BRANDI
RECHTSANWÄLTE

ZUGRIFF DES ARBEITGEBERS AUF E-MAIL-ACCOUNTS VON ARBEITNEHMERN

Informationen zum Datenschutz I Dezember 2022

English version

Einleitung

Zur Ausübung ihrer Tätigkeit verfügen sehr viele Arbeitnehmer über einen dienstlichen E-Mail-Account. Der anlassbezogene Zugriff auf diese E-Mail-Accounts ist für viele Unternehmen ein relevantes Thema. Konkret stellt sich in der Praxis insoweit häufig die Frage, ob bzw. in welchen Fällen und in welchem Umfang der Arbeitgeber auf die dienstlichen E-Mail-Accounts seiner Mitarbeiter zugreifen darf und welche Anforderungen hierbei zu beachten sind.

Von besonderer praktischer Relevanz ist dabei zum einen der Fall, dass ein Zugriff auf das E-Mail-Postfach eines Mitarbeiters erforderlich ist, um die geschäftliche Korrespondenz des Arbeitnehmers im Falle von dessen Abwesenheit bearbeiten zu können. Zum anderen haben Arbeitgeber in bestimmten Fällen ein Interesse daran, zu überprüfen, ob der E-Mail-Account von einem Mitarbeiter missbräuchlich genutzt wird, etwa zur privaten Kommunikation während der Arbeitszeit oder gar zur Weitergabe von Geschäftsgeheimnissen.

Rechtsgrundlagen

Jede Datenverarbeitung – und dementsprechend auch der Zugriff auf ein E-Mail-Postfach – ist grundsätzlich nur dann zulässig, wenn sie auf eine Rechtsgrundlage gestützt werden kann. Es gilt insoweit das über Art. 6 Abs. 1 DSGVO verankerte Verbot mit Erlaubnisvorbehalt. Da es entgegen verschiedener Überlegungen in der Vergangenheit derzeit kein umfassendes Beschäftigtendatenschutzrecht gibt, ist bei der Verarbeitung von Mitarbeiterdaten auf die allgemeinen datenschutzrechtlichen Vorschriften der DSGVO und des BDSG sowie die spezielle Regelung des § 26 BDSG („Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“) zurückzugreifen.

Zwecke des Beschäftigungsverhältnisses, Vertragserfüllung und berechtigte Interessen

Als Rechtsgrundlage für den Zugriff auf das E-Mail-Postfach eines Mitarbeiters kommen insbesondere § 26 Abs. 1 S. 1 BDSG und Art. 6 Abs. 1 S. 1 lit. b) DSGVO in Betracht. Nach § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Die allgemeine Regelung gem. Art. 6 Abs. 1 S. 1 lit. b) DSGVO ist außerhalb der Durchführung des Beschäftigungsverhältnisses relevant und erfasst die Datenverarbeitung zur Erfüllung eines Vertrages mit dem Betroffenen. Liegt dementsprechend ein betriebliches Erfordernis mit Bezug zum Arbeitsverhältnis des Mitarbeiters – wie etwa die Vertretung und Bearbeitung offener Aufgaben im Abwesenheitsfall – für den Zugriff vor, können § 26 Abs. 1 S. 1 BDSG bzw. Art. 6 Abs. 1 S. 1 lit. b) DSGVO als Rechtsgrundlage herangezogen werden.

Fällt eine Person mangels Beschäftigteneigenschaft i. S. v. § 26 Abs. 8 BDSG (z. B. ein Geschäftsführer) nicht in den Anwendungsbereich von § 26 BDSG, kommt als weitere Rechtsgrundlage neben Art. 6 Abs. 1 S. 1 lit. b) DSGVO auch Art. 6 Abs. 1 S. 1 lit. f) DSGVO in Betracht. Nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO ist eine Datenverarbeitung dann zulässig, wenn das berechtigte Interesse des Verantwortlichen, also des Arbeitgebers, an der Datenverarbeitung die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegt. Es ist folglich eine Abwägung der Interessen der Beteiligten im konkreten Fall vorzunehmen. Ist ein Zugriff etwa erforderlich, um den Geschäftsbetrieb aufrechtzuerhalten, wird in der Regel von einem überwiegenden berechtigten Interesse auszugehen sein.

