudem ordnete sie in dem Testament Vermächtnisse an. Betreffend der Vermächtnisse sollten im Todesfall Wertpapiere der Erblasserin im Wert von etwa 780.000,00 Euro verkauft und der Erlös vom Erben zu je 1/6 an sechs benannte Vermächtnisnehmer ausgezahlt werden.

Die Besonderheit des Falles lag nun darin, dass die Anleihen, die sich bei der Testamentserrichtung noch im Wertpapierdepot der späteren Erblasserin befanden, zwischen der Errichtung des Testaments und dem Tod der Dame ausgezahlt und nicht wieder in Wertpapiere angelegt, sondern auf einem Festgeldkonto eingezahlt wurden. Das hatte zur Folge, dass sich der Wert des Wertpapierdepots der Erblasserin im Zeitpunkt ihres Todes auf rund 100.000 Euro belief, wohingegen ihr Festgeldkonto ein Guthaben von mehr als 600.000 Euro aufwies.

Die Gerichte mussten nun über mehrere Instanzen hinweg entscheiden, ob – wie der Erbe meinte – den Vermächtnisnehmern nur ein Anteil an dem Erlös des zum Zeitpunkt des Todesfalls verbleibenden Wertpapierdepots zustand oder – wie die Vermächtnisnehmer annahmen – sich die Höhe der Vermächtnisse nach dem Wert des Festgeldkontos bemessen müsste.

Das OLG Frankfurt a. M. schloss sich der Auffassung der begünstigten Vermächtnisnehmer an und entschied, dass den Vermächtnisnehmern auch ein Anteil am Festgeldkonto zusteht. Zur Begründung seiner Entscheidung zog das Gericht die Vorschrift des § 2173 BGB heran. Als Zweifelsregel dient § 2173 BGB für die Konstellationen, in denen der Erblasser eine ihm zustehende Forderung vermacht und die vermachte Forderung vor dem Erbfall erfüllt wird. Im Speziellen regelt Satz 2 der Vorschrift diejenigen Fälle, in denen die Forderung auf die Zahlung einer Geldsumme gerichtet war. Nach Ansicht des Oberlandesgerichts handelte es sich bei dem vorliegenden Vermächtnis zwar um ein Geldvermächtnis, jedoch lag eine vergleichbare Interessenlage vor, so dass § 2173 BGB angewendet werden konnte. So bestand nach den gerichtlichen Feststellungen aus Sicht der Erblasserin kein wesentlicher Unterschied zwischen Wertpapieren und dem hier vermachten Erlös aus der Wertpapierveräußerung nach dem Erbfall. Die Erblasserin wollte lediglich die Abwicklung

des Nachlasses erleichtern. Weil das Gericht also einen für die Vermächtnisnehmer günstigen Willen der Erblasserin annahm, konnte es auf eine Zweifelsregel im Gesetz zurückgreifen. Zu beachten ist, dass die Vermächtnisnehmer diesen Willen der Erblasserin zunächst beweisen mussten.

Unter Rückgriff auf § 2173 Satz 2 BGB erfasste das Vermächtnis nach Meinung des OLG Frankfurt a. M. im Zweifel das Festgeldkonto bzw. das Sparvermögen, welches das Surrogat der Anleihen bildetet. Danach konnten die begünstigten Vermächtnisnehmer verlangen, dass ihnen auch ein Anteil an dem Festgeldkonto ausgezahlt wird.

Die Entscheidung zeigt die Bedeutung für Erblasser, ihren Willen in einem Testament nach Möglichkeit derart klar zum Ausdruck zu bringen, dass nicht über mehrere Instanzen und Jahre hinweg über den Umfang eines Vermächtnisses gestritten werden muss. Zugleich verdeutlicht das Urteil, wie wichtig es ist, in regelmäßigen Abständen das eigene Testament auf seine Aktualität zu überprüfen und ggf. an sich veränderte Umstände (hier Umschichtung im Depot) anzupassen.

Dr. Steffen Kurth, LL.M.
Rechtsanwalt und Notar mit Amtssitz in Bielefeld
Fachanwalt für Erbrecht
Fachberater für Unternehmensnachfolge (DStV e.V.)
steffen.kurth@brandi.net

Dr. Jürgen Löbbe

Verhinderung des Vermögensübergangs auf den Ex-Partner

Nach einer Trennung haben Personen, die sich mit der Errichtung eines Testaments beschäftigen, nicht selten den nachvollziehbaren Wunsch, dass der ehemalige Lebensgefährte nach dem eigenen Tod in keiner Weise am eigenen Nachlass und dessen Verwaltung beteiligt wird. Ist ein gemeinsames Kind vorhanden, erfordert die Umsetzung dieser Vorstellung ein nicht unerhebliches Maß an Weitsicht.

