Datenschutzrecht

August 2017

Die Einwilligung in E-Mail-Werbung und der Umgang mit sog. Robinson-Listen bei Widerspruch des Betroffenen

Der Bundesgerichtshof hat seine Rechtsprechung konkretisiert, wonach eine wirksam vorformulierte Einwilligungserklärung in den Erhalt von Werbe-E-Mails voraussetzt, dass hieraus unmissverständlich hervorgeht, von welchem Unternehmen die Werbung stammt und welche konkreten Produkte oder Leistungen beworben werden (Urt. v. 14.03.2017 – VI ZR 721/15).

Im zugrundliegenden Fall verneinte der BGH eine wirksame Einwilligung wegen des Vorliegens einer (verdeckten) Generaleinwilligung. Das werbende Unternehmen hatte auf seiner Internetseite eine Software zum kostenlosen Download angeboten. Zum Start des Downloads waren die Angabe einer E-Mail-Adresse und die Annahme der Nutzungsbedingungen erforderlich, in der eine vorformulierte Einwilligungserklärung in E-Mail-Werbung enthalten war. Im Rahmen dieser Einwilligungserklärung kam man über einen als „hier" betitelten Link auf eine Liste von Sponsoren bzw. Werbepartnern, die von der Einwilligung zum Erhalt von Werbe-E-Mails erfasst sein sollten. Eine Umschreibung der zu bewerbenden Waren und Dienstleistungen fehlte. Problematisch war aus Sicht des BGH vor allem, dass einige dieser Sponsoren Marketingunternehmen waren, die wiederum für andere Kunden Werbekampagnen entwerfen. Hierdurch werde der Kreis der beworbenen Unternehmen gänzlich unübersehbar. Durch die Formulierung der Klausel werde dem Einwilligenden hingegen der Eindruck vermittelt, dass er nur in den Erhalt von Werbung des konkreten Softwareanbieters einwillige, diese sich folglich auf die Werbung für Software beziehe. Tatsächlich enthalte die Klausel aber eine unzulässige, weil verdeckte, Generaleinwilligung (§ 7 Abs. 1 UWG). Vorformulierte Einwilligungserklärungen unterlägen zudem der AGB-Kontrolle, weshalb hier von einem Verstoß gegen das Transparenzgebot im Sinne des § 307 Abs. 1 Satz 1 und 2, Abs. 3 Satz 2 BGB auszugehen sei.

Des Weiteren setzt sich der BGH mit der Frage auseinander, ob eine Verarbeitung personenbezogener Daten trotz Widerspruchs zulässig ist, wenn der zur Unterlassung von Werbung Verpflichtete die E-Mail-Adresse des Betroffenen gegen dessen Willen nutzen möchte, um sie zu Lösch- und Sperrzwecken an seine Werbepartner weiterzuleiten. Im konkreten Fall hatte das abgemahnte Unternehmen angekündigt, die E-Mail-Adresse des Abmahnenden auf eine sog. interne Robinson-Liste setzen zu wollen, um so den zukünftigen Versand von E-Mail-Werbung an diesen Adressaten zu unterbinden. Dem widersprach der betroffene E-Mail-Empfänger.

Nimmt das Unternehmen den Widersprechenden auf eine Sperrliste, um den Widerspruch auch für die Zukunft beachten zu können, liegt darin eine Verarbeitung personenbezogener Daten, die nach Auffassung des BGH grundsätzlich gemäß § 28 Abs. 1 Nr. 2 BDSG gestattet ist, da ein berechtigtes Interesse des Werbenden vorliegt, keine unerwünschte E-Mail-Werbung zu versenden. Selbst wenn der Betroffene der Aufnahme seiner E-Mail-Adresse in die Sperrliste ausdrücklich widerspreche, sei es möglich, dass die hier erforderliche Interessenabwägung zu dem Ergebnis führe, dass ausnahmsweise die berechtigten Interessen des werbenden Unternehmens zur Erfüllung der eigenen Unterlassungsverpflichtung überwiegen. Der BGH stellt jedoch klar, dass diese Erwägungen ausschließlich für die betroffene E-Mail-Adresse gelten, da der Werbetreibende diesbezüglich ein konkretes Interesse hat, die in der Unterlassungsverpflichtung enthaltene Folgenbeseitigung zur Vermeidung weitergehender Ansprüche umzusetzen. Das Interesse gehe jedoch nicht so weit, alle E-Mail-Adressen eines Betroffenen auf die Sperrliste zu setzen, um etwaige zukünftige Abmahnungen zu vermeiden. Der BGH weist darauf hin, dass es im Aufgabenbereich des Werbetreibenden liegt, rechtswirksame Einwilligungen für seine Werbe-E-Mails einzuholen. Wenn er dieser Verpflichtung nachkomme, könne ihm auch keine Abmahnung drohen, weshalb er dann auch kein berechtigtes Interesse daran haben könne, diese E-Mail-Adressen zusätzlich zu sperren.

