Newsletter Datenschutz
Ausgabe 04 | 2015

Newsletter Datenschutz

Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

der Datenschutz steckt voller Überraschungen. Ein Gerichtsurteil über die Veröffentlichung von Fotos im Internet bietet Ihnen ebenso neue Einsichten in den Schutz der Privatsphäre wie das neue Bundesmeldegesetz. Es bringt Änderungen mit sich für Privatpersonen, die in eine andere Stadt umziehen. Unter anderem müssen sie künftig eine Bescheinigung des Wohnungsgebers vorlegen.

Verblüffend ist für viele auch die Erkenntnis, dass Daten in einer Cloud verloren gehen können. Backups nur in der Cloud sind deshalb nicht zu empfehlen. Ein böses Erwachen kann es auch nach der Installation einer App geben, die in einem offiziellen App-Store angeboten wird, aber trotzdem Schadfunktionen enthält. Lesen Sie deshalb am besten gleich Ihre neue Datenschutz-Zeitung, um unliebsame Überraschungen zu vermeiden.

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

Muss sich eine Hostess fotografieren lassen?

Eine Arbeitnehmerin macht ihren Job. Dabei wird sie fotografiert. Am Tag danach steht das Foto im Internet. Kann das rechtlich wirklich in Ordnung sein?

Der Job: Gästen Zigaretten anbieten

Der Job war für die junge Frau interessant. Eine Promotion-Agentur bot ihr an, als "Zigaretten-Hostess" zu arbeiten. Ihre Aufgabe bestand darin, auf großen Partys den Gästen in einem Korb verschiedene Zigarettenmarken anzubieten. Genau das tat sie dann auf der Casting-Company-Abriss-Party in Berlin. Zu dieser Veranstaltung kamen zahlreiche Prominente. Eingeladen hatte ein Mann, der durch die Fernsehsendung "Germany's next Topmodel" allgemein bekannt war.

Ein Foto landet im Internet

Ein Foto, auf dem die Hostess Zigaretten anbietet, landete im Internet auf einem Eventportal. Damit war die junge Frau überhaupt nicht einverstanden. Sie war der Auffassung, dass eine solche Veröffentlichung nur zulässig wäre, wenn sie vorher ausdrücklich und schriftlich ihre Einwilligung dazu erklärt hätte.

Laut Bundesgerichtshof hat die Frau darin eingewilligt

Der Rechtsstreit landete schließlich beim Bundesgerichtshof. Dort fand die Frau wenig Verständnis. Nach Auffassung des Gerichts hatte sie sehr wohl in eine solche Veröffentlichung von Fotos eingewilligt, allerdings nicht ausdrücklich, sondern aufgrund der Umstände ihrer Tätigkeit. Und eine solche stillschweigende Einwilligung aufgrund der Umstände ist nach Auffassung des Gerichts ausreichend. Als Begründung hierfür nennt der Bundesgerichtshof mehrere Aspekte:

Die Einwilligung ergibt sich aus den Umständen

- Die Frau hatte von ihrem Arbeitgeber Informationsmaterial erhalten. Dazu gehörten auch "Beispielbilder für die Fotodokumentation". Auf diesen Bildern sind lächelnde Hostessen mit einem Zigarettenkorb zu sehen, die zusammen mit anderen Personen für Fotos posieren.

Nicht immer ist eine ausdrückliche und schriftliche Einwilligung nötig (Bild: Michael Blann/Digital Vision/Thinkstock)

- Damit war der Frau nach Auffassung des Gerichts klar, dass sie mit der Veröffentlichung von Fotos ihrer Person zu rechnen hatte und dass genau dies aus Werbegründen auch erwünscht war.

- Medienvertreter, die auf der Veranstaltung anwesend waren, mussten davon ausgehen, dass sie mit Fotos einverstanden war.

Fotos waren ein Zweck der Tätigkeit

Im Ergebnis musste sie es deshalb als Teil ihrer Tätigkeit akzeptieren, dass sie fotografiert wird und dass diese Fotos öffentlich verbreitet werden - auch im Internet. Ihr musste klar sein, dass auch das der Zweck ihres Jobs war.

Schriftliche Einwilligung - nicht immer ein Muss

An der Entscheidung fällt auf, dass das Gericht kein Wort dazu verliert, ob eine Einwilligung schriftlich erteilt werden muss. Daraus lässt sich ableiten, dass dies jedenfalls in einer Situation wie hier nicht erforderlich ist. Trotzdem: Im Normalfall wissen alle Beteiligten besser, woran sie sind, wenn eine Einwilligung schriftlich formuliert und dann auch unterschrieben wird.