Ist das gemeinsame Kind bei Eintritt des eigenen Todes noch minderjährig, wird der überlebende Elternteil nach § 1680 Abs. 1 BGB grundsätzlich alleiniger gesetzlicher Vertreter des Kindes und damit auch Vermögensverwalter. Soll nun das gemeinsame Kind, wie es in der überwiegenden Zahl der Fälle gewünscht ist, den eigenen Nachlass erhalten, bedarf es einer ausdrücklichen testamentarischen Anordnung, um zu verhindern, dass der (oftmals verhasste) Ex-Partner neben dem eigenen Vermögen des Kindes auch den angefallenen Nachlass verwaltet (vgl. § 1638 Abs. 1 BGB).

Eine noch größere Gefahr besteht darin, dass das gemeinsame Kind nach dem eigenen Tod ebenfalls vorzeitig kinderlos verstirbt und von dem Ex-Partner überlebt wird. Ohne testamentarische Verfügungen des Kindes wird der Ex-Partner dessen gesetzlicher (Allein-)Erbe (vgl. § 1925 Abs. 3 S. 2 BGB) und partizipiert als solcher indirekt auch am eigenen Nachlass. Außerdem muss beachtet werden, dass der Ex-Partner als Elternteil des Kindes gemäß § 2303 BGB zum Kreis der Pflichtteilsberechtigten gehört. Macht er beim Nachversterben des Kindes Pflichtteilsansprüche geltend, berechnen sich diese wertmäßig nicht nur aus dem hinzuerworbenen Vermögen des Kindes, sondern auch aus dem bis dahin unverbrauchten eigenen Nachlass.

Wer diese Gefahren vermeiden oder reduzieren möchte, muss testamentarische Regelungen treffen. In der juristischen Literatur wird diese Regelungskonstellation als „Geschiedenentestament" bezeichnet.

Üblicherweise wird für das Geschiedenentestament die sog. „Erblösung" gewählt, bei der das gemeinsame Kind zum Vorerben und dessen Abkömmlinge oder andere Verwandte (mit Ausnahme des Ex-Partners) zu Nacherben eingesetzt werden. Mit Eintritt des Nacherbfalls fällt die Erbschaft den Nacherben ohne Weiteres an, was eine Teilhabe des Ex-Partners ausschließt.

Der Nachteil bei dieser Gestaltungsvariante liegt darin, dass das Kind als Vorerbe gewissen zwingenden gesetzlichen Verfügungsbeschränkungen und Einschränkungen unterliegt, beispielsweise dem Verbot unentgeltlicher Verfügungen über Nachlassgegenstände. Dem Kind wäre es deshalb zu Lebzeiten nicht ohne Einschränkungen möglich, nach freiem Belieben über das ererbte Vermögen zu verfügen.

Um für das Kind eine größere Flexibilität zu erreichen, wird zuweilen auf die sog. „Vermächtnislösung" ausgewichen. Dabei wird das gemeinsame Kind entweder zum Erben eingesetzt und – anstelle der Anordnung einer Nacherbfolge – mit einem Herausgabevermächtnis zugunsten der Abkömmlinge oder sonstiger Verwandter beschwert, oder aber zum Vorvermächtnisnehmer und Dritte (mit Ausnahme des Ex-Partners) zu Nachvermächtnisnehmern eingesetzt. Nachteil dieser Gestaltungsvariante ist, dass sie im Vergleich zur Erblösung weniger Sicherheit bietet. Denn aufgrund des rein schuldrechtlichen Charakters des Vermächtnisses können lebzeitige Zuwendungen des Kindes an den Ex-Partner nur durch aufwendige Sicherungsmaßnahmen verhindert werden. Sieht man solche vor, nähert sich der Umfang der Einschränkung des Kindes jenem bei einer Vor- und Nacherbschaft.

Die schwierigste Aufgabe bei der praktischen Gestaltung solcher Geschiedenentestamente ist es deshalb, eine Balance zwischen der größtmöglichen Absicherung der gewünschten Regelungsziele und der Erhaltung einer möglichst weitgehenden Gestaltungsfreiheit des Kindes zu finden. Die dafür erforderlichen Maßnahmen hängen von vielen Faktoren ab (Alter des Kindes, Vorhandensein eigener Abkömmlinge des Kindes, familiäre Situation des Ex-Partners usw.) und müssen auf die konkreten Lebensumstände zugeschnitten werden. Eine pauschal zu empfehlende „beste Lösung" gibt es nicht.

