
cloud
cloud world präsentiert:
Datenschutz im Netz
Tipps und Hinweise für den sicheren Umgang mit Ihren Daten

Werte Leser/innen,

„Daten sind der Rohstoff der Zukunft“
Angela Merkel auf der Hannover Messe, September 2015

Wie wichtig sind uns unsere Daten? Tagtäglich tragen wir unsere Kontaktdaten in Online-Formulare ein, laden Fotos auf soziale Netzwerke hoch, speichern Dokumente in der Cloud und tauschen Informationen via Chat. Dabei schwebt immer das Damokles-Schwert der Datenschutzrisiken über unseren Köpfen - die Hacker und die NSA, die seit einigen Jahren das Wort „Cloud“ wie ein Schatten begleiten.
Da herrscht viel Unsicherheit und dennoch können wir nicht umhin, wir loggen uns ein, laden hoch, laden herunter und tauschen aus. Warum auch nicht, das Internet ist ein fester Bestandteil unseres Lebens, die Dämonisierung bringt also nichts außer Frust und Angst.
Was wir als Nutzer brauchen, sind klare Anweisungen, wie wir mit unseren Daten umgehen sollen, welche Unterschiede Daten haben können und worauf wir beispielsweise bei den AGB von Cloud-Anbietern und Co achten müssen.
Wie gut, dass Sie dieses Whitepaper in den Händen halten, denn es dient dazu, Ihnen ein paar Hinweise auf den Weg durch den Datendschungel mitzugeben.

Ich wünsche Ihnen viel Spaß beim Lesen und Teilen.

Mit freundlichen Grüßen,

Juliane Waack
Redakteurin, cloud world

Inhalt

Wichtiger Hinweis

Dieses Whitepaper wurde von cloud world nach bestem Gewissen und Wissen erstellt. Wir übernehmen jedoch keine Gewähr für Richtigkeit, Vollständigkeit oder Aktualität der Inhalte.

1. Was - die Datenqualität

Sie werden immer wieder von Cloud-Anbietern und besonders besorgten Datenschützern hören, dass Sie unmöglich Daten auf Dropbox und Co speichern können, wenn es sich dabei etwa um Unternehmensdaten handelt. Das stimmt allerdings nicht so pauschal, denn immerhin kommt es darauf an, welche Daten Sie überhaupt irgendwo speichern oder verarbeiten wollen.

Wir wollen daher im Folgenden von 3 verschiedenen Arten von Daten reden:

- neutrale Daten ND (unverfängliche Dokumente und Texte)
- private Daten PD (Urlaubsfotos, persönliche Briefe)
- sensible Daten SD (vorwiegend personengebundene Daten, aber auch unternehmensinterne Daten wie etwa Finanzberichte, etc.)

ND haben keinen großen Anspruch und können weitestgehend ohne Nachteile Online gespeichert werden, ohne, dass Risiken entstehen (die Verwendung auf sozialen Netzwerken lässt jedoch u.U. andere Schlüsse in der Kombination der Daten zu).

Beispiel: Katzenfotos, fachliche Dokumente, allgemeine Unterlagen wie etwa Infos zur Firmenfeier, Stylesheets oder aber auch Lernmaterialien

PD haben zumindest für den Besitzer einen eigenen Wert und können im Fall eines Datenklaus dazu führen, dass der Dieb nun mehr über die betroffene Person weiß, als es für sie angenehm ist. Das kann sogar so weit gehen, dass jemand sich als diese Person ausgeben kann. Daher sollten Privatpersonen ganz und gar nicht lapidar mit ihren Daten umgehen, sondern sich zumindest die AGB der entsprechenden Dienste durchlesen und sich darüber informieren, was die Anbieter mit den Daten machen. Darüber hinaus stehen sie in der Verantwortung, Passwörter sicher zu wählen und aufzubewahren.

Beispiel: Urlaubsfotos, Mailwechsel, selbstgeschriebene Prosa o.Ä., eigene Bewerbungsunterlagen

SD müssen unter einem besonderen Schutz stehen, da bei einem potenziellen Diebstahl andere Personen (oder auch ganze Unternehmen) erhebliche Nachteile erfahren können. Für Privatpersonen sind SD beispielsweise Arbeitsverträge und interne Unternehmensinformationen, die eigentlich nicht außerhalb des Unternehmens verbreitet werden dürfen.

