

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

der Datenschutz ist voller Dynamik: Neue technische Entwicklungen, neue Bedrohungen, neue Gesetze und die aktuelle Rechtsprechung beeinflussen den Schutz personenbezogener Daten. Das zeigt auch diese Ausgabe, die Ihnen Folgen der kommenden EU-Datenschutz-Grundverordnung (EU-DSGVO) und zweier Gerichtsurteile näherbringt.

Es geht um Facebook-Daten verstorbener Kinder, um den Umzug von Daten, um Auskunftsrechte von Patienten und um das sogenannte Recht auf Vergessenwerden. Sie werden sehen: Der Datenschutz ist immer für eine Überraschung gut. Deshalb ist es wichtig, immer informiert zu bleiben. Genau dabei hilft Ihnen Ihre Datenschutz-Zeitung.

Wir wünschen Ihnen wieder viele wertvolle Einsichten in den Datenschutz!

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

Erben dürfen auf Facebook-Konto zugreifen

Was wird aus einem Facebook-Account, wenn sein Inhaber stirbt? Können die Erben Zugriff auf die Inhalte verlangen? Das Landgericht Berlin beantwortet diese Frage mit Ja. Das Persönlichkeitsrecht des Verstorbenen stehe dem nicht entgegen.

Digitale Nachlässe - eine alltägliche Erscheinung

"Digitale Nachlässe" gehören inzwischen zum Alltag. Junge wie alte Menschen hinterlassen zwar kaum noch Briefe, dafür aber immer öfter einen Facebook-Account. So war es auch bei einem tragischen Fall in Berlin. Ein 14-jähriges Mädchen hatte mit Zustimmung seiner Eltern einen Facebook-Account eingerichtet. Die Zugangsdaten hatte es seinen Eltern überlassen. Ein Jahr später verstarb das Mädchen unter unklaren Umständen. Ein Selbstmord liegt im Bereich des Möglichen.

Facebook verweigert Erben den Zugriff

Die Eltern wollten auf den Inhalt des Accounts zugreifen. Facebook verweigerte ihnen das jedoch. Stattdessen froh Facebook den Inhalt des Accounts gewissermaßen ein. In diesem "Gedenkzustand" ist der Inhalt zwar noch vorhanden, und "Facebook-Freunde" können auf ihn weiterhin zugreifen. Sie können sogar neue Kommentare einfügen. Ein Zugriff auf den Account durch Eingabe der (an sich kor-

rekten) Zugangsdaten ist aber nicht mehr möglich. Wenn dies versucht wird, erscheint lediglich ein Hinweis auf den Gedenkzustand des Accounts. Hierdurch will Facebook die Persönlichkeitsrechte des verstorbenen Account-Inhabers schützen.

Landgericht Berlin gewährt den Zugriff

Die Eltern ließen sich das nicht gefallen. Als rechtmäßige Erben forderten sie Facebook auf, ihnen Zugang zum Account zu gewähren. Das Landgericht Berlin gab den Eltern Recht.



Erben haben Anspruch auf Zugang zum Facebook-Account (Bild: dolphyn/Stock/Thinkstock)

Zur Begründung weist das Gericht darauf hin, dass das Recht auf Zugang zu dem Account schlicht und einfach ein Teil des Erbes ist, den das Mädchen hinterlassen hat. Aufgrund seines Vertrags mit Facebook habe das Mädchen das Recht gehabt, auf die Server von Facebook zuzugreifen, soweit es seinen eigenen Account betrifft. Dieses Recht sei auf die Eltern als Erben übergegangen. Deshalb dürften nunmehr sie durch Eingabe der Zugangsdaten auf den Account zugreifen.

Unentgeltlich heißt nicht rechtlos

Von dem Hinweis, dass das Mädchen für die Nutzung des Accounts nichts zahlen musste, lässt sich das Gericht nicht beeindrucken. Dies ändere nämlich nichts daran, dass eine vertragliche Vereinbarung vorliege, aus der sich Rechte für den Account-Inhaber ergeben. Und diese vertraglichen Rechte könnten vererbt werden. Dass sie keinen materiellen Wert haben, sondern allenfalls einen ideellen Wert, ändere daran nichts.

Generell anwendbare Grundsätze zu sozialen Netzwerken

Die Entscheidung des Landgerichts Berlin vom 17.12.2015 (Aktenzeichen 20 O 172/15) ist die erste Entscheidung eines deutschen Gerichts zu diesem Thema. Sie betraf direkt zwar nur Facebook, ist aber auf Accounts bei anderen sozialen Netzwerken übertragbar.