So kann es in einigen Fällen sogar sinnvoll sein, die beiden vorstehenden Gestaltungsvarianten miteinander zu kombinieren. Es ist nämlich möglich, die Geltung der Vor- und Nacherbfolge nur für den Zeitraum anzuordnen, in dem der Ex-Partner noch am Leben ist. Sobald dieser selbst verstorben ist, kommt er als (gesetzlicher) Erbe des gemeinsamen Kindes nicht mehr in Betracht. Das verbleibende Restrisiko des Anfalls an die einseitigen Verwandten des Ex-Partners kann durch eine zusätzliche, aufschiebend bedingte Anordnung von Herausgabevermächtnissen – ggf. in Kombination mit einer Testamentsvollstreckung – abgemildert werden. Ob diese zusätzliche Beeinträchtigung des Erben (durch Anordnung der Vermächtnisse) zur Erreichung des gewünschten Maßes an Sicherheit überhaupt erforderlich ist, wird sich wiederrum nur auf Grundlage der konkreten Lebensumstände bestimmen lassen.

Fazit

Bei der Testamentserstellung sind nicht nur die Folgen des eigenen Versterbens zu berücksichtigen, sondern auch die Möglichkeit eines kurzfristigen Nachversterbens des eigenen Kindes zu bedenken. Durch eine vorausschauende Gestaltung ist es möglich, den eigenen Nachlass bzw. bestimmte Gegenstände nicht den Erben des Erstbedachten zukommen zu lassen, diesem jedoch gleichzeitig ein sehr hohes Maß an Verfügungsfreiheit zu erhalten.

Dr. Jürgen Löbbe
Rechtsanwalt und Notar mit Amtssitz in Bielefeld
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für Erbrecht
juergen.loebbe@brandi.net

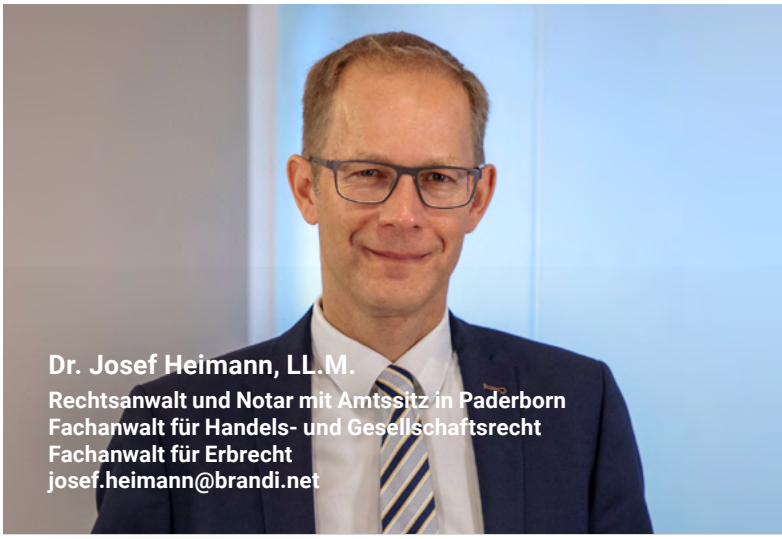
Dr. Josef Heimann, LL.M.

Höhere Schenkungsteuer bei Immobilienschenkungen ab 2023

Schenkungen lösen Schenkungsteuer aus, wenn Freibeträge überschritten werden und wenn sie nicht im Einzelfall aus besonderen Gründen schenkungsteuerfrei sind (z. B. mitunter bei der Übertragung des Familienheims). Ein Ehegatte kann dem anderen Ehegatten alle zehn Jahre schenkungsteuerfrei Werte von bis zu 500.000 Euro schenken oder vererben, ein Elternteil jedem seiner Kinder bis zu 400.000 Euro.

