agentia wirtschaftsdienst

# Newsletter Datenschutz

## Die Kundenzeitung der agentia wirtschaftsdienst

Liebe Leserin, lieber Leser,

wenn Sie mit dem Auto unterwegs sind, sollte nicht nur die Verkehrssicherheit, sondern auch der Schutz Ihrer Privatsphäre gewährleistet sein. Hinter mancher Windschutzscheibe befinden sich private Videokameras und filmen benachbarte Fahrzeuge. Ein neues Urteil zeigt diesen Dash-Cams und der Beweiskraft der Aufnahmen Grenzen auf.

Auch die Apps auf Ihrem Smartphone könnten Sie heimlich beobachten. Hinter scheinbar harmlosen Werbeanzeigen in den Apps können Attacken auf Ihre Daten stecken. Die neue Ausgabe informiert Sie zudem über die Bedeutung von Scoring sowie über den IT-Trend Big Data und seine Auswirkungen auf den Datenschutz.

Wir wünschen Ihnen wieder viele hilfreiche Einsichten!

Ihre *Datenschutzbeauftragten der agentia wirtschaftsdienst*

## Traum oder Albtraum? Der Video-Beweis bei Verkehrsunfällen

**Wer kennt diese Situation nicht? Ein Verkehrsunfall, gottlob nur mit Blechschaden, der Unfallgegner ist einsichtig und gibt vor Ort mündlich alles zu. Später, als es ans Zahlen geht, soll aber alles ganz anders gewesen sein. Wäre es da nicht schön, ein Video vom Unfall zu haben? Lesen Sie, warum das Amtsgericht München davon überhaupt nichts wissen will!**

Ein Autofahrer biegt aus einer Grundstücksausfahrt nach rechts in eine Straße mit zwei Fahrspuren ein. Er meint, die rechte Fahrspur sei frei gewesen, und zum Zusammenstoß sei es nur gekommen, weil der Kontrahent, der sich von links näherte, plötzlich und ohne zu blinken von der linken auf die rechte Spur herübergezogen sei. Der Kontrahent stellt alles ganz anders dar: Er sei sehr wohl schon auf der rechten Spur gefahren, als das andere Auto aus dem Grundstück herausgeschossen kam.

### Die Kamera hat alles gesehen

Zeugen gibt es keine. Allerdings hatte der Autofahrer, der in die Straße eingebogen ist, hinter seiner Windschutzscheibe eine Videokamera installiert. Sie hat den Vorfall aufgezeichnet. Nun möchte er mit diesen Aufnahmen vor Gericht seine Unschuld beweisen.

### Das Gericht schaut sich die Aufnahmen jedoch nicht einmal an

Damit hat er allerdings beim Amtsgericht München kein Glück. Das Gericht lehnt es ab, die Aufnahmen als Beweismittel zuzulassen, und will sie deshalb nicht einmal anschauen. Seine Begründung:

- Die permanente Überwachung des Straßenverkehrs durch eine Kamera ohne konkreten Anlass verstößt gegen den Datenschutz.

- Die Zulassung der Aufnahmen als Beweismittel würde dazu führen, dass sich solche Kameras immer weiter verbreiten und dass möglicherweise Fahrzeuge damit sogar standardmäßig ausgestattet werden.

- Das hätte eine generelle Überwachung aller Verkehrsteilnehmer zur Folge.

- Dies würde auf eine dauerhafte und flächendeckende Überwachung aller Personen hinauslaufen, die am Straßenverkehr teilnehmen.

- Denkbar wäre dann sogar, dass jeder Bürger eine entsprechende Kamera nicht nur in seinem Pkw, sondern auch an seiner Kleidung befestigt.

- Dann würde permanent die gesamte Bevölkerung überwacht.