Umzugshelfer für Daten gesucht!

Wenn der Kunde es möchte, sollen seine Daten in Zukunft vom alten Anbieter auf den neuen übertragen werden können. So will es die Europäische Union. Bei solch einem Datenumzug ist jeder im Unternehmen gefordert - auch Sie.

Umziehen für mehr Wettbewerb und Datenschutz

Das neue Datenschutzrecht der EU, die EU-Datenschutz-Grundverordnung (EU-DSGVO), kommt - nicht sofort, aber dafür sicher. Bereits jetzt wirft die Grundverordnung ihre Schatten voraus. Denn die Unternehmen müssen sich darauf vorbereiten. Eine der neuen Vorgaben ist das sogenannte Recht auf Datenübertragbarkeit: Personenbezogene Daten sollen einfacher von einem Anbieter auf einen anderen übertragen werden können.

Dieses neue Recht soll den Wettbewerb unter den Anbietern fördern. Denn bisher können Kunden nicht so einfach den Anbieter wechseln, die gespeicherten Daten lassen sich nur sehr mühsam umziehen. Gleichzeitig sollen Kunden mehr Kontrolle über ihre Daten bekommen und verlangen können, die eigenen Daten an einen neuen Anbieter zu übertragen. Damit dieses neue Recht nicht nur den Wettbewerb, sondern auch den Datenschutz voranbringt, gibt es noch viel zu tun.

Umzüge sind immer eine Herausforderung

Jeder, der selbst schon umgezogen ist, kann bestätigen, dass ein Umzug kein einfaches Unterfangen ist. Man muss sehr viel vorbereiten und organisieren, und man sollte möglichst nichts vergessen. Wenn Daten von einem anderen Anbieter in die IT Ihres Unternehmens übernommen werden sollen, weil Ihr Unternehmen einen neuen Kunden gewonnen hat, dürfen genauso wenig Fehler passieren wie in dem Fall, dass Ihr Unternehmen einen Kunden verliert und die Daten an den neuen Anbieter abgeben soll. Gerade bei der Herausgabe, also dem Export von Daten, muss klar sein, welche Daten genau betroffen sind und übertragen werden sollen. Es darf nicht passieren, dass Daten unbelegter Dritter übermittelt werden.

Nun klingt der Umzug von Daten, der allein schon durch das neue EU-Datenschutzrecht in Zukunft öfter anstehen könnte, wie ein rein technisches Thema, das die IT schon lösen wird. Doch tatsächlich sind auch die Fachbereiche und die einzelnen Nutzer im Unternehmen gefragt.



*Auch ein Umzug von Daten will gut organisiert sein
(Bild: LuminaStock/iStock/Thinkstock)*

Datenumzug braucht besonderen Datenschutz

Jeder, der mit den Daten des bisherigen oder neuen Kunden umgeht, muss sich bewusst sein, dass eine Datenübertragung ein Risiko darstellt. Die Schnittstellen und Module, die für den Umzug genutzt werden, können fehlerhaft sein. Die Daten können unterschiedlich strukturiert sein, wenn man das alte System mit dem neuen vergleicht. Technisch würde man sagen, dass die Datenformate nicht richtig passen.

Doch auch bei der inhaltlichen Zuordnung können Fehler auftreten: Vielleicht wurde eine Adresse in ein Kommentarfeld geschrieben, weil der Straßename für das richtige Feld zu lang war. Oder das neue System interpretiert die alten Daten falsch. Solche inhaltlichen Fehler kann die IT nicht allein erkennen, hier sind die fachlichen Experten gefragt.

Umzüge brauchen klare Regeln

Es sollte auch nicht passieren, dass echte Kundendaten für eine Testübermittlung bereitgestellt werden. Hier sollten anonymisierte Daten ohne echten Kundenbezug, also Demo-Daten, zum Einsatz kommen. Zudem sollten Kundendaten nicht ohne ausdrückliche interne Freigabe übermittelt werden, zum Beispiel weil ein (angeblicher) Kunde anruft und sagt, er wechsle zu einem anderen Anbieter und brauche seine Daten nun dort.

Zum einen muss klar sein, welche Daten wirklich übertragen werden können, zum anderen muss die Identität des Kunden überprüft sein. Sonst könnten Datendiebe auf krumme Ideen kommen und Daten wegen eines angeblichen Anbieterwechsels abfragen.

Die folgende Umzugsliste hilft dabei, dass Sie als möglicher Umzugshelfer nichts vergessen, weder bei neuen Kunden und Kundendaten, noch beim Wechsel eines Kunden zum Wettbewerber. Der Schutz der Kundendaten hat eine hohe Bedeutung, auch bei ehemaligen Kunden.