Trotz hoher Inflation plant der Gesetzgeber keine Erhöhung der Freibeträge. Im Gegenteil: Der kürzlich bekannt gewordene Entwurf des Jahressteuergesetzes 2022 sieht Änderungen vor, die manche heute noch steuerfreie Schenkung ab dem 1. Januar 2023 schenkungsteuerpflichtig macht. Der Gesetzgeber plant eine Änderung des Bewertungsgesetzes, welche Immobilien und Anteile an grundbesitzenden Gesellschaften in der Silvesternacht – jedenfalls aus Sicht des Finanzamtes – wertvoller macht. Die bislang gültigen Regeln führen nämlich zu für die Schenkungsteuer maßgeblichen Bewertungen, welche unterhalb des tatsächlichen Verkehrswertes liegen. Das soll sich ändern. Es liegt auf der Hand, dass hierdurch in Zukunft bei vielen Immobilienschenkungen mehr Schenkungsteuer anfällt als aktuell. Je besser die Lage der Immobilie, desto höher ist das Risiko, dass bei einer Übertragung ab dem nächsten Jahr der Freibetrag überschritten wird bzw. sich die Schenkungsteuerbelastung erhöht.

Wer ohnehin die Schenkung einer Immobilie oder eines Anteils an einer grundbesitzenden Gesellschaft plant, sollte daher überlegen, ob er die Übertragung noch in diesem Jahr notariell beurkunden lässt. Hierdurch können – natürlich abhängig vom Einzelfall – erhebliche Steuerbelastungen vermieden werden. Allerdings sollte niemand überstürzt handeln: Eine Immobilie lediglich zur Steuerersparnis zu übertragen, ist nie eine gute Idee. Nur wenn der Schenker sicher ist, dass er seine Immobilie nicht z. B. eines Tages zur Altersvorsorge verkaufen muss, sollte er sie verschenken. Dabei kann er sich Rechte vorbehalten, welche ihm den Zugriff auf die Immobilie zu seinen Lebzeiten sichern, wie z. B. ein Wohnungs- oder Nießbrauchsrecht. Positiver Nebeneffekt: Der Vorbehalt von Rechten mindert den Wert der Schenkung und damit auch die Schenkungsteuerbelastung. Hieran wird sich nichts ändern.



Dr. Josef Heimann, LL.M.
Rechtsanwalt und Notar mit Amtssitz in Paderborn
Fachanwalt für Handels- und Gesellschaftsrecht
Fachanwalt für Erbrecht
josef.heimann@brandi.net

Rüdiger Hitz

Finanzverwaltung aktuell – Versagung des Vorsteuerabzugs und der Steuerbefreiung bei Beteiligung an einer Steuerhinterziehung (§25 f UStG)

Zur Bekämpfung von Steuerbetrügereien sah § 25d UStG bis Ende 2019 eine Haftungsregelung vor. Diese Regelung wurde zum 31. Dezember 2019 gestrichen. Dafür nahm der Gesetzgeber zum 01.01.2020 eine direkt einen Unternehmer betreffende Regelung in § 25f UStG auf. Bei Vorliegen der nachfolgend dargelegten Voraussetzungen ist die Steuerbefreiung für eine innergemeinschaftliche Lieferung nach § 4 Nr. 1b UStG in Verbindung mit § 6a UStG ebenso wie der Vorsteuerabzug nach § 15 Abs. 1 S. 1 Nr. 1, Nr. 3 sowie Nr. 4 UStG zu versagen.

Das Finanzamt hat nachzuweisen, dass der Unternehmer wusste oder hätte wissen müssen, dass er sich mit seinem Eingangs- oder Ausgangsumsatz an einem Umsatz beteiligt, bei dem der Leistende oder ein anderer Beteiligter auf einer vorhergehenden oder nachfolgenden Umsatzstufe in eine begangene Hinterziehung von Umsatzsteuern, an einer Erlangung eines nicht gerechtfertigten Vorsteuerabzugs im Sinne des § 370 AO oder in eine Schädigung des Umsatzsteueraufkommens im Sinne der § 26a und 26c UStG einbezogen war. **Eine Einbeziehung des Unternehmers selbst in die Steuerhinterziehung oder den ungerechtfertigten Steuervorteil ist nicht erforderlich!**

Nach dem Schreiben des Bundesministeriums der Finanzen vom 15. Juni 2022 wurde der Umsatzsteueranwendungserlass um die Abschnitte 25f.1 und 25f.2 zur einheitlichen Anwendung der Regelung des § 25f UStG durch die Finanzverwaltung veröffentlicht. Dieses Schreiben dokumentiert ausschließlich die Ansicht der Finanzverwaltung zu diesem Themenbereich.