Für Unternehmen und Selbstständige können dies personalisierte Kunden- oder auch Personaldaten sein, etwa Krankeninformationen, Klientendaten und Patientenmappen. Gemäß des deutschen Datenschutzrechtes müssen Unternehmen eigenständig dafür sorgen, dass diese als „personengebundene Daten“ bezeichneten Daten besonders sicher aufbewahrt und gehandhabt werden. Wer sich also einen Cloud-Speicher oder eine Cloud-Anwendung (oder generell eine dritte Partei zur Verarbeitung) sucht, muss selbstständig sicherstellen, dass die Dienstleister die Daten compliancegerecht aufbewahren und//oder verarbeiten können (mehr dazu finden Sie im Kapitel 05).

Beispiel: Personaldaten, Krankenakten, Vertragsunterlagen, Kundendaten (Mailadressen, Social Media-Accounts, etc.)

Übrigens gibt es auch für bestimmte Finanzdaten gesonderte Regelungen zur Aufbewahrung[1], die bei der Auswahl eines Cloud-Programmes beachtet werden müssen.

Die Verantwortung bei der Handhabung sensibler Daten liegt immer an erster Stelle beim Unternehmen, das sie sammelt und verarbeitet.

Wenn Sie also Ihre Daten im Netz speichern oder verarbeiten wollen, überlegen Sie sich, welche Daten das sind, ob sich Datensätze aufteilen lassen und inwieweit diese Daten zu den SD gehören. Wenn Sie nur unverfängliche Listen, Whitepaper und Termine auf Dropbox speichern wollen, dann spricht nichts dagegen, auch wenn die Server weder in Deutschland liegen oder die Verschlüsselung der Daten nicht ganz so lobenswert ist.
Sobald Sie jedoch Personalunterlagen oder anderweitig sensible Informationen lagern und verarbeiten wollen, müssen Sie sichergehen, dass dies unter den entsprechenden Compliance-Anforderungen erfolgt (sichere Server-Strukturen, Verschlüsselung oder anderweitige Maßnahmen sowie möglichst Zwei-Wege-Authentifizierung). Hier müssen notfalls auch erweiterte Verträge abgeschlossen und Prüfungen bei den Unternehmen durchgeführt werden.

Bestimmen Sie die Art Ihrer Daten, um die entsprechenden Sicherheitsvorkehrungen anpassen zu können. Nur wenn Sie wissen, welche Daten sensibel sind, können Sie diese auch entsprechend schützen.

2. Wozu - die Datennutzung

Wenn ich mir bei der Bank ein Schließfach miete, dann ist es ganz einfach: ich bringe meine Wertsachen zum Schließfach, lege sie rein, schließe ab und sie sind sicher, bis ich sie mir wiederhole.
Bei den Daten im Netz ist es leider nicht so simpel, denn dort lege ich sie nicht nur ins Schließfach, sondern schaue regelmäßig vorbei, hole Sachen raus, verändere sie, teile sie, lege neue Sachen hinzu, etc..
Schlimmer noch, ich hole sie nicht immer nur von meinem PC aus ab (hier verlassen wir den Vergleich mit dem Schließfach), sondern greife auch mal via Handy oder dem Laptop eines Bekannten oder Kollegen auf sie zu. Für alle diese Aktionen müssen die Sicherheitsvorkehrungen gewappnet sein, aber das ist gar nicht so einfach.

Sicher ist nicht gleich sicher

Wenn Sie Ihre Daten irgendwo ablagern und als Backup speichern wollen, reichen bereits grundlegende Sicherheitsvorkehrungen (also Verschlüsselung, Zweifach-Authentifizierung und ein sicheres Passwort).
Doch sobald die Daten regelmäßig den Cloud-Server verlassen, um zwischen Ihrem Handy, Computer und dem Server hin und her zu reisen, braucht es zusätzliche Vorkehrungen, die die Daten auch dann sichern, wenn sie eben nicht auf dem Server sind. Ende-zu-Ende-Verschlüsselung sorgt beispielsweise dafür, dass Ihre Daten eine Art „Geldtransport“ erhalten, da sie erst dann entschlüsselt werden, wenn sie auf Ihrem Rechner bzw. Endgerät der Wahl gelandet sind.
Wer also viel Daten-Fluktuation zwischen Speicher und Computer hat oder etwa Software verwendet, bei der die Daten auf einem Cloud-Server landen und dort verarbeitet werden (etwa bei Browser-basierender Software), muss sich bessere Alternativen suchen als derjenige, der wirklich nur eine Art Bankschließfach sucht.