Die Umzugs-Checkliste für Daten

- Jeder Umzug ist eine Herausforderung, auch bei Daten.
- Module, Schnittstellen und Formate, die beim Umzug zum Einsatz kommen, können fehlerhaft sein.
- Die Zuordnung der alten Datenstruktur zur neuen Struktur muss nicht nur technisch, sondern auch fachlich geprüft werden.
- Um Umzüge zu erleichtern, sollten Datenfelder immer nur so genutzt werden, wie es die Dokumentation beschreibt, Umfunktionieren kann dazu führen, dass die falschen Daten übertragen oder dass die richtigen Daten falsch interpretiert werden.
- Verlangt der neue Anbieter Testdaten für die Umzugsprobe, dürfen nur anonymisierte Daten herausgegeben und genutzt werden, keine echten Kundendaten.
- Es muss geklärt sein, wer welche Daten erhalten darf. Also keine Datenübertragung auf Zuruf!
- Bevor die Daten nach der Übertragung im alten System gelöscht werden, muss klar sein, ob noch Aufbewahrungspflichten bestehen.

Impressum

agentia wirtschaftsdienst
dipl.-inform. udo wenzel
budapester straße 31
10787 berlin

tel.: 030 2196 4390
fax: 030 2196 4393

udo.wenzel@agentia.de
thorsten.ritter@agentia.de

Körperverletzung durch einen Mitpatienten

Sie sind Patient in einem Krankenhaus. Ein Mitpatient hat einen Wutanfall und bricht Ihnen den Arm. Können Sie vom Krankenhaus seine Anschrift verlangen? Und warum hat auch Ihr Arbeitgeber Interesse an dieser Anschrift?

Wüterich im Krankenhaus

Mancher, der ins Krankenhaus muss, wird dort nicht gesund, sondern im Gegenteil noch kränker. Und das liegt keineswegs immer an den Ärzten. Auch Mitpatienten können eine echte Gesundheitsgefahr darstellen. Diese Erfahrung musste ein junger Mann machen, der sich in einer Fachklinik behandeln ließ. Von Anfang an hatte er sich mit seinem Bett-nachbarn nicht gut verstanden. Aber nun kam es ganz dick: Der Mitpatient bekam einen Wutanfall und schlug mit aller Kraft zweimal die Zimmertür gegen den Arm des jungen Mannes. Der Arm war danach gebrochen.

Schmerzensgeld - aber ohne Anschrift des Täters?

Als das Opfer wieder zu Hause war, wollte es Schmerzensgeld vom Täter. Den Vor- und den Nachnamen des Täters hatte das Opfer während seines Krankenhausaufenthalts zufällig mitbekommen. Die Adresse leider nicht. Deshalb wandte es sich an das Krankenhaus und bat dort um die Anschrift. Das Krankenhaus lehnte diese Auskunft jedoch ab.

Sorge des Krankenhauses wegen seiner Schweigepflicht

Bei der Anschrift gehe es - so die Klinik - um personenbezogene Daten, und für diese Daten gelte die ärztliche Schweigepflicht. Deshalb könne man dem Opfer die Anschrift leider nicht mitteilen. Falls man dies tun würde, müssten die Verantwortlichen mit einem Verfahren wegen Verletzung der ärztlichen Schweigepflicht rechnen.

BGH: Anspruch auf Auskunft durch das Krankenhaus besteht!

Damit wollte sich das Opfer nicht zufrieden geben. Es verklagte das Krankenhaus auf Herausgabe der Anschrift. Mit Urteil vom 9. Juli 2015 (Aktenzeichen III ZR 329/14) gab der Bundesgerichtshof (BGH), bis zu dem der Fall schließlich gelangt war, dem Opfer Recht. Das geschah fast drei Jahre nach dem Krankenhausaufenthalt im November 2012.

Begründung des Gerichts

Zur Begründung seiner Entscheidung wies der Bundesgerichtshof auf Folgendes hin:

Um Schadensersatzansprüche durchsetzen zu können, muss ein Kläger nicht nur den Namen des mutmaßlichen Täters kennen. Vielmehr braucht er auch dessen Anschrift. Ansonsten ist es nämlich schlicht nicht möglich, eine Klage auf Schadensersatz zuzustellen.