1. „wissen müssen“

Für das „wissen müssen“ stellt die Finanzverwaltung Vermutungsregelungen auf, nach welchen bei den folgenden Anhaltspunkten weitergehende Prüfungen erforderlich sind:

> die Rahmenbedingungen für das Umsatzgeschäft werden dem Unternehmer von einem Dritten vorgegeben (z. B. Vermittlung von Beteiligungen, Vorgabe von Einkaufs-/Verkaufspreisen, Zahlungsmodalitäten oder Liefer- bzw. Leistungswegen),
>
> die Finanzierung des Wareneinkaufs ist erst nach erfolgtem Warenverkauf möglich,
>
> Mehrfachdurchläufe von Waren werden festgestellt,
>
> dem Unternehmer werden Waren bzw. Leistungen angeboten, deren Preis unter dem Marktpreis liegt,
>
> es erfolgt eine ungewöhnliche Zahlungsabwicklung oder branchenunübliche Barzahlung,
>
> die Ansprechpartner in den Unternehmen oder die Ansprechpartner die Unternehmen selbst häufig wechseln,
>
> berufliche Erfahrungen und Branchenkenntnisse fehlen bei den Beteiligten,
>
> die Beteiligten verlegen wiederholt ihren Unternehmenssitz,
>
> es bestehen Zweifel an der Richtigkeit der Angaben der Beteiligten (z. B. aufgrund von Abweichungen des Gesellschaftszwecks oder der Geschäftsadressen zu den Angaben lt. Handelsregister),
>
> der tatsächlich ausgeübte Gesellschaftszweck entspricht nicht dem Gesellschaftszweck lt. Handelsregister,
>
> dem Unternehmer werden Warenmengen oder ein Leistungsumfang angeboten, welcher für die Größe des Unternehmens in der Branche unüblich ist (z. B. ungewöhnlich hohe Stückzahlen trotz Neugründung),
>
> die Beteiligten verfügen über keine ausreichende Möglichkeit zur Kontaktaufnahme (z. B. Webseite ohne Impressum, Rufnummer oder E-Mailadresse),
>
> es liegen ungewöhnliche Leistungsbedingungen vor (z. B. die Leistungen werden von einem oder an einen nicht an dem Umsatz beteiligten Unternehmen erbracht) und
>
> durch den Unternehmer kann über zugängliche Informationsquellen (z. B. **Internetrecherche**) festgestellt werden, dass die Anlieferung der Ware an die vom Abnehmer angegebene Lieferadresse nicht möglich erscheint.

2. Vorliegen einer Steuerhinterziehung/Verletzung der Strafregelungen des UStG

Weitere Voraussetzung ist, dass die objektiven und subjektiven Tatbestandsmerkmale einer Steuerhinterziehung bzw. der Bußgeld- oder Strafregelungen des UStG erfüllt sind.

Dabei ist eine strafgerichtliche Verurteilung oder eine bußgeldrechtliche Ahndung nicht erforderlich. An Entscheidungen im straf- oder bußgeldrechtlichen Verfahren ist das Finanzamt bei Anwendung des § 25f UStG nicht gebunden!

Das Wissen oder wissen müssen seiner Angestellten ist dem Unternehmer zuzurechnen, BFH vom 19.05.2010 –XI R 78/07.

3. Infizierte Lieferkette

Die Feststellung einer Steuerhinterziehung kann sowohl den unmittelbaren Eingangs- oder Ausgangsumsatz des Unternehmers, als auch einen Umsatz auf allen vor- und nachgelagerten Umsatzstufen innerhalb der Lieferkette umfassen.

4. Handlungsempfehlung

Durch die neue Regelung des § 25f UStG wurde die sogenannte Missbrauchs-Rechtsprechung des EUGH ins nationale Gesetz umgesetzt. In der Entscheidung vom 2. Juli 2022 (XI R 40/19) hat der BFH entschieden, dass allein die Erfüllung der materiellen Voraussetzungen gerade noch keinen Anspruch des Unternehmers auf eine steuerbefreite innergemeinschaftliche Lieferung darstellt. Mit Blick auf diese Entscheidung ist es für einen Unternehmer nicht nur ratsam, sondern absolut erforderlich, vor Eingehung einer neuen Geschäftsbeziehung die Beteiligten einer neuen Lieferkette exakt zu prüfen. Um den Sorgfaltspflichten eines ordentlichen Kaufmanns nachzukommen und in den