Praxishinweis
Mit dem Urteil führt der BGH seine Rechtsprechung zu den Wirksamkeitsvoraussetzungen einer Einwilligung zu Werbezwecken fort und gibt Hinweise, in welchen Fällen die Nutzung einer sog. Robinson-Liste selbst gegen den Willen des Betroffenen zulässig sein kann.

Welche Kriterien für die Wirksamkeit einer Einwilligung in Werbe-E-Mails zu erfüllen sind, hat der BGH mehrfach konkretisiert. Danach ist die Einwilligung des Verbrauchers nur dann wirksam, wenn die „*Willensbekundung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage*" erfolgt. „*Für den konkreten Fall*" erfolgt eine Einwilligung, wenn klar wird, welche Produkte oder Dienstleistungen welcher Unternehmen erfasst sind. Unbeantwortet bleibt hingegen die Frage, ob eine über einen Link erreichbare Liste von Werbepartnern die Anforderungen an das Transparenzgebot erfüllen kann. Unternehmen, die derartige Listen in ihren Nutzungsbedingungen über einen Link integrieren, sollten diese auf den Prüfstand stellen. In jedem Fall sind Listen mit aufgeführten Werbepartnern vor dem Hintergrund des Transparenzgebots so verständlich wie nur möglich zu formulieren und die zu bewerbenden Waren und Dienstleistungen sollten konkret benannt werden.

Berücksichtigen Unternehmen die Wirksamkeitserfordernisse an eine Einwilligungserklärung nicht hinreichend, riskieren sie Beseitigungs- und Unterlassungsansprüche der Betroffenen, von Wettbewerbern wie auch von Verbraucherschutzorganisationen. Angesichts der Tatsache, dass im Falle einer unwirksamen Einwilligung bereits die Übermittlung der E-Mail-Adressen an Werbepartner einen Datenschutzverstoß darstellt, können hier zusätzlich hohe Bußgelder der Aufsichtsbehörden für den Datenschutz drohen. Insgesamt dürfte das Abmahnrisiko insbesondere in den Fällen hoch sein, in denen die Einwilligungserklärung über eine Webseite eingeholt wird und damit für jedermann leicht zugänglich und überprüfbar ist.

Gerade auch im Hinblick auf die ab dem 25. Mai 2018 geltende EU-Datenschutz-Grundverordnung („DSGVO") sollten die derzeit verwendeten Vorlagen für die Einwilligungserklärung auf ihre Vereinbarkeit mit dem zukünftigen Datenschutzrecht, insbesondere dem verschärften Kopplungsverbot, wie auch allgemein auf deren Verständlichkeit und Transparenz überprüft werden.

Dr. Claudio G. Chirco,
Rechtsanwalt, Fachanwalt für Informationstechnologierecht

Schmerzensgeld wegen konzerninterner Weitergabe von Gesundheitsdaten

Das Oberlandesgericht Düsseldorf hat entschieden, dass die ungerechtfertigte Weitergabe von Gesundheitsdaten innerhalb eines Konzerns einen Schadensersatzanspruch begründen kann, der auch Schmerzensgeld umfasst (Urt. v. 30.09.2016 – Az. 20 U 83/16).

Dem Sachverhalt lag ein Gerichtsurteil aus einem früheren Verfahren zugrunde, welches Gesundheitsdaten des Klägers enthielt. Streitgegenstand dieses früheren Verfahrens waren Ansprüche aus einer Berufsunfähigkeitsversicherung, die der Kläger gegen die beklagte Versicherungsgesellschaft geltend machte. Ohne die Gesundheitsdaten zu anonymisieren, gab die Beklagte sodann das Urteil an den Arbeitgeber des Klägers weiter, der auch gleichzeitig die Konzernmutter der Beklagten war. Grund für die Weitergabe des Urteils war

die Prüfung einer möglichen Strafanzeige gegen den Kläger durch die Konzernrechtsabteilung. Das OLG Düsseldorf hatte nun zu überprüfen, ob diese Weitergabe gerechtfertigt war.