Bundesmeldegesetz: in Kraft ab 1. November 2015

An Allerheiligen 2015 ist es so weit: Das Bundesmeldegesetz tritt in Kraft. Spätestens wenn jemand umzieht, wirken sich die Neuerungen spürbar aus. Manches werden die Betroffenen dabei als unangenehme Bürokratie empfinden - in einigen Fällen aber zu Unrecht!

Meldepflicht für alle Personen in Deutschland

In den Registern der Einwohnermeldeämter sind alle Personen verzeichnet, die in Deutschland wohnen, Deutsche wie Ausländer. Das beruht auf der "Meldepflicht", die es in Deutschland traditionell gibt. Die meisten anderen Länder kennen keine Meldepflicht. Trotzdem ist sie keineswegs "typisch deutsch". In Österreich ist sie beispielsweise ebenfalls etwas Gewohntes.

Bisher war das Einwohnermeldewesen in Gesetzen der Bundesländer geregelt. Das ändert sich am 1. November 2015. An diesem Tag tritt das Bundesmeldegesetz als bundesweit einheitliche Regelung in Kraft.

Für viele etwas völlig Neues: "Bescheinigung des Wohnungsgebers"

Will sich künftig jemand in einer Kommune neu als Einwohner anmelden, muss er eine "Bescheinigung des Wohnungsgebers" vorlegen. "Wohnungsgeber" ist im Regelfall der Vermieter. Seine Bescheinigung soll sicherstellen, dass es tatsächlich eine Wohnung gibt, die bezogen wird, und dass nicht nur eine "Scheinwohnung" vorliegt. So jedenfalls die Theorie. Denn wenn der (dann scheinbare) Vermieter und der (dann scheinbare) Mieter einvernehmlich lügen, wird das oft nicht gleich auffallen. Doch Vorsicht: In einem solchen Fall droht dem Vermieter ein Bußgeld bis 1000 Euro.

Was ist übrigens, wenn die Wohnung, in die der neue Einwohner einzieht, ihm selbst gehört? Dann ist er sozusagen sein eigener Wohnungsgeber, und eine Bescheinigung, die er sich selbst ausstellt, hat natürlich keinen Sinn. Meist wird man von ihm dann allerdings verlangen, dass er sein Eigentum nachweist, etwa durch einen Grundsteuerbescheid auf seinen Namen.

Vornamen und "Rufname"

Viele Menschen haben laut Geburtsurkunde mehrere Vornamen. Im Alltag benutzen sie meist nur einen dieser Vornamen als "Rufnamen". Manche Einwohnermeldeämter haben schon bisher nach dem Rufnamen gefragt und ihn dann entsprechend im Register eingetragen. In vielen Bundesländern war das allerdings weder vorgesehen noch üblich. Auch dies ändert sich mit dem neuen Bundesmeldegesetz. Künftig wird jeder Einwohner nach seinem Rufnamen gefragt.

Zukünftig braucht jeder, der sich anmelden will, eine Bescheinigung des Wohnungsgebers, also in der Regel des Vermieters (Bild: bbbrrn/iStock/Thinkstock)

Der Zweck ist dabei sehr banal: Die Behörden möchten es sich bequemer machen und bei amtlichen Schreiben an den Einwohner nur noch einen Vornamen, nämlich den Rufnamen, ins Adressfeld eindrucken.

Kein Zwang zur Festlegung eines Rufnamens

Ob das in der Praxis viel bringen wird, kann man bezweifeln. Wenn eine Person nur einen Vornamen hat, ist das Ganze sowieso gleichgültig. Und wenn jemand auf die Frage, welcher seiner Vornamen denn sein Rufname ist, verblüfft antwortet "Darüber habe ich noch nie nachgedacht", dann muss er auch jetzt keinen Rufnamen festlegen. Zudem ist die einmal getroffene Wahl eines Rufnamens nicht verbindlich. Wer seinen Rufnamen ändern will, kann dies jederzeit und ohne jede Begründung tun.

Kein Rufname in Pässen oder Personalausweisen

Beim Ausstellen von Pässen und Personalausweisen hat der Rufname übrigens auch künftig keine Bedeutung. Für solche Dokumente ist festgelegt, dass alle Vornamen zu speichern sind, und zwar genau in der Reihenfolge und der Schreibweise, wie sie sich aus der Geburtsurkunde ergeben. Eine Wahlfreiheit gibt es hier nicht, Rufname hin oder her. Er ist und bleibt insoweit ohne Belang.