Aufdeckung einer Straftat

Soll auf das E-Mail-Postfach zugegriffen werden, um eine Straftat aufzudecken, kann der besondere Erlaubnistatbestand des § 26 Abs. 1 S. 2 BDSG herangezogen werden. Hiernach dürfen Daten von Beschäftigten zur Aufdeckung von Straftaten aber nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten nicht überwiegt. Steht also ein begründeter Verdacht einer Straftat eines Mitarbeiters im Beschäftigungsverhältnis im Raum, kann ein Zugriff nach § 26 Abs. 1 S. 2 BDSG zulässig sein.

Einwilligung

Als weitere Rechtsgrundlage kommt auch die Einwilligung des Betroffenen in den Zugriff auf das E-Mail-Postfach in Betracht. Es ist jedoch darauf zu achten, dass das Abstellen auf eine Einwilligung im Arbeitsverhältnis nicht unproblematisch ist. Nach § 26 Abs. 2 BDSG sind insoweit vor allem an die Freiwilligkeit der Einwilligung aufgrund des Abhängigkeitsverhältnisses zwischen Arbeitnehmer und Arbeitgeber hohe Anforderungen zu stellen. Inwieweit das Einholen einer Einwilligung des Betroffenen tatsächlich praktikabel ist, dürfte sich in der Regel nach dem Grund für den gewünschten Zugriff richten. Steht ein Fehlverhalten des Mitarbeiters im Raum, wird dieser wohl kaum seine Einwilligung in den Zugriff erteilen, während dies im Vertretungsfall wohl wahrscheinlich sein dürfte.

Betriebsvereinbarung
Schließlich kommt auch der Abschluss einer Betriebsvereinbarung zur Rechtfertigung des Zugriffs auf den E-Mail-Account eines Mitarbeiters in Betracht. Nach § 26 Abs. 4 BDSG ist die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, auch auf der Grundlage von Kollektivvereinbarungen zulässig. Der Abschluss einer Betriebsvereinbarung kann sich anbieten, wenn im Rahmen der Vereinbarung auch weitere Punkte, wie etwa der Ausschluss einer Privatnutzung und das konkrete Vorgehen im Zugriffsfall rechtssicher unter Berücksichtigung der Interessen von Arbeitgeber, Arbeitnehmer und Betriebsrat verbindlich geregelt und Unsicherheiten vermieden werden sollen.

Grundsatz der Verhältnismäßigkeit und der Datenminimierung
Grundsätzlich ist bei jedem Zugriff unabhängig von der konkreten Rechtsgrundlage eine Verhältnismäßigkeitsprüfung, also eine Abwägung zwischen den Interessen des Arbeitgebers und den Interessen des Arbeitnehmers erforderlich. Zudem ist der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c) DSGVO einzuhalten. Es darf insoweit nicht unbegrenzt, sondern nur in erforderlichem Umfang auf die E-Mails des Mitarbeiters zugegriffen werden.

Aus dem Verhältnismäßigkeitsgrundsatz kann sich darüber hinaus die Pflicht des Arbeitgebers ergeben, den betroffenen Arbeitnehmer – ggf. im Nachhinein – über den Zugriff auf sein E-Mail-Postfach zu informieren.

(Erlaubte) Privatnutzung des E-Mail-Accounts

Eine besondere Problematik ergibt sich dann, wenn Mitarbeitern die Privatnutzung ihres E-Mail-Accounts gestattet oder diese zumindest geduldet wird. Fraglich ist in diesem Fall zum einen, ob neben den datenschutzrechtlichen Bestimmungen aus DSGVO und BDSG auch das Fernmeldegeheimnis nach § 3 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) vom Arbeitgeber zu beachten ist. Weiter stellt sich die Frage, in welchen Fällen von einer erlaubten Privatnutzung auszugehen ist.