Gesundheitsdaten zählen nach den Vorgaben des Bundesdatenschutzgesetzes („BDSG") zu den besonders schützenswerten personenbezogenen Daten (§ 3 Abs. 9 BDSG). Grundsätzlich kann auch die Weitergabe solcher Daten an einen Dritten durch eine Einwilligung des Betroffenen gerechtfertigt werden. Tatsächlich hatte der Kläger der Beklagten eine Einwilligung in die Verwendung seiner Gesundheitsdaten zwecks Gewährung von Leistungen aus der Berufsunfähigkeitsversicherung erteilt, die auch die Datenverwendung durch andere Personen innerhalb des Konzerns zum Zweck der Erledigung der ihnen übertragenen Aufgaben umfasste. Dennoch hielt das OLG Düsseldorf die mit der Urteilsweitergabe verbundene Datenübermittlung für unzulässig. Die Prüfung einer Strafanzeige durch die Konzernmutter sei von der Einwilligung des Klägers nicht umfasst gewesen, weshalb die Beklagte mit der Urteilsweitergabe eine unzulässige Zweckänderung vorgenommen habe.

Auch eine Rechtfertigung gemäß § 28 Abs. 6 Nr. 3, Abs. 8 BDSG komme vorliegend nicht in Betracht. Hiernach sei eine Übermittlung besonders schützenswerter Daten ohne Vorliegen einer Einwilligung nur gerechtfertigt, wenn sie dem eigenen geschäftlichen Zweck des Übermittlers diene und zur Geltendmachung von rechtlichen Ansprüchen erforderlich sei. Die Prüfung einer Strafanzeige durch die Konzernmutter gehöre jedoch nicht dazu. Das Gericht hob hervor, dass dem deutschen Datenschutzrecht ein Konzernprivileg unbekannt ist und somit der geschäftliche Zweck der Konzernmutter (Prüfung einer Strafanzeige) nicht gleichzeitig der eigene Geschäftszweck der Beklagten sein kann.

Zusätzlich beanstandete es die vollständige und nicht anonymisierte Weitergabe des Urteils. Ein solches Vorgehen stehe nicht im Einklang mit den datenschutzrechtlichen Grundsätzen der Datenvermeidung und Datensparsamkeit und könne auch nicht als erforderlich angesehen werden. Vielmehr hätte die Beklagte sich bei der Weitergabe auf solche Gesundheitsdaten beschränken müssen, die für die Prüfung einer Strafanzeige notwendig gewesen wären.

Praxishinweis
Die Entscheidung verdeutlicht, wie wichtig eine konsequente Anwendung der datenschutzrechtlichen Grundprinzipien bei der konzerninternen Datenübermittlung ist und dass deren Nichtbeachtung zu Schadensersatzansprüchen führen kann. Sofern die Datenverarbeitung durch eine Einwilligung gerechtfertigt wird, sind die Vorgaben für die Wirksamkeit der Einwilligungserklärung besonders relevant. Namentlich der Zweckbindungsgrundsatz ist von hervorgehobener Bedeutung: Die verantwortliche Stelle muss in der vorformulierten Einwilligungserklärung die Zwecke der zukünftigen Datenverarbeitung hinreichend genau angeben. Zwar hat eine weite Zweckformulierung den Vorteil, dass der Verantwortliche bei einer späteren Erweiterung der Datenverarbeitung nicht unbedingt eine zusätzliche Einwilligung einholen muss. Allerdings müssen zugleich die Verwendungszwecke für den Betroffenen klar genug formuliert sein, damit dieser erkennen kann, was mit seinen Daten zukünftig geschieht (siehe hierzu auch den ersten Beitrag).

Unbeschadet dessen müssen stets die Grundsätze der Datenvermeidung und Datensparsamkeit beachtet werden. Sofern möglich und kein unverhältnismäßiger Aufwand betrieben werden muss, sind personenbezogene Daten bei der Verarbeitung zu anonymisieren oder zu pseudonymisieren.