Es ist richtig, dass die Anschrift eines Patienten der ärztlichen Schweigepflicht unterliegt. Auf der anderen Seite hat das Opfer jedoch ein berechtigtes Interesse daran, mögliche Ansprüche gegen den Täter gerichtlich durchzusetzen. Das berechtigte Interesse, Ansprüche auch durchsetzen zu können, berührt den "Anspruch auf Justizgewährung". Er ist im Grundgesetz zwar nicht ausdrücklich erwähnt, aber letztlich aus den Grundrechten des Opfers abzuleiten.

Mit dieser Rechtslage wäre es nicht zu vereinbaren, wenn sich ein Krankenhaus ausnahmslos und ohne jede Abwägung weigern könnte, Angaben zur Identität des mutmaßlichen Täters zu machen. Datenschutzregelungen haben nicht den Zweck, einem Patienten die vollständige Anonymität auch dann zu sichern, wenn er einen Mitpatienten vorsätzlich verletzt. Deshalb ist das Krankenhaus verpflichtet, dem Opfer die

Anschrift seines früheren Mitpatienten zu nennen. Ansonsten stünde das Opfer nämlich faktisch rechtlos da. Es hätte zwar vom Prinzip her einen Schadensersatzanspruch gegen den Täter, könnte ihn aber nicht durchsetzen.

Jedenfalls wenn eine vorsätzliche Körperverletzung im Raum steht, ist es regelmäßig angemessen und geboten, dass das Auskunftsinteresse des Geschädigten den Vorrang gegenüber dem Datenschutzinteresse des Schädigers hat.

Entscheidung auch für Arbeitgeber wichtig

Vordergründig hat die Entscheidung nur für denjenigen Bedeutung, der durch einen Mitpatienten verletzt worden ist. Bei näherer Betrachtung ist sie jedoch auch für Arbeitgeber wichtig. Der Grund: Wer krank ist und deshalb nicht arbeiten kann, genießt normalerweise Lohnfortzahlung. Das gilt auch dann, wenn die Krankheit auf eine vorsätzliche Körperverletzung zurückgeht, die ein anderer dem Arbeitnehmer zugefügt hat.

Information des Arbeitgebers geboten

Dem Arbeitgeber ist es jedoch natürlich nicht zuzumuten, gewissermaßen für die Straftaten anderer zu zahlen. Deshalb hat er in solchen Fällen gegen den Täter einen Ausgleichsanspruch hinsichtlich der Kosten für die Lohnfortzahlung. Er ist in § 6 Entgeltfortzahlungsgesetz geregelt. Falls man als Arbeitnehmer von jemandem verletzt wird und deshalb Lohnfortzahlung in Anspruch nimmt, sollte man deshalb seinen Arbeitgeber unverzüglich über die Hintergründe informieren. Das ist ein Gebot der Fairness, aber auch eine rechtliche Pflicht.



Nicht in allen Fällen kann sich ein Krankenhaus auf die ärztliche Schweigepflicht berufen.

(Bild: takasuu/iStock/Thinkstock)

Datenschutz-Grundverordnung: Vergessen will gelernt sein

Das neue EU-Datenschutzrecht wird das sogenannte Recht auf Vergessenwerden einfordern. Doch kann das Internet denn überhaupt vergessen? Nicht wirklich!

Es gibt keinen digitalen Radiergummi

Schon vor Jahren gab es die Idee, Daten mit einem digitalen Radiergummi für immer aus dem Internet zu löschen. Mehrere Seiten forderten ein Recht auf Vergessenwerden. Allerdings zeigte sich schnell, dass das Internet nicht vergisst. Auch wenn man zum Beispiel ein Bild verschlüsselt und den Schlüssel löscht, ist das Bild nicht weg. Es kann zahllose Kopien im Internet geben, die ohne Schlüssel sichtbar sind.

Das Recht auf Vergessenwerden kommt trotzdem

Aber obwohl es den Radiergummi für das Internet nicht gibt, steht das Recht auf Vergessenwerden in der kommenden EU-Datenschutz-Grundverordnung (EU-DSGVO).

Nun könnte man meinen, es mache doch keinen Sinn, ein Recht vorzusehen, das sich technisch nicht umsetzen lässt. Doch die EU-DSGVO verlangt nichts Unmögliches - aber sie verlangt viel. So gehört zum Recht auf Vergessenwerden, dass die schon aus dem deutschen Datenschutzrecht bekannten Löschpflichten umgesetzt werden: Wenn die Betroffenen nicht möchten, dass ihre Daten weiterverarbeitet werden, und es keine legitimen Gründe für deren Speicherung gibt, müssen die Daten gelöscht werden.