### Das "Beweisinteresse" ist zu abstrakt

Im Vergleich zu diesen Gefahren wiegen die Interessen dessen, der die Aufnahmen als Beweismittel vor Gericht verwenden will, deutlich geringer. Dabei spielt es eine wichtige Rolle, dass die allermeisten Aufnahmen nie als Beweismittel gebraucht werden, weil kein Unfall passiert. Die Videoaufnahmen sind damit letztlich überflüssig.

### Schon früher wurde so entschieden

Im Ergebnis lehnt das Gericht die Verwendung solcher Videoaufnahmen als Beweismittel strikt ab. Es ist übrigens bereits das zweite Mal, dass das Amtsgericht München so entschieden hat. Jedenfalls in dieser großen Stadt wird der Versuch, solche Aufnahmen vor Gericht zu präsentieren, daher aller Voraussicht nach auch künftig scheitern.

### Gesetzliche Regelung denkbar

Teils wird schon nach einer gesetzlichen Regelung gerufen. Sie könnte solche Aufnahmen prinzipiell zulassen, aber beispielsweise festlegen, dass sie bereits nach ein oder zwei Minuten zu löschen sind, sofern das Auto nicht heftig abgebremst worden ist. Ob eine solche Regelung jemals kommt, steht aber noch völlig in den Sternen.

# Wenig bekannt, aber sehr wichtig: Was bedeutet Ihr Score-Wert?

**Wer einen Kredit von der Bank möchte, will sofort bedient werden. Und wer etwas über das Internet bestellt, wünscht sofortige Lieferung. Aber wie kann Ihr Geschäftspartner sicher sein, dass Sie genügend Geld haben und deshalb später auch zahlen werden? Scoring-Systeme helfen bei der Beurteilung und sind bei richtiger Ausgestaltung problemlos mit dem Datenschutz zu vereinbaren. Lesen Sie, was es mit dem Scoring auf sich hat!**

### Gute alte Zeit?

Wer früher einen Kredit von der Bank wollte, tat gut daran, beim Kreditgespräch einen guten Eindruck zu hinterlassen. Hierfür gab es zahlreiche Tipps für den Antragsteller, von der richtigen Kleidung bis hin zum lächelnden Auftreten. Die Bankmitarbeiter wiederum wurden geschult, auf was sie zu achten hatten, damit sie nur mit zahlungskräftigen Kunden Kreditverträge abschließen.

Wirklich objektiv war ein solches Vorgehen natürlich nicht, und es gab Pannen in beide Richtungen. Manchmal erhielt ein Kunde einen Kredit, den er besser nicht bekommen hätte. Umgekehrt verweigerten die Bankmitarbeiter manchmal einen Kredit, nur weil irgendwelche Äußerlichkeiten ein Misstrauen gegenüber dem Kunden auslösten, zu dem überhaupt kein Anlass bestand.

### Scoring-System als gute neue Zeit?

An diesem Punkt setzen Scoring-Systeme an. Sie beruhen auf statistischen Daten, die aus einer großen Zahl von Zahlungsvorgängen bei Krediten ermittelt werden.

So könnte zum Beispiel die statistische Erfahrung zeigen, dass Kreditnehmer mit mehreren Kindern ihre Kredite zuverlässiger tilgen als Personen ohne Kinder (was tatsächlich der Fall ist!). Oder es könnte sich herausstellen, dass Menschen zwischen 20 und 30 zwar die Rechnungen ihres Mobiltelefons sehr pünktlich zahlen, Autokredite jedoch überdurchschnittlich häufig verzögert tilgen.

Zweck von Scoring-Systemen ist es also nicht, das Verhalten auszuwerten, das ein konkreter Kunde in der Vergangenheit an den Tag gelegt hat, und daraus dann Schlüsse zu ziehen. Vielmehr geht es um eine Zukunftsprognose für diesen Kunden auf der Basis der Erfahrungen, die man in der Vergangenheit mit vergleichbaren Kunden gemacht hat.