Neue Anschrift beim Umzug ins Ausland

Wer für einige Jahre ins Ausland zieht, konnte in der Praxis schon bisher die neue Anschrift beim Einwohnermeldeamt bzw. Bürgerbüro seines bisherigen Wohnorts hinterlassen. Ausdrücklich rechtlich vorgesehen war dies aber nicht. Sobald das Bundesmeldegesetz in Kraft getreten ist, wird das anders. Dann besteht die Pflicht, die neue Anschrift im Ausland zu nennen, und sie wird ganz offiziell im Melderegister verzeichnet.

Das dient wieder in erster Linie Abläufen in der Verwaltung. So kann es etwa vorkommen, dass jemandem auch im Ausland ein Steuerbescheid zugestellt werden muss. Dann ist es praktisch, wenn sich seine Anschrift einfach aus dem Melderegister entnehmen lässt.

Bringt es einem im Zweifel also nur Nachteile, wenn man wahrheitsgemäß die neue Anschrift im Ausland nennt? Das wäre zu kurzsichtig gedacht. Denn ein Steuerbescheid kann ja auch eine Steuerrückzahlung bringen! Außerdem bekommt der "Auslandsdeutsche" dann vor jeder Bundestags- und Europawahl eine Nachricht, dass die Wahl stattfindet, und eine Information darüber, wie er Wahlunterlagen beantragen kann.

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

Datenverlust in der Cloud: Was jetzt?

Dateien in der Cloud lassen sich von jedem Endgerät mit Internetzugang aus bequem erreichen, vorausgesetzt, die Dateien verschwinden nicht. Denken Sie bei Backups daran: Wolken können Löcher haben.

Der Speicherplatz in der Wolke

Jeder fünfte Bundesbürger speichert oder teilt Dateien wie Dokumente, Fotos oder Videos im Netz, wie eine Umfrage des Digitalverbands BITKOM ergeben hat. 36 Prozent der deutschen Internetnutzer ab 14 Jahren können sich vorstellen, Daten künftig ausschließlich in der Cloud zu speichern.

Wenn Sie nun denken, Sie gehören nicht zu denjenigen, die einen Speicherplatz in der Cloud nutzen, könnten Sie falsch liegen. Verwenden Sie einen Webmail-Dienst, dann liegen Ihre gespeicherten E-Mails in der Cloud. Und wenn Sie ein Smartphone verwenden, landen ebenfalls viele Dateien in der Cloud, da sowohl das iPhone als auch die Android-Smartphones beharrlich anbieten, Kontaktdaten, Dokumente, Fotos und Videos mit der jeweiligen Cloud zu synchronisieren.

Flexibilität, Komfort und Gefahr in einem

Der Wunsch, von überall auf die eigenen Daten zugreifen zu können, lässt sich mit der Cloud verwirklichen. Einzige Voraussetzung für diese flexible und komfortable IT-Nutzung scheint eine gute Internetverbindung zu sein. In Wirklichkeit aber müssen die Dateien auch in der Cloud verfügbar sein, um auf sie zugreifen zu können.

Vor allem bei mobilen Endgeräten ist es mittlerweile üblich, vieles in der Cloud zu speichern. Ohne Backup ist das nicht unbedingt die beste Idee.
(Bild: belekekin/iStock/Thinkstock)

Obwohl viele Nutzer die Cloud als ihr Backup nutzen, ist ein Datenverlust in der Cloud nicht ausgeschlossen, im Gegenteil. Die Verfügbarkeit in einer Cloud ist keineswegs selbstverständlich, wie viele Ausfälle und Datenverluste in Clouds in den letzten Monaten und Jahren gezeigt haben.

Unerlaubte Zugriffe sind nicht das einzige Cloud-Risiko

21 Prozent der Bundesbürger sind laut Umfrage besorgt um den Datenschutz, wenn es um die Datenspeicherung in der Cloud geht. Die meisten aber fürchten den Kontrollverlust und einen möglichen Datenmissbrauch durch unbefugte Zugriffe auf ihre Daten. Zweifellos muss man diese Risiken ernst nehmen.

Das Problem Verfügbarkeit

Doch die Verfügbarkeit der Daten in der Cloud ist ebenfalls in Gefahr:

- Einerseits kann der Cloud-Dienst ausfallen oder gestört sein. Die Daten sind dann zwar nicht automatisch weg, aber zumindest nicht erreichbar, selbst nicht mit der besten Internetverbindung.