Dies sollte vor allem dann beachtet werden, wenn die Daten via Apps auf Smartphones verarbeitet werden. Im Gegensatz zu vielen PCs und Laptops achten die wenigsten Nutzer darauf, dass Ihre Smartphones die nötigen Firewalls und Virenprogramme haben, geschweige denn Verschlüsselungs-Maßnahmen. Doch gerade Handys sind ziemlich anfällig für Datenklau, weshalb besonders Unternehmen dazu angehalten sind, einen konkreten Plan zur Verwaltung und dem Schutz mobiler Endgeräte zu erstellen.

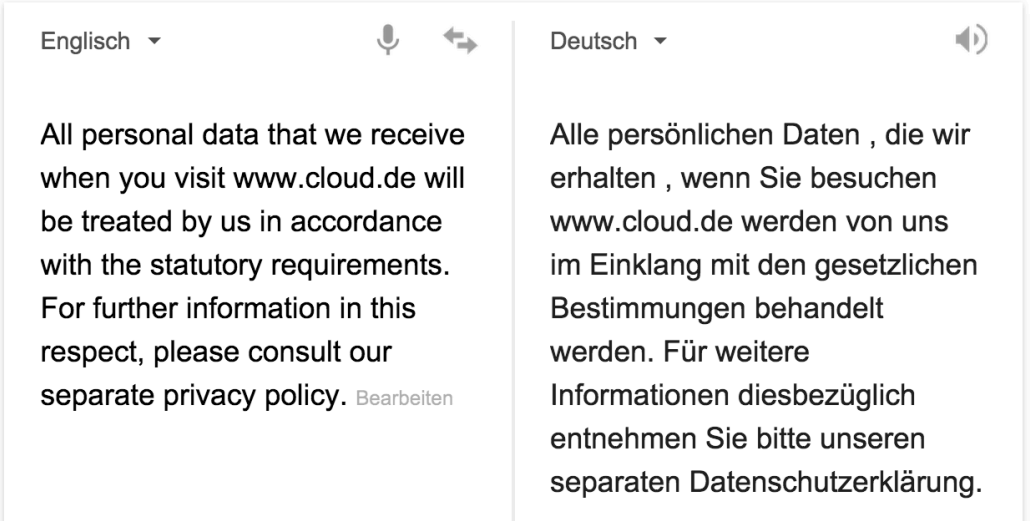
Ein Wort zum Standort

„Made in Germany“ ist Schall und Rauch, so tönte es 2015 aus der Online-Sphäre der Cloud-Experten[2]. Doch ein deutscher Unternehmens- und Server-Standort hat dennoch eins, zwei Vorteile, die man nicht außer Acht lassen sollte.
Vorab sei jedoch gesagt: Verteufeln sollte man amerikanische Cloud-Angebote nicht, denn wenn es um Bedienungsfreundlichkeit und Innovation geht, sind diese teilweise (leider) noch um einiges Voraus. Zumindest ich glaube jedoch genug an den deutschen Markt, dass ich von einer Änderung zum Positiven in den nächsten 5-10 Jahren ausgehe.
Doch zurück zum Standort-Dilemma.

1. AGB

Ich werde in einem späteren Kapitel noch ausführlich auf AGB zu sprechen kommen, doch eins sei gesagt: deutsche Unternehmen sind sehr viel kundenfreundlicher, wenn es um Kündigung, Datenaufbewahrung und Information geht. Es ist nahezu unglaublich, wie viele schlecht oder spärlich formulierte AGB es im internationalen Raum gibt, so manch ein internationales Unternehmen mit einer deutschen Seite hat schlecht übersetzte AGB und mir ist mindestens ein Fall bekannt, in dem der deutsche Nutzer sich – sollte er nicht genug Englisch verstehen – mit der Google Translate-Version begnügen muss. Glauben Sie mir – bei dem Stand, auf dem Google Translate aktuell (09/15) ist, dürfte so eine AGB vor keinem Gericht standhalten.

Bild: Google Translate



Ein kleines Beispiel, wie unsere AGB aussehen würden, wenn wir sie via Google Translate übersetzt hätten.

Eine deutsche AGB geht derweil insbesondere bei Unternehmens-Lösungen sehr genau auf notwendige Datenschutzrichtlinien und vertragliche Verantwortungen beider Parteien ein (es gibt natürlich auch Ausnahmen), nicht zuletzt, weil die Kunden nun einmal genau das einfordern (ein amerikanisches Unternehmen, selbst wenn es sich auf dem deutschen Markt positionieren will, wird eher schrittweise die deutsche Bürokratie aufbröseln und in die Datenschutzrichtlinien und AGB integrieren).