### Typische Merkmale werden verglichen

Dazu werden die Merkmale von früheren Kunden ermittelt, die nach den statistischen Erfahrungen der Vergangenheit typischerweise etwas über die Zahlungsfähigkeit und den Zahlungswillen aussagen, also etwa das Alter des Kunden, der Verwendungszweck des Kredits und die Frage, ob der Kunde Kinder hat.

*Scoring-Systeme helfen bei der Bewertung der Kreditwürdigkeit* (Bild: typhoonski/iStock/Thinkstock

Diese Scoring-Merkmale werden mit den Merkmalen verglichen, die ein neuer Kunde aufweist. Stimmen die Merkmale überein, geht man davon aus, dass der neue Kunde sich im Prinzip so verhalten wird wie vergleichbare frühere Kunden. Wie wahrscheinlich das ist, bringt ein Score-Wert zum Ausdruck.

### Tut wirklich jeder, was alle anderen tun?

An dieser Stelle setzen die Kritiker solcher Verfahren an. Sie verweisen darauf, dabei bleibe außer Betracht, dass Menschen, die dieselben Merkmale wie andere Menschen aufweisen, sich individuell trotzdem anders verhalten könnten. Im Klartext: Nur weil andere Menschen zwischen 20 und 30 Jahren Autokredite normalerweise tatsächlich zögerlicher zurückzahlen als Menschen zwischen 30 und 40 Jahren, müsse dies nicht bei jedem einzelnen jungen Menschen so sein.

### Statistik lügt nicht

Diese Kritik trifft im Kern zu. Sie ändert aber andererseits nichts daran, dass das typische Zahlungsverhalten eben doch so ist, wie es die Statistik beschreibt. Und zudem beantwortet diese Kritik nicht die Frage, welche anderen Kriterien sich alternativ besser heranziehen ließen. Den berühmten ersten Eindruck, der früher bei der Kreditvergabe eine so große Rolle spielte, wünscht sich nämlich auch unter den Kritikern kaum jemand als ausschlaggebenden Maßstab zurück.

### Merkmale müssen relevant sein

Allerdings gelten alle diese Überlegungen nur dann, wenn die Verfahren, die für die statistische Auswertung zum Einsatz kommen, tatsächlich mathematisch korrekt funktionieren und - ganz wichtig - wenn nur Kriterien Verwendung finden, deren Relevanz für das Zahlungsverhalten nachgewiesen ist.

### Diskriminierungen sind verboten

Schließlich darf es auch nicht zu Diskriminierungen kommen. Selbstverständlich wäre es beispielsweise keinesfalls zulässig, an die Hautfarbe oder ähnliche Kriterien anzuknüpfen. Dies tut in der Praxis aber auch niemand. Denn allenfalls einzelne verbohrte Menschen meinen ernsthaft, daraus etwas ableiten zu können. Mathematik und Statistik beweisen das genaue Gegenteil.

### Ausdrückliche Regelung im Gesetz

Werden die geschilderten Vorgaben beachtet, liefern Scoring-Systeme im Ergebnis durchaus aussagekräftige Daten. Dies ist der Grund dafür, dass das Bundesdatenschutzgesetz (BDSG) diese Systeme ausdrücklich zulässt (siehe dazu § 28b BDSG zum Scoring).

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

# Big Data in aller Munde: Wo liegen die Probleme für den Datenschutz?

**Wahrscheinlich haben Sie schon von Big Data als neuem IT-Trend gehört. Für den Datenschutz ist dies mehr als ein Trend, es ist ein mögliches Datenrisiko. Warum ist das so, und wie betrifft Sie das?**

### Viele Daten, viele Sorgen?

Wenn Sie in IT-Zeitschriften blättern oder IT-Messen besuchen, stoßen Sie fast immer auf die Trend-Themen Cloud Computing, mobile Endgeräte und soziale Netzwerke.