Die Feststellung des Gerichts, dass dem deutschen Datenschutzrecht ein Konzernprivileg fremd ist, gibt lediglich die (noch) aktuelle Rechtslage wieder. Es ist allgemein anerkannt, dass ein konzerninterner Datenaustausch der Einwilligung der Betroffenen bedarf oder auf einer gesetzlichen Erlaubnisnorm beruhen muss. Dennoch werden sich die deutschen Aufsichtsbehörden und Gerichte zukünftig mit dem Konzernprivileg als Erlaubnistatbestand auseinanderzusetzen haben: Die DSGVO sieht in der konzerninternen Datenverarbeitung ein berechtigtes Interesse der verantwortlichen Stelle, welches als Rechtfertigungsgrund in Frage kommen kann. Inwieweit sich Konzernunternehmen daher ab dem 25. Mai 2018 auf ein Konzernprivileg berufen können, bleibt abzuwarten.

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin für Informationstechnologierecht
und wissenschaftlicher Mitarbeiter **Florian Groothuis**

Kein „Recht auf Vergessenwerden" für Gesellschaftsregister-Einträge

Der EuGH hat entschieden, dass ein „Recht auf Vergessenwerden" für personenbezogene Daten, die im Gesellschaftsregister eingetragen sind, nicht besteht (Urteil v. 09.03.2017 – C-398/15).

Geklagt hatte der italienische Geschäftsführer einer Baufirma, der im Gesellschaftsregister noch als alleiniger Geschäftsführer und Liquidator einer früheren, insolvent gewordenen Gesellschaft eingetragen war. Da sich der Eintrag seiner Auffassung nach geschäftsschädigend auf seine aktuelle berufliche Tätigkeit auswirkte, verlangte er von der zuständigen Handelskammer die Anonymisierung seiner personenbezogenen Daten, die ihn mit der Insolvenz der früheren Gesellschaft in Verbindung brachten. Die Berufungsinstanz legte dem EuGH die Frage vor, ob die Datenschutzrichtlinie (RL 95/46/EG) und die Richtlinie über die Offenlegung von Gesellschaftsurkunden (RL 68/151/EWG) eine dauerhafte Zugänglichkeit zu personenbezogenen Daten im Gesellschaftsregister verbieten.

Der EuGH wies zunächst auf die unterschiedlichen Ziele der beiden Richtlinien hin. So stünden dem Schutz personenbezogener Daten und dem daraus resultierenden Grundrecht, eine Löschung oder Sperrung von Daten zu verlangen, wenn diese nicht mehr benötigt werden, die Offenlegungszwecke von Gesellschaftsregistern gegenüber. Deren Ziel sei es, dass sich jeder, der Geschäftsverbindungen mit Gesellschaften in anderen Mitgliedstaaten aufnehmen oder fortsetzen wolle, unschwer Kenntnis von den wesentlichen Angaben über die Gründung der Handelsgesellschaften und über die Befugnisse der mit ihrer Vertretung betrauten Personen verschaffen könne. Daher müssten alle einschlägigen Angaben ausdrücklich im Register aufgeführt werden und allen interessierten Dritten zugänglich sein, ohne dass diese ein schutzbedürftiges Recht oder Interesse nachweisen müssten. Dabei könnten auch nach Auflösung einer Gesellschaft Rechte und Rechtsbeziehungen in Bezug auf diese fortbestehen und auch noch mehrere Jahre später Fragen auftreten, die einen Rückgriff auf diese Daten erforderten. In Anbetracht der Vielzahl möglicher Szenarien, in denen die Daten noch benötigt werden könnten, und der unterschiedlichen Verjährungsfristen in den Mitgliedstaaten erscheine es daher nicht möglich, eine einheitliche Frist festzulegen, die mit der Auflösung einer Gesellschaft zu laufen beginne und nach deren Ablauf die Eintragung der Daten im Register und ihre Offenlegung nicht mehr notwendig wären.

Zwar stelle dies einen Eingriff in die Grundrechte der betroffenen Person dar, namentlich in das Recht auf Achtung des Privatlebens und auf Schutz ihrer personenbezogenen Daten. Dies sei aber nicht unverhältnismäßig, weil schließlich nur eine begrenzte Anzahl von personenbezogenen Daten im Gesellschaftsregister eingetragen werde. Zudem betonte der EuGH, dass Personen, die über eine Aktiengesellschaft oder eine GmbH am Wirtschaftsleben teilnehmen, diesbezüglich eine aktive Entscheidung treffen und deshalb auch verpflichtet sind, die Daten zu ihren Personalien und Aufgaben innerhalb der Gesellschaft offenzulegen. Dies gelte insbesondere dann, wenn zum Schutz Dritter lediglich das Vermögen der jeweiligen Gesellschaft zur Verfügung stehe.