2. Sprachwirren im Support

Wussten Sie, dass Dropbox eine eigene Support-Community hat? Schade nur, dass diese nur teilweise Deutsch ist. Ähnlich sieht es mit zahlreichen anderen internationalen Anbietern aus. Selbst wenn die Seite (und die AGB und Datenschutzrichtlinien) auf Deutsch ist, müssen die deutschen Unternehmensstandorte vorerst mit dem englischsprachigen Content vorlieb nehmen. Communities, Foren, Whitepaper und Blogs sind daher in vielen Fällen nur auf Englisch vorhanden, wer sich also nicht ganz so sicher mit der Lingua Franca fühlt, hat hier das Nachsehen.
In einigen seltenen Fällen kann es sogar sein, dass es nicht einmal einen deutschen Kontakt bei Fragen und Problemen gibt (achten Sie daher selbst bei einem deutschen Webauftritt immer darauf, ob es auch einen deutschen Unternehmensstandort gibt)

3. Datenschutzbestimmungen & Compliance

Wenn sich Ihre (sensiblen Daten) auf einem Server befinden, der nicht in Deutschland ist bzw. der von einem internationalen Unternehmen gehostet wird, müssen Sie als Unternehmen oder Selbstständiger erhöhte Sicherheitsvorkehrungen und –prüfungen erfüllen
Die Ursache dafür ist einfach zu erklären: innerhalb Deutschlands müssen Unternehmen bestimmte Datenschutzrichtlinien einhalten, wenn Sie Daten von Kunden oder Mitarbeitern lagern und/oder verarbeiten wollen. Darunter zählen entweder die Einwilligung der Kunden in die Weitergabe ihrer Daten, das Vereinbaren eines Datenverarbeitungsauftrags mit dem entsprechenden Dienstleister oder besondere Ausnahmefälle, die vor allem dem Nutzer zugute kommen sollen. Um jedoch so einen Auftragsdatenverarbeitungs-Vertrag, kurz ADV-Vertrag, auch rechtsgültig aufsetzen zu können, muss der Dienstleister seinen Sitz bzw. den Sitz seiner Rechner in einem Land mit ausreichendem Datenschutzniveau haben. Die USA oder China zählen beispielsweise nicht dazu. Daher sind Unternehmen in Deutschland angehalten, diese Risiken so weit wie möglich zu vermindern, indem sie internationale Unternehmen etwas stärker unter die Lupe nehmen (mehr dazu finden Sie im folgenden Kapitel „Personengebundene Daten“).

3. Wie - ein paar sichere Methoden zum Datenschutz

Das Passwort

Sicherlich werden Sie jetzt mit den Augen rollen, aber ein sicheres Passwort gehört zu den Grundlagen des effektiven Datenschutzes. Natürlich ist es kein Allheilmittel, aber nur weil Diebe auch Fahrradschlösser knacken können, binden Sie Ihr Fahrrad ja auch nicht mit einer Schnur an, oder?
Ein sicheres Passwort ist im Idealfall kein Wort aus dem Lexikon, besteht aus Sonderzeichen, Zahlen, Groß- und Kleinbuchstaben und sollte länger als 8 Zeichen sein. Außerdem empfiehlt es sich, das Passwort in regelmäßigen Abständen zu wechseln und es nicht mehrfach für verschiedene Accounts zu verwenden.

Verschlüsselung

Verschlüsselung codiert Ihre Daten und macht sie für jeden unleserlich, der über keinen Schlüssel verfügt. Der Schlüssel gehört im Idealfall nur Ihnen, so dass nicht einmal der Anbieter, der Ihre Daten verwaltet, Zugriff darauf hat.
Besonderes Augenmerk sei auf die Ende-zu-Ende-Verschlüsselung gelegt, die Daten nicht nur auf einem Server verschlüsselt (also im Banksafe), sondern auch auf dem Weg zu anderen Servern (quasi im Geldtransport). Besonders, wenn Sie Ihre Daten öfter herunter- und wieder hochladen oder an Kunden oder Kollegen verschicken, ist Ende-zu-Ende-Verschlüsselung angeraten.

Zweifach-Authentifizierung

Wer seinen Passwort-Künsten nicht traut, sollte auf die Zweifach-Authentifizierung vertrauen, denn die verlässt sich nicht auf eine einzige Login-Möglichkeit, sondern verlangt zwei. Beim Online-Banking werden beispielsweise nach Eingabe des Passwortes für Transaktionen Codes (TAN) auf Ihr Handy verschickt und erst nach Eingabe des Codes kann die Transaktion erfolgen.
Die Zweifach-Authentifizierung lohnt sich insbesondere dann, wenn Ihre Mitarbeiter sich beispielsweise nicht nur an einem Computer ins System einloggen, sondern auch unterwegs an fremden Computern, via Smartphone, etc.