Anwendbarkeit des Fernmeldegeheimnisses
Nach Auffassung einiger Datenschutzaufsichtsbehörden findet das Fernmeldegeheimnis auch in Arbeitsverhältnissen Anwendung, sofern den Arbeitnehmern eine Privatnutzung ihres E-Mail-Accounts erlaubt ist. Der Arbeitgeber wird hierbei als Anbieter von Telekommunikationsdiensten eingeordnet, was zur Folge hat, dass der Arbeitgeber das Fernmeldegeheimnis zu beachten hat und nicht auf die E-Mail-Accounts seiner Mitarbeiter zugreifen darf. Anbieter von TKG-Diensten dürfen nur dann die übermittelten Inhalte einsehen, wenn dies zur Erbringung des Dienstes einschließlich des Schutzes der dafür notwendigen technischen Systeme erforderlich ist. Hiervon kann jedoch weder im Abwesenheitsfall zur Bearbeitung geschäftlicher Korrespondenz noch in vermeintlichen Missbrauchsfällen ausgegangen werden, sodass ein Zugriff auf das E-Mail-Postfach nach dieser Auffassung grundsätzlich gegen das Fernmeldegeheimnis verstoßen würde und damit unzulässig wäre.

Das LG Erfurt (LG Erfurt, Urt. v. 28.04.2021, Az. 1 HK O 43/20) und das LG Krefeld (LG Krefeld, Urt. v. 07.02.2018, Az. 7 O 175/17) lehnen die Anwendbarkeit des Fernmeldegeheimnisses bei erlaubter Privatnutzung hingegen ab und halten den Zugriff auf E-Mail-Accounts von Mitarbeitern in bestimmten Fällen für zulässig. Entsprechend der Ausführungen der Gerichte richtet sich die Rechtmäßigkeit der Einsichtnahme ausschließlich nach den datenschutzrechtlichen Vorschriften und Grundsätzen. Bereits verschiedene andere Gerichte haben in der Vergangenheit wie das LG Erfurt und das LG Krefeld entschieden (vgl. u. a. LAG Berlin-Brandenburg, Urt. v. 14.01.2016, Az. 5 Sa 657/15, LAG Niedersachsen, Urt. v. 31.05.2010, Az. 12 Sa 875/09). Gleichwohl ist die Rechtsprechung zu dieser Frage nicht einheitlich (a. A.: LAG Hessen, Urt. v. 21.09.2018, Az. 10 Sa 601/18, LAG Rheinland-Pfalz, Urt. v. 04.12.2017, Az. 3 Sa 143/17) und es fehlt es an einer abschließenden höchstrichterlichen Klärung der Thematik. Greift ein Arbeitgeber auf ein E-Mail-Postfach zu, obwohl dieses durch das Fernmeldegeheimnis geschützt ist, kann sich der Arbeitgeber nach § 206 Abs. 1 StGB strafbar machen. Zudem drohen empfindliche Geldbußen.

Selbst wenn man sich gegen die Anwendung des Fernmeldegeheimnisses ausspricht, bedeutet dies jedoch nicht, dass ein Zugriff jederzeit ohne Weiteres möglich ist; die bereits dargestellten datenschutzrechtlichen Grundsätze sind in jedem Fall zu berücksichtigen. Ist den Mitarbeitern die Privatnutzung ihres E-Mail-Accounts gestattet, bedeutet dies, dass dem Interesse des Arbeitgebers an einem Zugriff, gewichtige Interessen des Arbeitnehmers an der Wahrung seiner Privatsphäre gegenüberstehen und diese bei der Interessenabwägung in ausreichendem Maße zu berücksichtigen sind.

Erlaubte Privatnutzung
Bei einem dienstlichen E-Mail-Account handelt es sich vom Grundsatz her um ein Betriebsmittel. Wird ein solches Betriebsmittel Arbeitnehmern ohne weitere Informationen zur Verfügung gestellt, gilt der Grundsatz, dass dieses ausschließlich dienstlich genutzt werden darf und eine Privatnutzung gerade nicht zulässig ist, sodass der Anwendungsbereich des Fernmeldegeheimnisses grundsätzlich nicht eröffnet ist. Etwas anderes kann jedoch dann gelten, wenn die Mitarbeiter den E-Mail-Account gleichwohl privat nutzen, der Arbeitgeber hiervon Kenntnis hat und das Verhalten seiner Mitarbeiter nicht unterbindet. Nicht nur dann, wenn der Arbeitgeber die Privatnutzung ausdrücklich erlaubt hat, sondern auch, wenn er diese lediglich duldet, kann der Anwendungsbereich des Fernmeldegeheimnisses – je nach vertretener Auffassung – eröffnet sein. Nutzt ein Mitarbeiter den E-Mail-Account hingegen weisungswidrig privat, fehlt es an einem schutzwürdigen Interesse des Mitarbeiters.