- Zudem können die Daten auch tatsächlich verloren gehen. Es gab selbst bei führenden Cloud-Anbietern bereits Ausfälle und Störungen, bei denen Daten zerstört wurden, die sich nicht mehr wiederherstellen ließen.

Die Cloud braucht selbst ein Backup

Gerade bei der Nutzung mobiler Endgeräte scheint die Cloud das ideale Medium für die Datensicherung zu sein, und die meisten mobilen Backup-Lösungen nutzen Cloud-Speicher.

Allerdings kann man sich nicht einfach darauf verlassen, dass die Cloud ein Speicher ohne Löcher wäre. Ein Datenverlust ist auch in der Cloud möglich, und die Wiederherstellung und Datenrettung sind nicht einfach. Denn dazu muss man ja den ursprünglichen Speicherort kennen und die Bedingungen für eine Datenrettung herstellen, was gerade in einer Cloud, die man sich mit vielen anderen Nutzern teilt (Public Cloud), nicht ohne Weiteres möglich ist.

Wenn Sie also einen Cloud-Speicherdienst nutzen, um die Daten auf Ihrem Smartphone zu sichern oder um wichtige Dateien von jedem Standort mit Internetzugang im Zugriff zu haben, sollten Sie an das Verlustrisiko denken. Die Cloud braucht selbst ein Backup, auch wenn sie oftmals als Backup-Medium genutzt wird. Dass der Cloud-Anbieter für regelmäßige Backups sorgt, können Sie leider nicht einfach voraussetzen.

Was bedeutet das für Ihre Arbeit?

Clouds spielen nicht nur im Privatleben eine zunehmend wichtige Rolle. Im vergangenen Jahr haben in Deutschland 44 Prozent aller Unternehmen Cloud Computing eingesetzt. Das ist ein Anstieg um 4 Prozentpunkte im Vergleich zum Vorjahr, wie eine Studie der Wirtschaftsprüfungsgesellschaft KPMG gezeigt hat.

Bei der Nutzung von Public Clouds sind Lösungen wie E-Mail und Kalender mit 46 Prozent die am weitesten verbreitete Anwendung. 36 Prozent der befragten Unternehmen nutzen Cloud-Lösungen für das Kundenmanagement.

Allein die Verwendung einer Cloud-Lösung sorgt nicht dafür, dass die E-Mails, Termine und Kundenadressen vor Verlust geschützt sind. Denken Sie deshalb daran, die internen Vorgaben zur Datensicherung genau einzuhalten.

Wenn Sie selbst Backups Ihrer Arbeitsdateien machen wollen, nutzen Sie bitte nur die intern freigegebenen Möglichkeiten. Verwenden Sie nicht einfach Ihren privaten Cloud-Speicherplatz, um Ihre beruflichen Dateien zu sichern. Das kann den Datenschutz gleich mehrfach gefährden, unter anderem durch das Risiko, Daten in der Cloud zu verlieren. Wolken können Löcher haben, durch die am Himmel die Sonne durchkommt, in der IT aber gehen auf diese Weise Daten verloren.

Nutzung von App-Stores: Worauf Sie achten sollten

Selbst wenn Apps aus den offiziellen App-Stores stammen, können Sie nicht von ihrer Sicherheit und Datenschutzfreundlichkeit ausgehen. Die Herkunftsgarantie allein reicht bei Apps nicht.

Gefährliche Apps muss man nicht lange suchen

Der Sicherheitsanbieter FireEye hat sieben Millionen Apps für die Betriebssysteme Android und iOS untersucht. Im Fokus der Untersuchung standen beliebte Apps, die mindestens 50.000 Mal heruntergeladen wurden. 31 Prozent der Apps erwiesen sich als angreifbar, waren also als unsicher einzustufen. 18 Prozent der angreifbaren Apps verwalteten persönliche Informationen ihrer Nutzer, wie Finanzdaten, Gesprächsverläufe oder Daten zum Kaufverhalten. Bei diesen Apps waren eindeutig personenbezogene Daten in Gefahr.

Die Sicherheitsstudie von FireEye beschränkte sich nicht etwa auf Apps, die aus unseriösen oder unprofessionellen Quellen stammten. Die unsicheren Apps stammten aus den offiziellen App-Stores.

Sicherheitshinweise nicht missverstehen

Sie kennen sicherlich die Sicherheitsempfehlung, Apps nur aus den offiziellen App-Stores wie Apple App Store oder Google Play zu beziehen. Dieser Hinweis dient dazu, Anwender davon abzuhalten, jede beliebige Download-Quelle für Apps zu nutzen. Denn Datendiebe könnten leicht eine Webseite bereitstellen, auf der angeblich nützliche Apps zu finden sind, die sich nach Installation als Schadsoftware oder Spionage-Tools erweisen.