Genuss der Vertrauensschutzregelung nach § 6a Abs. 4 UStG zu gelangen, gehört eine permanente Gültigkeitsabfrage der Umsatzsteuer-Identifikationsnummer des Leistungsempfängers zum Mindeststandard. Sofern Anhaltspunkte für Unregelmäßigkeiten, insbesondere eine Steuerhinterziehung entweder bei der Aufnahme neuer oder bei bestehenden Geschäftsbeziehungen erkennbar werden, muss der Unternehmer weitergehende, über die üblicherweise zu verlangenden geeigneten Maßnahmen zur Prüfung ergreifen (z. B. Auskünfte einholen) und dies auch **geeignet dokumentieren**. Kommt der Unternehmer dem nicht nach oder kann vorliegend Zweifel durch die ergriffenen Maßnahmen nicht ausräumen, und geht die Geschäftsbeziehung dennoch ein oder führt diese fort, ist von einem „Wissen oder wissen müssen" und damit der Versagung des Vorsteuerabzugs bzw. der Steuerfreiheit der innergemeinschaftlichen Lieferung, des Unternehmers auszugehen.

„Know your customer" war gestern, „know your supply chain" ist heute!

Rüdiger Hitz
Rechtsanwalt und Steuerberater
Fachanwalt für Steuerrecht
Fachanwalt für Strafrecht
Zertifizierter Berater für Steuerstrafrecht (DAA)
ruediger.hitz@brandi.net

Dr. Anne-Louise Schümer

Die Gewinnabschöpfung im Ordnungswidrigkeitenverfahren – Vorteile und „Tücken"

Das Ordnungswidrigkeitenrecht kennt den Begriff der Gewinnabschöpfung nicht, sondern bezeichnet dieses Instrument als die Einziehung des Wertes von Taterträgen. Die rechtlichen Voraussetzungen finden sich in § 29 a OWiG.

Die Einziehungsanordnung ist ein bei den Verwaltungsbehörden beliebtes Mittel, denn es ermöglicht, Gewinne bei Unternehmen abzuschöpfen und daher höhere Einnahmen für die öffentlichen Kassen zu generieren. Allerdings sind bei dem rechtlichen Konstrukt der Einziehungsanordnung verfahrensrechtliche Besonderheiten zu beachten, die den Verwaltungsbehörden (und auch den Amtsgerichten) nicht immer vollumfänglich bekannt sind. Insofern bietet sich hier ein Einfallstor für die Angreifbarkeit von solchen Einziehungsanordnungen. Dies gilt um so mehr, als die obergerichtliche Rechtsprechung eher dünn und zudem nicht einheitlich ist.

Vorteile einer Einziehungsanordnung

Geldbußen über 200 € finden gem. § 149 Abs. 2 Nr. 3 GewO Eintragung in das Gewerbezentralregister. Auszüge aus dem Gewerbezentralregister müssen beispielsweise bei öffentlichen Ausschreibungen vorgelegt werden oder sind relevant bei der Beurteilung der gewerberechtlichen Zuverlässigkeit.

Die Einziehungsanordnung ist hingegen lediglich Nebenfolge einer Ordnungswidrigkeit und findet daher gerade keinen Eintrag in das Gewerbezentralregister. Die Höhe der Einziehungsanordnung ist daher ohne Belang.

„Tücken" der Einziehungsanordnung

Das Ordnungswidrigkeitenrecht räumt unterschiedliche Möglichkeiten einer Einziehungsanordnung an:

Nach § 29 a OWiG kann gegen den Täter einer Ordnungswidrigkeit, gegen den eine Geldbuße nicht festgesetzt wird, die Einziehung eines Geldbetrages angeordnet werden, der dem Gewinn aus der Ordnungswidrigkeit entspricht. Diese Variante der alleinigen Einziehungsanordnung gegen den Täter ist verfahrensrechtlich unproblematisch und daher auch in der Praxis wenig relevant.

Sofern die Ordnungswidrigkeit eines Unternehmensangehörigen im Zusammenhang mit seiner betrieblichen Tätigkeit steht (z. B. Überladung von Lastkraftwagen oder Schwerlasttransporte und Güterkraftverkehr) kann der dem Unternehmen aus dieser Ordnungswidrigkeit erwachsene Gewinn gem. § 29 a Abs. 2 OWiG abgeschöpft werden. Dies wird als sogenannte Dritteinziehung bezeichnet, die in der Regel als selbständige und isolierte Einziehungsanordnung gegen das Unternehmen ergeht.

Das Ordnungswidrigkeitenrecht räumt allerdings auch die Möglichkeit ein, dass eine Geldbuße gegen den Täter und zudem eine Einziehungsanordnung gegen das Unternehmen erlassen wird.