Um Unsicherheiten zu vermeiden, empfiehlt es sich, die Thematik unternehmensintern ausdrücklich – etwa im Rahmen einer Datenschutz & IT-Richtlinie – zu regeln. Bestenfalls sollte Arbeitnehmern bis zu einer höchstrichterlich und gesetzlich abschließenden Klärung der Frage die Privatnutzung ihrer dienstlichen E-Mail-Accounts ausdrücklich verboten werden, um die Anwendbarkeit des Fernmeldegeheimnisses sicher auszuschließen und etwaige Zugriffsrechte im Einzelfall nicht grundsätzlich auszuschließen. Ein solches Verbot bedeutet für Arbeitnehmer schließlich nicht, dass diese nicht gelegentlich private E-Mails über einen Webmail-Dienst oder ihr privates Smartphone versenden dürfen. Sofern dennoch eine Privatnutzung des dienstlichen E-Mail-Accounts gestattet werden soll, sollten sich Unternehmen alternativ durch die ausdrückliche Einwilligung der Mitarbeiter von den Beschränkungen des Fernmeldegeheimnisses befreien lassen.

Zugriff bei Abwesenheit eines Mitarbeiters

Wird ein Mitarbeiter krank oder ist aus einem anderen Grund (zum Beispiel Urlaub oder Elternzeit) mitunter auch länger abwesend und wurden für den konkreten Fall vorab keine Vorkehrungen getroffen, wird häufig ein Zugriff des Arbeitgebers oder anderer Arbeitnehmer des Unternehmens auf das jeweilige E-Mail-Postfach erforderlich, um die betrieblichen Abläufe aufrechtzuerhalten. Insbesondere dann, wenn der abwesende Mitarbeiter über seinen E-Mail-Account größtenteils mit externen Personen kommuniziert, kann ein Zugriff

auf die E-Mails und eine Sichtung der jeweiligen Korrespondenz notwendig sein, um aktuell relevante Themen unternehmensseitig weiterverfolgen und zeitnah bearbeiten zu können.

Zugriff bei vorübergehender Abwesenheit

Um einem etwaigen Zugriffsbedarf und damit verbundenen Problemen vorzugreifen, empfiehlt es sich, bereits vorab allgemeine Regelungen für die Abwesenheit von Mitarbeitern festzulegen. Dieses gilt vor allem für planbare Abwesenheiten wie Urlaub oder Elternzeit. Als mildestes Mittel kommt insoweit das Einstellen einer automatischen Abwesenheitsnotiz durch den Mitarbeiter selbst in Betracht. Ist dies zum Beispiel aufgrund der Tätigkeit des Mitarbeiters oder der über den E-Mail-Account eingehenden Dokumente und Anfragen nicht ausreichend, kann auch eine Weiterleitung der E-Mails an die Vertretung des abwesenden Mitarbeiters angeordnet werden und vom Mitarbeiter vor dessen Abwesenheit einzurichten sein.

Bei nicht vorhersehbaren Abwesenheiten, wie etwa im Krankheitsfall, reichen derartige Vorgaben in der Regel nicht aus, da es dem Mitarbeiter mangels Zugriffsmöglichkeit häufig selbst nicht mehr möglich sein dürfte, die Abwesenheitsnotiz einzustellen oder eine E-Mail-Weiterleitung einzurichten. In diesem Fall kann ein Zugriff des Arbeitgebers auf den E-Mail-Account des Mitarbeiters erforderlich werden.