In den meisten Fällen gesellt sich ein weiteres Trend-Thema hinzu: Big Data. Dahinter verbirgt sich erst einmal der Umstand, dass die Menge der erhobenen, verarbeiteten und gespeicherten Daten immer größer wird. Aus Sicht der IT führt das zu Problemen wie zu einem steigenden Bedarf an Speicherplatz, Rechenleistung und Internetbandbreite. Aus Sicht des Datenschutzes gibt es ebenfalls Probleme mit Big Data, sie sind allerdings anderer Natur.

### Datenberge ziehen Datendiebe an

Die immer größeren Datenmengen bedeuten auch, dass sich Daten anhäufen und konzentrieren. Wenn zum Beispiel die Daten, die ein Unternehmen über seine Kunden gespeichert hat, immer umfangreicher werden, führt das zu einer Datenkonzentration, die nicht nur für den eigenen Vertrieb und das eigene Marketing spannend ist. Auch Datendiebe fühlen sich geradezu magisch angezogen von Datenansammlungen: Gelingt die Attacke und damit der Zugriff auf die Daten, ist die Beute wesentlich größer als bei kleinen, verteilten Datenbeständen, die einzeln angegriffen werden müssen.

Allein schon aus diesem Grund ist die Entwicklung hin zu Datenanhäufungen, hin zu Big Data, ein Thema für die Datensicherheit. Doch ist dies nicht nur eine weitere Herausforderung für die IT-Abteilung? Warum sind Sie selbst von dem Trend Big Data betroffen?

### Große Datenmengen ermöglichen tiefe Einblicke

Die Sammlung von großen Datenmengen ist nicht nur eine Folge der zunehmenden Digitalisierung in den meisten Lebens- und Arbeitsbereichen. Viele Unternehmen haben ein hohes Interesse an Datensammlungen und führen leistungsstarke Analyseprogramme ein, die die Datenauswertung optimieren. Suchmaschinenanbieter oder Betreiber sozialer Netzwerke haben meist schon spezielle Anwendungen für Big-Data-Analysen im Einsatz. Kritisch wird es für den Datenschutz immer dann, wenn die gesammelten Daten oder die Auswertungen einen Personenbezug haben oder personenbeziehbar sind.

### Risiko Nutzerprofile

Für Sie als Internetnutzer und wahrscheinlich auch Mitglied in einem sozialen Netzwerk bedeutet die Entwicklung zu leistungsstarken Analysen und zu Datenansammlungen ein steigendes Risiko, dass sich aussagekräftige Nutzerprofile über Sie anlegen lassen. Die Zusammenhänge zwischen Ihren einzelnen Klicks im Internet können Erstaunliches über Sie als Person verraten oder zumindest über Ihre Vorlieben, Ihre Interessen und Ihr Verhalten nahelegen.

### Big Data braucht besonderen Schutz

Es sollte Sie also nicht wundern, wenn die Datenschützer und Verbraucherschützer vor einer ungehemmten Nutzung von Big Data warnen und einen speziellen Schutz fordern, wenn große Datenmengen gespeichert und ausgewertet werden. Tatsächlich ist es auch gar nicht so einfach, die klassischen Methoden der Datensicherheit auf große Datenmengen zu übertragen. So ist ein Vorwurf gegenüber Verschlüsselungslösungen, dass sie zu langsam sind und scheinbar ewig brauchen, um ein Speichermedium zu verschlüsseln und gegen unbefugte Zugriffe zu schützen.


*Das Thema "Big Data" dürfte mittlerweile jeden betreffen. Wer ein ausführliches Nutzerprofil verhindern möchte, sollte sich daher in Datensparsamkeit üben.* (Bild: xrender/iStock/Thinkstock)

### Das Problem "Verschlüsselung"

Wenn nun aber die Datenmengen immer größer werden, die zu schützen sind, wird der zeitliche Engpass durch Verschlüsselung noch größer. Deshalb müssen nicht nur leistungsstarke Analyseprogramme für Big Data entwickelt werden, sondern auch leistungsstarke Verschlüsselungsprogramme und andere Schutzverfahren.