Allein in eng begrenzten Einzelfällen könne es gerechtfertigt sein, den Zugang zu den im Register eingetragenen personenbezogenen Daten nach Ablauf einer hinreichend langen Frist nach Auflösung der Gesellschaft auf solche Dritte zu beschränken, die ein besonderes Interesse an der Einsichtnahme in diese Daten nachweisen. Allerdings

sei es Sache der nationalen Gesetzgeber, derartige Ausnahmetatbestände in den anwendbaren Gesetzen zu schaffen.

Praxishinweis
Der EuGH trifft die klare Aussage, dass die Publizität des Registers einschließlich der dort gespeicherten und öffentlich zugänglichen personenbezogenen Daten Vorrang genießt und der Datenschutz dahinter zurücktreten muss.

Zwar sind Ausnahmen von diesen Grundsätzen prinzipiell möglich. Der Zugang zu den personenbezogenen Registerdaten soll aber nur in besonderen Situationen aufgrund überwiegender, schutzwürdiger und sich aus dem konkreten Fall der Person ergebenden Gründen beschränkt werden. Damit stellt der EuGH eine hohe Hürde für etwaige Ausnahmetatbestände auf, die zudem erst noch von den nationalen Gesetzgebern geschaffen werden müssen. Im vorliegenden Fall hat der EuGH dementsprechend auch das Vorliegen einer solchen Ausnahme abgelehnt. Allein der Umstand, dass sich die Immobilien des Klägers nicht verkaufen ließen, weil die potenziellen Käufer Zugang zu den über ihn im Gesellschaftsregister gespeicherten Daten haben, reiche nicht für die Rechtfertigung einer Zugangsbeschränkung zu diesen Daten aus, zumal die Käufer ein berechtigtes Interesse gerade an der Kenntnis dieser Daten haben könnten.

Personen, die als Geschäftsführer oder sonstige Vertreter von Gesellschaften tätig sind bzw. sein wollen, sollten sich daher bewusst sein, dass ihre diesbezüglichen im Register eingetragenen Daten öffentlich zugänglich sind und bis auf weiteres auch bleiben werden.

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin für Informationstechnologierecht

Sonderkündigungsschutz für stellvertretenden Datenschutz-Beauftragten

Das LAG Hamburg hat den nachwirkenden Sonderkündigungsschutz auch auf den stellvertretenden Datenschutzbeauftragten für anwendbar erklärt (Urt. v. 21.07.2016 – Az. 8 Sa 32/16).

Nach § 4f Abs. 3 S. 5, 6 BDSG genießt der betriebliche Datenschutzbeauftragte einen besonderen Kündigungsschutz, da eine Kündigung des Arbeitsverhältnisses unzulässig ist, außer wenn Tatsachen vorliegen, welche die verantwortliche Stelle zu einer fristlosen Kündigung aus wichtigem Grund berechtigen. Dieser besondere Kündigungsschutz gilt noch für ein Jahr nach der Abberufung als Datenschutzbeauftragter fort. Streitig waren nun die Fragen, ob überhaupt ein stellvertretender Datenschutzbeauftragter verpflichtend zu bestellen ist und ob auch dieser in den Genuss der Privilegierung kommt.

Das Gericht stellte zunächst fest, dass es im BDSG an einer gesetzlichen Vorschrift fehlt, die eine verantwortliche Stelle zur Bestellung eines stellvertretenden Datenschutzbeauftragten explizit auffordert. Jedoch ergebe sich eine solche Pflicht aus dem Sinn und Zweck von § 4f Abs. 3 BDSG. Nach Auffassung des Gerichts ist der Verantwortliche zur Bestellung eines stellvertretenden Datenschutzbeauftragten jedenfalls dann verpflichtet, wenn der ursprüngliche Datenschutzbeauftragte über einen länger andauernden Zeitraum verhindert ist und es hierdurch an der gesetzlich vorgesehenen Kontrollinstanz zur Einhaltung datenschutzrechtlicher Regelungen im Unternehmen fehlt.