Der Zugriff und das anschließende Einrichten einer Abwesenheitsnotiz können sodann auf § 26 Abs. 1 S. 1 BDSG bzw. Art. 6 Abs. 1 S. 1 lit. b) DSGVO oder bei Personen, die nicht unter den Beschäftigtenbegriff fallen, auf Art. 6 Abs. 1 S. 1 lit. f) DSGVO gestützt werden. Gleiches gilt für die Anordnung oder Einrichtung einer E-Mail-Weiterleitung sowie den Zugriff auf zwischenzeitlich bereits eingegangene E-Mails, soweit die Sichtung und das weitere Mitlesen für die stellvertretende (Weiter-)Bearbeitung der Aufgaben oder das Aufrechterhalten des Geschäftsbetriebs erforderlich sind. Liegt eine Betriebsvereinbarung mit entsprechenden Regelungen für den Abwesenheitsfall vor, kann diese als Rechtsgrundlage für den Zugriff herangezogen werden. Darüber hinaus kommt ggf. auch eine Einwilligung des Mitarbeiters in Betracht.

Wird im Vertretungsfall auf ein E-Mail-Postfach zugegriffen, ist zudem grundsätzlich darauf zu achten, dass kein Dritter (etwa die Vertretung) über das E-Mail-Postfach des abwesenden Arbeitnehmers arbeitet, da ansonsten nicht mehr nachvollzogen werden kann, wer die E-Mails verfasst hat. Zur stellvertretenden Weiterbearbeitung offener Aufgaben sollte vielmehr ausschließlich das eigene Postfach verwendet werden.

Zugriff nach Ausscheiden eines Mitarbeiters

Auch nach dem Ausscheiden eines Mitarbeiters darf nicht ohne Weiteres auf dessen E-Mails zugegriffen werden. In diesem Fall ist für die Datenverarbeitung ebenfalls eine Rechtsgrundlage erforderlich. Es empfiehlt sich deshalb, die Thematik bereits im Vorfeld im Rahmen des Arbeitsvertrages oder einer gesonderten Vereinbarung zu regeln, damit keine für den Geschäftsbetrieb relevanten Informationen verloren gehen. Es kann etwa vereinbart werden, dass der Arbeitgeber nach Ausscheiden des Mitarbeiters auf dessen E-Mails zugreifen oder diese an den nunmehr zuständigen Kollegen weiterleiten darf. Alternativ kommt auch eine Verpflichtung des Mitarbeiters, offene Aufgaben im Falle des Ausscheidens zu übergeben und für den Geschäftsbetrieb erforderliche Dokumente und Korrespondenz an einem bestimmten Speicherort abzulegen, in Betracht. Im Übrigen kann hinsichtlich der Rechtsgrundlagen auf die Ausführungen zur vorübergehenden Abwesenheit verwiesen werden.

Zugriff bei Verdacht auf missbräuchliches Verhalten

Hat der Arbeitgeber den Verdacht, dass ein Mitarbeiter sein dienstliches E-Mail-Postfach missbräuchlich verwendet, etwa durch eine übermäßige Privatnutzung, die Weitergabe von Geschäftsgeheimnissen oder gar den Verkauf von Kundendaten, besteht auf Seiten des Unternehmens häufig der Wunsch, auf das E-Mail-Postfach des Mitarbeiters zuzugreifen, um dem Verdacht nachzugehen und den Sachverhalt zu klären. Insbesondere auch für diese mitunter streitbehafteten Fälle bietet sich der Abschluss einer entsprechenden Betriebsvereinbarung an, um zügig und rechtssicher handeln zu können.

Steht der konkrete Verdacht im Raum, dass ein Mitarbeiter im Rahmen seines Beschäftigungsverhältnisses eine Straftat begangen hat – insoweit kommt etwa die Weitergabe von Geschäftsgeheimnissen und vertraulichen Informationen oder der Verkauf von Kundendaten in Betracht –, kann der Zugriff auch nach § 26 Abs. 1 S. 2 BDSG gerechtfertigt werden, soweit die Voraussetzungen der Norm erfüllt sind. Konkret muss der Verdacht sich zunächst auf eine Straftat beziehen, diese muss im Beschäftigtenverhältnis begangen worden sein, es müssen tatsächliche Anhaltspunkte für den Verdacht vorliegen und der Zugriff muss erforderlich sein, um die Straftat aufzudecken. Schließlich ist wiederum eine Abwägung der sich gegenüberstehenden Interessen vorzunehmen.