Solange aber die Angebote zur Big-Data-Analyse gegenüber den Angeboten für "Big-Data-Schutz" dominieren, kann Big Data ein Datenschutzproblem werden - und zwar ein immer größer werdendes.

### Ihr Big-Data-Programm: Datenvermeidung und Datensparsamkeit

Für Sie als Anwender und Internetnutzer bedeuten die Probleme im Schutz von Big Data, dass Sie noch vorsichtiger sein müssen bei der Preisgabe Ihrer Daten. Sie müssen noch mehr Datenvermeidung und Datensparsamkeit üben, gerade wenn Sie das Internet und soziale Netzwerke nutzen.

Dazu gehört auch, dass Sie Ihre Online-Profile im Internet nicht selbst verknüpfen, indem Sie von einem Online-Profil auf die anderen verweisen. Damit machen Sie es den Analyseprogrammen, die Internetdaten auswerten, noch leichter, zusätzliche Verbindungen zu ziehen und noch weitere Einblicke in Ihre Online-Aktivitäten zu erhalten.

### Nutzen Sie Pseudonyme

Nutzen Sie deshalb wo immer möglich und sinnvoll Pseudonyme. Das Telemediengesetz gibt Ihnen hierauf einen Anspruch gegenüber den Betreibern. So heißt es dort: "Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren." Die Aufsichtsbehörden für den Datenschutz haben schon mehrfach Online-Anbieter ermahnt, diese Möglichkeit auch tatsächlich anzubieten. Es liegt an Ihnen als Nutzer, davon wirklich Gebrauch zu machen.

# Werbung in Apps: Kleine Anzeigen, große Angriffsflächen

**Die meisten Smartphone-Apps sind kostenlos, viele finanzieren sich über Werbung. Teilweise taucht die Werbung auch innerhalb der Apps selbst auf. Das kann nicht nur lästig werden, sondern sogar gefährlich.**

### Online-Werbung nicht nur im Browser

Wenn Sie die Online-Ausgabe einer Zeitung im Internet lesen, werden Sie in den meisten Fällen eine Vielzahl an Werbeanzeigen auf den Seiten sehen. Das sollte Sie nicht verwundern, denn in aller Regel ist die Online-Ausgabe einer Zeitung kostenlos und finanziert sich über entsprechende Online-Werbeanzeigen.

Auch im mobilen Internet gibt es viele kostenlose Angebote. So sind die meisten Apps für Smartphones und Tablets ohne jede Zahlung nutzbar, so scheint es. Doch bei einigen Apps zahlen Sie mit Ihren Daten, die der App-Anbieter über Ihr Nutzungsverhalten sammelt. Die Analyse Ihres mobilen Online-Verhaltens hilft wiederum Werbenetzwerken, die für Sie passende Werbung zu finden und anzuzeigen. Diese Werbung erscheint dann nicht nur im mobilen Browser, sondern auch innerhalb bestimmter Apps auf Ihrem mobilen Endgerät.

### In-App-Advertising wird zunehmen

Marktforscher gehen davon aus, dass die Werbung innerhalb von Apps, das sogenannte In-App-Advertising, eine große Bedeutung erlangen wird, da sich Smartphone-Apps einer großen Beliebtheit erfreuen. Wenn Sie nun denken, dass man Werbung in den kleinen Apps doch kaum sehen kann, haben Sie einerseits Recht. Doch der Trend bei Smartphones geht hin zu Modellen mit immer größeren Displays. Trotzdem sollte man nicht vergessen, dass Apps eigentlich nur wenig Platz für Anzeigen bieten.