Der Sonderkündigungsschutz und seine einjährige Nachwirkung greifen zugunsten des Stellvertreters aber nur, wenn dieser auch tatsächlich tätig wird und die Aufgaben des verhinderten Datenschutzbeauftragten wahrnimmt. Grund für den gesetzlich vorgesehenen Sonderkündigungsschutz ist die Tatsache, dass der Arbeitnehmer, der gleichzeitig als Datenschutzbeauftragter bestellt ist, sich regelmäßig in einem Spannungsfeld zwischen der Einhaltung und Verbesserung des Datenschutzes und den Interessen des Arbeitgebers befindet. Deshalb soll der nachwirkende Sonderkündigungsschutz eine unbelastete Aufgabenwahrnehmung gewährleisten. Nach Auffassung des LAG Hamburg tritt der stellvertretende Datenschutzbeauftragte durch die Wahrnehmung dieser Funktion in alle Rechte und Pflichten des originären Datenschutzbeauftragten ein. Er sei damit dem gleichen Risiko ausgesetzt, mit dem Arbeitgeber in Konflikt zu geraten, und es sei kein sachlicher Grund ersichtlich, warum der Stellvertreter trotz nur vorübergehender Wahrnehmung der Funktion eines Datenschutzbeauftragten weniger schutzbedürftig sein sollte. Daher sei ein gleichwertiger Kündigungsschutz mit Nachwirkung angemessen.

Praxishinweis
Die Entscheidung zeigt, dass Unternehmen, die verpflichtet sind einen Datenschutzbeauftragten zu bestellen, bei dessen längerfristigen Verhinderung auch verpflichtet sind, einen Stellvertreter zu benennen. Wird dieser auch tatsächlich tätig, genießt er einen Sonderkündigungsschutz, welcher nach Beendigung der Tätigkeit innerhalb eines Jahres weiter bestehen bleibt. Vor diesem Hintergrund sollten Unternehmen sich frühzeitig, idealerweise schon bei Bestellung des betrieblichen Datenschutzbeauftragten Gedanken darüber machen, welche Person als dessen Stellvertreter in Betracht kommt, damit es nicht bei einem unvorhergesehenen Ausfall des originären Datenschutzbeauftragten zu einer überstürzten Entscheidung kommt, die in personeller Hinsicht für den Arbeitgeber lange Nachwirkungen haben könnte.

Susanne Klein, LL.M.
Rechtsanwältin, Fachanwältin für Informationstechnologierecht
und wissenschaftlicher Mitarbeiter **Florian Groothuis**

Krisenfall Cyberattacke – Sind Sie vorbereitet?

Nicht erst seit der weltweiten Cyberattacke „WannaCrypt" (in den Medien auch bekannt als „WannaCry"), bei der im Mai 2017 mehr als 200.000 Computersysteme angegriffen wurden, steht fest: Schwachstellen von Hard- und Software werden immer wieder gezielt für kriminelle Zwecke genutzt. Unternehmen sollten daher gewappnet sein.

Angesichts der zunehmenden Bedeutung von Kundendaten als wichtigem Erfolgsfaktor für viele Unternehmen werden solche Daten auch für Kriminelle interessant.

Im Ernstfall bestehen umfassende Melde- und Informationspflichten. Ab dem 25. Mai 2018 werden die Bußgelder durch DSGVO drastisch erhöht (bis zu 4 Prozent des weltweiten Konzernumsatzes). Die proaktive Erstellung einer Reaktionsstrategie ist für den Ernstfall also unerlässlich.

Krisenteam statt Einzelkämpfer!

Ein optimaler Umgang mit Cyberattacken gelingt nur durch eine enge Zusammenarbeit verschiedener (interner und/oder externer) Stellen. Es empfiehlt sich, für den Krisenfall ein Team aus den Bereichen IT/Technik, Recht und PR/Marketing zusammenzustellen. Entscheidend ist dabei die enge Abstimmung zwischen den Teammitgliedern, um hier eine einheitliche Handlungs- und Kommunikationsstrategie zu erreichen.