Geht der Arbeitgeber hingegen lediglich davon aus, dass ein Arbeitnehmer seine arbeitsvertraglichen Pflichten zum Beispiel durch eine übermäßige Privatnutzung verletzt hat, kann § 26 Abs. 1 S. 2 BDSG mangels einer Straftat grundsätzlich nicht herangezogen werden. In diesem Fall ist vielmehr wiederum ein Rückgriff auf § 26 Abs. 1 S. 1 BDSG erforderlich. Zusätzliche Probleme können sich allerdings dadurch ergeben, dass der Arbeitgeber bereits von einer Privatnutzung ausgeht, wodurch sich die Interessenabwägung aufgrund des Schutzes der Privatsphäre des Arbeitnehmers unter Umständen zu dessen Gunsten verschieben kann. Angesichts der Sensibilität und Streitanfälligkeit des Themas, sollte zunächst eine Prüfung des Falls durch den Datenschutzbeauftragten erfolgen.

Vorgehen beim Zugriff auf den E-Mail-Account

Ist der Zugriff auf das E-Mail-Postfach von einer Rechtsgrundlage gedeckt, stellt sich im Weiteren die Frage, wie bei dem Zugriff konkret vorzugehen ist. Grundsätzlich sollte unternehmensseitig zunächst berücksichtigt werden, dass nicht nur die im konkreten Fall einschlägige Rechtsgrundlage, sondern auch das weitere Vorgehen von den jeweiligen Umständen des Einzelfalls abhängen. Um sicherzustellen, dass die datenschutzrechtlichen Vorschriften eingehalten und die Interessen des Arbeitnehmers ausreichend gewahrt werden, bietet sich grundsätzlich ein Vorgehen nach dem „Mehr-Augen-Prinzip“. Gibt es einen Betriebsrat, dürfte es in der Regel sinnvoll sein, diesen zu beteiligen. Zudem bietet es sich an, vorab eine Bewertung der Situation durch den Datenschutzbeauftragten einzuholen und das konkrete Vorgehen mit ihm abzustimmen, auch wenn dieser den Zugriff letztlich nicht zwingend unmittelbar begleiten muss. Zu Nachweiszwecken sollte der Zugriff zudem detailliert protokolliert und die jeweiligen Erwägungen über den Zugriff, insbesondere die Interessenabwägung, dokumentiert werden.

Fazit

Der Zugriff auf E-Mail-Accounts von Arbeitnehmern bringt viele Fragen mit sich und ist insbesondere dann, wenn eine Privatnutzung nicht sicher ausgeschlossen ist, nicht unproblematisch. Es ist deshalb sinnvoll, bereits im Vorfeld klare Regelungen für den Zugriff auf ein E-Mail-Postfach aufzustellen, um Unsicherheiten und einem etwaigen Streitpotential aus dem Weg zu gehen. Insoweit bietet

sich insbesondere auch der Abschluss einer entsprechenden Betriebsvereinbarung sowie einer Datenschutz & IT-Richtlinie an, im Rahmen derer darüber hinaus auch andere Fragen zur Nutzung der IT-Systeme geregelt werden können.

Ist der Zugriff auf den E-Mail-Account eines Mitarbeiters im Arbeitsalltag tatsächlich einmal erforderlich, sollte ein datenschutzkonformer Umgang mit den Daten in jedem Fall durch entsprechende Absicherungsmaßnahmen, wie die Nutzung des „Mehr-Augen-Prinzips“ und eine umfassende Dokumentation, sichergestellt werden. In Anbetracht der Sensibilität des Themas und der möglichen Konsequenzen bei einem unberechtigten Zugriff, bietet sich zudem die Abstimmung des konkreten Vorgehens mit dem Datenschutzbeauftragten an.

Christina Prowald

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Christina Prowald
Wissenschaftliche Mitarbeiterin

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