Selbständige (isolierte) Dritteinziehungsanordnung gegen das Unternehmen

§ 29 Abs. 5 OWiG bestimmt, dass die Einziehungsanordnung in einem selbständigen Verfahren angeordnet werden kann, sofern gegen den Täter ein Ordnungswidrigkeitenverfahren nicht eingeleitet oder es eingestellt wird.

Die Verwaltungsbehörde braucht also nur festzustellen, dass überhaupt eine betriebsbezogene Ordnungswidrigkeit vorliegt und kann in einem isolierten Bescheid gegen das Unternehmen den Gewinn aus dieser Ordnungswidrigkeit abschöpfen. Das Verfahren gegen den Täter der betriebsbezogenen Ordnungswidrigkeit wird dann überhaupt nicht durch die Verwaltungsbehörde eingeleitet oder es wird eingestellt.

In verfahrensrechtlicher Hinsicht ist es allerdings erforderlich, dass die Nebenbeteiligung des Unternehmens nach § 87 OWiG von der Verwaltungsbehörde ausdrücklich angeordnet wird. Diese Anordnung versäumt die Verwaltungsbehörde gelegentlich. Hier bietet sich zumindest ein Angriffspunkt.

Bußgeldbescheid gegen den Täter und Dritteinziehungsanordnung gegen das Unternehmen

Es ist zunehmend zu beobachten, dass die Verwaltungsbehörde sich nicht mit einer selbständigen Einziehungsanordnung gegen

das Unternehmen zufrieden gibt, sondern zusätzlich auch eine Geldbuße gegen den Täter festsetzen möchte.

Nach den Vorgaben aus § 29 a OWiG wäre der zutreffende verfahrensrechtliche Weg, einen Bußgeldbescheid gegen den Täter zu erlassen und als Annex in diesem Bußgeldbescheid die Einziehung des Unternehmensgewinns anzuordnen.

Aus nicht nachvollziehbaren Gründen tendieren die Verwaltungsbehörden jedoch dazu, zwei unterschiedliche und gesonderte Verfahren, also gegen den Täter einerseits und das Unternehmen andererseits, zu führen und in logischer Konsequenz einen isolierten Bußgeldbescheid und eine isolierte Einziehungsanordnung zu erlassen. Diese behördliche Verfahrensweise ist rechtsfehlerhaft.

Diese rechtsfehlerhafte behördliche Verfahrensweise wird durch die Oberlandesgerichte aber unterschiedlich beurteilt.

Das Oberlandesgericht Zweibrücken vertritt hierzu in seinem Beschluss vom 08.05.2018 (Az.: 1 OWi 2 Ss Bs 6718) die Einzelmeinung, die gesonderte (fehlerhafte) Verfahrensführung könne dadurch geheilt werden, dass die Verwaltungsbehörde eine „besondere Verknüpfungsfunktion“ herstelle, indem in den gesonderten Bescheiden jeweils ein Hinweis auf den jeweils anderen Bescheid enthalten sei.

Demgegenüber hält es das Oberlandesgericht Celle in einem Beschluss vom 29.10.2008 (Az.: 322 SsBs 172/08) lediglich für möglich, dass die gesonderte Verfahrensführung durch das Amtsgericht geheilt werden könnte, wenn es nach den Einsprüchen gegen den Bußgeldbescheid und die Einziehungsanordnung die beiden Verfahren gerichtlich verbindet.

Übereinstimmend geht aber die sonstige obergerichtliche Rechtsprechung von der Rechtsfehlerhaftigkeit der gesonderten Verfahrensführung aus. Diese rechtliche Einschätzung manifestiert sich daran, dass der Einziehungsanordnung gegen das Unternehmen bei einer rechtskräftigen Sachentscheidung gegen den Täter ein Verfahrenshindernis entgegensteht, sie also unzulässig ist.

Liegt also ein rechtskräftiger Bußgeldbescheid, respektive eine rechtskräftige Verurteilung des Täters vor, so kann die auf diese Ordnungswidrigkeit Bezug nehmende Einziehungsanordnung nicht erlassen werden.

Praxishinweis:

Einziehungsanordnungen, die Unternehmensgewinne abschöpfen, sollten genauestens geprüft werden, da sie in der überwiegenden Anzahl in verfahrensrechtlicher Hinsicht angreifbar sind.