Melde- und Informationspflichten

Derzeit müssen bei Vorfällen, bei denen vom Gesetzgeber als besonders sensibel eingestufte Daten in falsche Hände gelangt sein könnten, sowohl die hiervon betroffenen Personen als auch die zuständige Datenschutzbehörde informiert werden (vgl. § 42a BDSG). Dies ist insbesondere immer dann der Fall, wenn sog. besondere Arten personenbezogener Daten i.S.v. § 3 Abs. 9 BDSG (z.B. Angaben über die ethnische Herkunft, Religion, Gesundheit oder Sexualleben) oder Bank- bzw. Kreditkartendaten betroffen sind und hierdurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Nach der neuen DSGVO – also ab dem 25. Mai 2018 – gilt die Meldepflicht sogar bei jedem Vorfall, der „zur Vernichtung, zum Verlust,

zur Veränderung, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt". Eine Ausnahme besteht nur dann, wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33, 34 DSGVO).

Sechs Schritte aus der Krise

Sobald im Unternehmen ein Vorfall bekannt wird, bei dem auch personenbezogene Daten betroffen sein können, hat sich in der Praxis folgendes Vorgehen bewährt:

- Interne Ermittlung von Art und Umfang des Datenmissbrauchs bzw. Datenverlusts.
- Umsetzung technischer und organisatorischer Maßnahmen zur Beseitigung des Datenlecks.
- Anwaltliche Prüfung, ob und in welchem Umfang Melde- und Benachrichtigungspflichten bestehen.
- Bei Vorliegen der gesetzlichen Voraussetzungen: Unverzügliche Information des zuständigen Landesdatenschutzbeauftragten.
- Erstattung Strafanzeige.
- Nach Abstimmung des weiteren Vorgehens mit Datenschutz- und Strafverfolgungsbehörden: Information der Betroffenen (soweit erforderlich).

Dabei hat die Praxis gezeigt: Im Krisenfall ist die Datenschutzbehörde oft als Verbündeter des betroffenen Unternehmens anzusehen. Eine Benachrichtigung sollte somit schnell, vollständig und transparent erfolgen.

Es ist daher zweckmäßig, für den Krisenfall unternehmensinterne Verantwortlichkeiten und Prozesse im Vorfeld zu definieren, um so die Folgen einer Cyberattacke für das Unternehmen und die Betroffenen so gering wie möglich zu halten.

Mathias Zimmer-Goertz
Rechtsanwalt

Hinweise

Diese Veröffentlichung stellt keine Rechtsberatung dar.

Wenn Sie diesen Newsletter nicht mehr erhalten möchten, können Sie jederzeit per E-Mail (bitte E-Mail mit Betreff „Abbestellen" an **Melanie.Jost@bblaw.com**) oder sonst gegenüber BEITEN BURKHARDT widersprechen.

Impressum

BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
(Herausgeber)
Ganghoferstraße 33, D-80339 München
AG München HR B 155350/USt.-Idnr: DE-811218811

Weitere Informationen (Impressumsangaben) unter:
https://www.beiten-burkhardt.com/de/hinweise/impressum

Redaktion (verantwortlich)

Dr. Andreas Lober
Susanne Klein, LL.M.

Autoren

Dr. Claudio G. Chirco,
Rechtsanwalt, Fachanwalt für Informationstechnologierecht
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Düsseldorf

Susanne Klein, LL.M.,
Rechtsanwältin, Fachanwältin für Informationstechnologierecht
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Frankfurt am Main

Mathias Zimmer-Goertz,
Rechtsanwalt
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Düsseldorf

Weitere interessante Themen und Informationen zum Datenschutzrecht finden Sie in unserem Onlinebereich.

Ihre Ansprechpartner

Berlin • Kurfürstenstraße 72-74 • 10787 Berlin
Tel.: +49 30 26471-0 • Fax: +49 30 26471-123
Dr. Matthias Schote • Matthias.Schote@bblaw.com

Düsseldorf • Cecilienallee 7 • 40474 Düsseldorf
Tel.: +49 211 518989-0 • Fax: +49 211 518989-29
Mathias Zimmer-Goertz • Mathias.Zimmer-Goertz@bblaw.com

Frankfurt am Main • Mainzer Landstraße 36
60325 Frankfurt am Main
Tel.: +49 69 756095-0 • Fax: +49 69 756095-512
Dr. Andreas Lober • Andreas.Lober@bblaw.com

München • Ganghoferstraße 33 • 80339 München
Tel.: +49 89 35065-0 • Fax: +49 89 35065-123
Dr. Axel von Walter • Axel.Walter@bblaw.com