Löschen ist auch nach Veröffentlichung der Daten ein Muss

Ebenso sieht die EU-DSGVO vor, dass andere Stellen, die die zu löschenden Daten erhalten haben, über die Löschpflicht oder den Löschwunsch des Betroffenen informiert werden. Das ist im Bundesdatenschutzgesetz (BDSG) bereits heute so geregelt. Das neue EU-Datenschutzrecht spricht aber zusätzlich von öffentlich gemachten Daten und davon, Links auf die zu löschenden Daten oder auf zu löschende Datenkopien zu entfernen.

Man kann also davon ausgehen, dass Unternehmen und Behörden auch dann die Löschpflichten angehen müssen, wenn die Daten bereits im Internet veröffentlicht sind.

Dabei verlangt die Datenschutz-Grundverordnung jedoch keine Wunder, sondern das wirtschaftlich und technisch Machbare. Man kann aber nicht einfach sagen: "Die Daten sind im Internet zu finden, Löschen ist da sowieso nicht möglich." Vielmehr gilt es, zum Beispiel Suchmaschinenbetreiber dazu zu bringen, die Links auf die Daten aus ihrem Bestand zu nehmen.

Löschen betrifft auch die Offline-Welt

Bei all der Diskussion um einen digitalen Radiergummi und das bleibende Gedächtnis des Internets darf die Offline-Welt nicht vergessen werden. So hatte die EU-Agentur für Netz- und Informationssicherheit (ENISA)

nicht nur erklärt, dass ein digitaler Radiergummi technisch unmöglich ist. ENISA hatte vielmehr auch auf die entscheidende Rolle der Suchmaschinenbetreiber und auf die klassischen Speichermedien verwiesen. Das Recht auf Vergessenwerden betrifft nämlich auch alle zu löschenden Daten, die sich nicht im Internet befinden. Offline können zahllose Kopien von Daten vorliegen, die Sie beim Löschen nicht vergessen dürfen.

So können Daten, die im Firmennetzwerk gelöscht wurden, durchaus noch

- als Kopie auf externen Festplatten im Home-Office von Mitarbeitern,
- auf USB-Sticks des Außendienstes oder
- auf mobilen Endgeräten wie Smartphones

liegen. Auch wenn sie dort verschlüsselt gespeichert sind (was zu hoffen ist), besteht die Löschpflichtung, wenn es keine rechtlichen oder vertraglichen Gründe mehr dafür gibt, sie aufzubewahren. Deshalb: Vergessen Sie das Löschen nicht!

Denken Sie daran, personenbezogene Daten rechtzeitig zu löschen? Machen Sie den Test!

Frage: Ein Kunde hat seinen Vertrag gekündigt. Müssen Sie alle Daten sofort löschen?

- a) Ja, ohne gültigen Vertrag dürfen die Daten nicht mehr gespeichert werden.
- b) Nein, es ist nicht erforderlich, sie sofort zu löschen, wenn es Aufbewahrungspflichten gibt.

Lösung: Die Antwort b) ist richtig. Es gibt viele rechtliche Vorgaben, die fordern, Daten länger vorzuhalten. So sieht das Handelsgesetzbuch (HGB) eine Aufbewahrung von Geschäftsunterlagen (§§ 238, 257, 261 HGB) vor. Ebenso gibt es Aufbewahrungsvorschriften nach § 147 Abgabenordnung (AO), um nur einige Vorgaben zu nennen.

Frage: Sind Daten einmal im Internet gelandet, lassen sie sich nicht mehr löschen. Das Internet vergisst nichts, deshalb entfällt jede Löschpflicht für das Internet. Ist das so?

- a) Ja, denn wenn man im Internet etwas löscht, ist das vergebene Mühe. Es gibt zahllose Kopien, die man nicht komplett löschen kann.
- b) Nein, auch wenn man nicht alle Datenkopien im Internet finden und löschen kann, bleibt die Löschpflicht bestehen.

Lösung: Die Antwort b) ist wieder richtig. Die Löschpflicht betrifft auch Daten, die im Internet veröffentlicht wurden. Man muss alles tun, was wirtschaftlich vertretbar und technisch machbar ist, um die Daten im Internet zu löschen. Dazu gehört auch der Hinweis an Suchmaschinenbetreiber, dass sie die Links auf die zu löschenden Daten entfernen sollen. Vergessen werden dürfen aber auch nicht die Daten auf den lokalen Speichermedien, die viele Datenkopien vorhalten könnten. Das Recht auf Vergessenwerden ist also ein Recht auf umfassendes Löschen im Rahmen des wirtschaftlich und technisch Machbaren.