Dieser Umstand ist aber verschiedenen Gruppen sogar willkommen: Stellen Sie sich vor, Sie klicken innerhalb einer App ungewollt auf eine Werbeanzeige. Das ist schnell passiert bei einer Touchscreen-Bedienung, die nicht wirklich auf die durchschnittliche Größe der menschlichen Finger achtet. Das von Ihnen nicht gewollte Anklicken freut nun den App-Anbieter, wenn er vom Werbepartner nach Anzahl der Klicks bezahlt wird. Auch das werbende Unternehmen ist nicht unerfreut, sehen Sie doch die Werbung, obwohl Sie eigentlich eine Funktion in der App nutzen wollten. Vielleicht gibt es noch einen lachenden Dritten: den Datendieb!

### Auch mobile Werbebanner können verseucht sein

Genau wie im Webbrowser auf dem Desktop-PC oder Notebook können auch die Werbebanner innerhalb mobiler Apps mit Schadfunktionen versehen worden sein. Das ist nicht nur eine theoretische Möglichkeit, sondern es hat bereits Trojaner-Attacken auf Smartphones gegeben, weil mobile Werbeanzeigen angeklickt wurden. Dazu wird der Werbebanner nicht wie sonst üblich mit der mobilen Webseite des werbenden Unternehmens verknüpft, sondern mit einem Server, auf dem Schadprogramme darauf warten, heruntergeladen zu werden.

Leider können solche Angriffe über App-Werbung sehr erfolgreich für die Datendiebe laufen: Smartphones sind vielfach immer noch schlechter geschützt als PCs oder Notebooks.

Zudem sind Smartphones randvoll gefüllt mit personenbezogenen Daten, in den Adressbüchern, Kalendern, E-Mail-Postfächern, SMS-Ordnern und auf den leistungsstarken Speicherkarten, die ohne Weiteres 32 oder mehr Gigabyte Daten bevorraten können.

### Mobile Apps mit Vorsicht genießen

So praktisch viele der Apps auch sind, Sie sollten die Gefahren in den kleinen Anwendungen nicht vernachlässigen:

- Denken Sie daran, dass innerhalb von Apps die gleichen Gefahren drohen können wie im Browser, also zum Beispiel verseuchte Werbebanner.

- Klicken Sie nicht einfach auf Banner oder Dialoge in Apps, auch wenn sie lukrative Vorteile versprechen.

- Nutzen Sie Ihr Smartphone nur mit mobilem Anti-Malware-Programm.

- Prüfen Sie, ob die mobile App auch über eine Datenschutzerklärung verfügt und was dort über die Datennutzung für mobile Werbung steht.

- Nutzen Sie sogenannte Privacy-Scanner für Ihr Smartphone, die Ihnen anzeigen, welche Berechtigungen Apps verlangen, und die Hinweise auf kritische Datenzugriffe geben.

## Schätzen Sie die Risiken bei Apps richtig ein? Testen Sie Ihr Wissen!

**Frage: Für kostenlose Apps müssen Sie nichts bezahlen. Stimmt das?**

a) Ja, sonst dürften die Apps nicht kostenlos genannt werden.
b) Nein, denn mitunter bezahlt man eine App mit seinen Daten oder zumindest dadurch, dass man mobile Werbeanzeigen duldet.

Lösung: Die Antwort b) ist richtig. Niemand hat etwas zu verschenken. Die Entwicklung von Apps ist durchaus kostspielig. Sie müssen also damit rechnen, dass der App-Anbieter zumindest indirekt durch seine App verdienen möchte, etwa durch mobile Werbung.

**Frage: Werbung in Apps ist mitunter lästig, gefährlich ist sie aber nicht. Ist das richtig?**

a) Nein, leider kann durch das Anklicken einer App-Werbung auch ein Angriff durch Schadsoftware starten.
b) Was soll an Werbung schon gefährlich sein?

Lösung: Die Antwort a) ist richtig. Es sind bereits Trojaner-Angriffe auf Smartphones erfolgt, ausgelöst durch ungewolltes Anklicken mobiler Werbeanzeigen. Nutzen Sie deshalb immer einen professionellen Schutz auf Ihren mobilen Endgeräten.