Es ist tatsächlich gut und richtig, nur offizielle Quellen für den App-Download zu nutzen. Trotzdem darf man die Sicherheit dieser App-Stores nicht überbewerten. Obwohl die App-Store-Betreiber in der Regel umfangreiche Sicherheitstests durchführen, schaffen es immer wieder gefährliche Apps, offiziell gelistet zu werden.

Vorsicht: Bewertungen und Kommentare können gefälscht sein

Bei der Auswahl von Apps sollten Sie sich nicht darauf verlassen, dass unsichere Apps sicher schlechte Bewertungen der Nutzer erhalten haben. Die scheinbaren Kommentare und Bewertungen können schlicht erfunden sein, als Teil eines Angriffs. So wurde schon häufiger darüber berichtet, dass die Nutzerkommentare in den Stores manipuliert sein können. Wenn Sie also eine App ausgewählt haben, die bereits von mehreren Zehntausend Nutzern heruntergeladen wurde, zu der es nur positive Kommentare gibt und die eine ausgesprochen gute Bewertung bekommen hat, können diese Angaben stimmen und hilfreich sein, aber sie müssen es nicht.

Kontrollieren auch Sie selbst die App

Die strengen Sicherheitskontrollen der App-Stores sind natürlich zu begrüßen, trotzdem sollten Sie selbst die Sie interessierenden Apps einer Kontrolle unterziehen. Dazu müssen und sollten Sie die App nicht installieren. Es gibt Test-Plattformen, die Sie bei der Sicherheitskontrolle unterstützen. Testmöglichkeiten für Apps ohne jede Installation finden Sie zum Beispiel unter *http://zap.zscaler.com/*.

Ist eine Datenschutzerklärung vorhanden?

Achten Sie zudem auf die Datenschutzerklärung zur jeweiligen App. Die Aufsichtsbehörden für den Datenschutz haben auf deutliche Mängel hingewiesen und die Betreiber der App-Stores aufgefordert, auf das Vorhandensein einer Datenschutzerklärung zu achten, bevor sie eine App für den App-Store freigeben. Bisher können Sie nicht davon ausgehen, dass jede App aus einem offiziellen App-Store auch eine Datenschutzerklärung besitzt. Fehlt sie, sollten Sie lieber auf die Installation verzichten.

Wie vertrauenswürdig sind Apps aus den App-Stores? Testen Sie Ihr Wissen!

Frage: Apple und Google testen jede App ganz genau, bevor diese in den jeweiligen App-Store kommt. Deshalb sind die Apps sicher. Stimmt das?

a) Die App-Store-Betreiber testen zwar die Apps. Trotzdem finden sich immer wieder unsichere Apps in den App-Stores.
b) Ja, das stimmt, auf die Sicherheit der Apps ist Verlass.

Lösung: Die Antwort a) ist richtig. Leider kann man nicht davon ausgehen, dass jede App aus einem App-Store wirklich sicher ist und den Datenschutzvorgaben entspricht.

Frage: Jede App aus einem App-Store hat eine Datenschutzerklärung, sonst würde sie nicht gelistet. Stimmt das?

a) Natürlich, das gehört zu den Freigabekriterien.
b) Nein, die Aufsichtsbehörden haben bereits bemängelt, dass die App-Stores Apps ohne Datenschutzerklärung veröffentlichen.

Lösung: Die Antwort b) ist richtig. Als Nutzer sollte man selbst darauf achten, ob es wirklich eine Datenschutzerklärung zur App gibt. Fehlt sie, sollte man lieber auf die App verzichten.

Frage: Wenn bekannt wird, dass eine App gefährlich ist, wird sie sofort aus den App-Stores entfernt. Ist das so?

a) Die Betreiber der App-Stores werden in aller Regel umgehend reagieren, eine Garantie gibt es dafür allerdings nicht.
b) Meldungen über unsichere Apps führen automatisch zur Löschung aus den Stores.

Lösung: Die Antwort a) ist richtig. Wenn die Betreiber eines App-Stores erfahren, dass eine App gefährlich sein soll, werden sie dies sofort überprüfen, meist zur Sicherheit sogar die App erst einmal aus dem App-Store nehmen und danach die eigene Prüfung starten. Es gibt aber kein hundertprozentiges Verfahren, sodass nicht garantiert ist, dass alle als unsicher eingestuften Apps sofort aus den Download-Bereichen verschwinden würden.