Dr. Anne-Louise Schümer
Rechtsanwältin
Fachanwältin für Strafrecht
anne-louise.schuemer@brandi.net

UNSER BÜRO IN MINDEN ZIEHT UM

AB DEM 16. JANUAR 2023
LAUTET DIE NEUE ADRESSE

STIFTSALLEE 4
32425 MINDEN

FRAGEN AN DR. DANIEL WITTIG

WARUM BRANDI?

Ich selbst komme aus Ostwestfalen und wollte nach meinem Studium und dem Referendariat gerne wieder in OWL Fuß fassen. In dieser Region ist BRANDI im rechtsanwaltlichen Bereich eine Institution, die aber auch außerhalb der Grenzen OWLs für ihre guten Leistungen viel Anerkennung findet. Da war es für mich klar, dass ich zu BRANDI muss, wenn ich mit den Besten zusammenarbeiten möchte. Als ich dann noch im Rahmen meines Referendariats die „BRANDI Kultur“ kennenlernen durfte, stand meine Entscheidung endgültig fest. BRANDI zeichnet sich durch viele kompetente und nette Kollegen aus, für die es aber gleichzeitig nicht nur die Arbeit, sondern auch Familie und Freizeit gibt.

WAS TREIBT MICH AN?

Für mich war es stets wichtig, dass ich möglichst spezialisiert arbeite, um so ein hohes Niveau in den von mir bearbeiteten Rechtsbereichen erreichen zu können. Ich wollte mein Berufsleben nie als Generalist beschreiten, der alles ein bisschen, aber nichts so richtig kann. Genau diese Möglichkeit bietet mir BRANDI. Es treibt mich an für unsere Mandanten als spezialisierter Ansprechpartner gemeinsam dort Lösungen zu finden, wo sie selbst manchmal nicht weiterkommen. Gleichzeitig kann ich als Freiberufler frei und selbstständig entscheiden, wie ich mir die Arbeiten einteile. Auch für sich selbst verantwortlich zu sein, ist dabei ein Privileg.

AUSSER DEM JOB GIBT ES NOCH?

Abseits des Berufslebens verbringe ich am liebsten Zeit mit meiner Frau, der Familie und unseren Freunden. Wir reisen sehr gerne, da wir so nicht nur andere Orte und Kulturen entdecken, sondern uns auch auf uns und die privaten Dinge im Leben konzentrieren können.

HIGHLIGHTS AUS MEINER HEIMAT?

Ein einzelnes Highlight aus meiner Heimat kann ich nicht benennen. Es ist vielmehr die Region selbst, die ich als Highlight bezeichnen würde. Ostwestfalen, aber auch Paderborn, wird von Vielen unterschätzt. Dies muss ich immer wieder feststellen, wenn ich mit Freunden spreche, die nicht aus dieser Region kommen. Diese sind dann überrascht, welch hohe Lebensqualität die Region bietet. Abseits vom Stress der großen Metropolen kann man hier perfekt sein Leben genießen, ohne aber gleichzeitig komplett abgeschieden zu sein.

Dr. Daniel Wittig
Rechtsanwalt
Datenschutzbeauftragter (TÜV ®) gemäß DSGVO und BDSG
daniel.wittig@brandi.net

Bielefeld
Adenauerplatz 1
33602 Bielefeld
T +49 521 96535 - 0
F +49 521 96535 - 99
E bielefeld@brandi.net

Detmold
Lindenweg 2
32756 Detmold
T +49 5231 9857 - 0
F +49 5231 9857 - 50
E detmold@brandi.net

Gütersloh
Thesings Allee 3
33332 Gütersloh
T +49 5241 5358 - 0
F +49 5241 5358 - 40
E guetersloh@brandi.net

Paderborn
Rathenaustraße 96
33102 Paderborn
T +49 5251 7735 - 0
F +49 5251 7735 - 99
E paderborn@brandi.net

Minden
Königswall 47-49
32423 Minden
T +49 571 83706 - 0
F +49 571 83706 - 66
E minden@brandi.net

Hannover
Adenauerallee 12
30175 Hannover
T +49 511 899379 - 0
F +49 511 899379 - 77
E hannover@brandi.net

Paris
44, Avenue des Champs Elyées
F-75008 PARIS
T +33 1 44 95 20 00
F +33 1 49 53 03 97
E info@kleinwenner.eu

Beijing
Grandall Law Firm
9th Floor Taikang Financial Tower
No. 38 North Road East Third Ring
Choayang
Beijing (Peking) 100026
T +86 10 65 89 06 99
F +86 10 58 13 77 88
E peking@brandi.net

www.brandi.net