Firewall

Die klassische Firewall schützt alles, was hinter ihren Mauern verborgen ist. In der Cloud kann eine Firewall aber auch Ihre Daten von anderen Daten abschirmen, selbst wenn diese auf demselben physischen Rechner lagern. Oft ignoriert, aber sehr wohl notwendig ist das Wissen über die Firewall auch auf mobilen Endgeräten, also Tablets, Laptops und Smartphones.
Eine Firewall kann individuell eingestellt werden, so dass sie bestimmte Daten, Downloads, etc. gar nicht erst zulässt. Aber: eine Firewall ist kein Allheilmittel, denn schädliche Software (Malware) via Mail, USB-Stick oder Lücken im System lässt sich – einmal drin – nicht von einer Firewall aufhalten.

Sicherheitssoftware

Sicherheitssoftware kennen Sie wahrscheinlich, weil Sie schon mal McAfee von Ihrem Computer gelöscht, oder aber tatsächlich wirksame Software installiert haben. Sicherheitssoftware ist dazu da, Malware zu erkennen, zu isolieren und bestenfalls zu löschen. Darüber hinaus kann sie auch Zugriffsberechtigungen, Einstellungen der Firewall und etliche andere Dinge kontrollieren.
Gerade für moderne, digitale Unternehmen sollte Sicherheitssoftware immer auch in der Lage sein, außerhalb der eigenen vier (Feuer-) Wände Zugriffe auf das System zu kontrollieren (etwa via Smartphone).

Nutzermanagement

Wer hat Zugriff zu welchen Dateien und kann was mit ihnen tun? Das richtige Nutzermanagement ist gerade heutzutage notwendig, um auch Kontrolle darüber zu haben, wer von wo aus Zugriff auf Dateien hat, Software laden und Daten nutzen kann. Auch Zugriffsbereiche (etwa Personaldaten) können so sicher eingeschränkt werden, damit nicht jeder sieht, was Frau Engels verdient und wo Herr Müller wohnt.

Backup

Vor Hackern oder Spionage schützt ein Backup nicht, doch wer mit sensiblen Daten umgeht, muss auch für deren Schutz vor ungeplanter Löschung gewappnet sein. Ein Backup ist eine Sicherheitskopie aller relevanter Daten (und teilweise auch Systeme), so dass nach Server-, Strom- und anderen Ausfällen der Betrieb so schnell wie möglich wieder aufgenommen werden kann. Ein gutes Backup dient daher nicht dazu, wie etwa bei Dropbox oder Sharepoint regelmäßig auf die Daten zuzugreifen.

Updates

Der oftmals gepredigte Vorteil von Cloud-Software liegt ja darin, dass neue Updates auch im Sicherheitsbereich automatisch getätigt werden. Wer jedoch noch installierte Software hat bzw. Updates gerne aufschiebt, weil sie nun einmal nervig und zeitaufwändig sind, der riskiert auch, dass veraltete Versionen und vor allem Sicherheitslücken im System länger als nötig die Umgebung unsicher machen.

4. Der kleine Unterschied: Daten auf den Sozialen Netzwerken

Bevor ich das nicht unerhebliche Thema der personengebundenen Daten bespreche, möchte ich noch einmal auf einen mittlerweile alltäglichen Aspekt eingehen, der aus Datenschutz-Sicht vielerorts kritisch betrachtet wird: die sozialen Netzwerke.

Facebook, Twitter, Instagram und Co sind allesamt kostenlose Dienste. Der gängige Spruch dahingehend lautet auch gerne (und etwas zynisch):

Wenn etwas im Netz kostenlos ist, bist Du die Bezahlung.

Tatsächlich versammelt man wohl nirgends so viele persönliche Daten, wie auf den sozialen Netzwerken (wenn man sie denn nutzt). Dabei ist es nicht per se gefährlich oder riskant, seine Filmvorlieben oder Lieblingsgerichte auf Facebook zu listen, doch sollte man sich immer bewusst sein, dass dieses und andere Unternehmen:
a.) diese Daten nicht gesondert sehen, sondern in der Kombination (Alter, Herkunft, Kontakte, Hobbies, Beruf, etc.) verwerten und auch verwalten (und das leider – wie das Safe Harbor-Urteil bezüglich Facebook gezeigt hat – nicht immer sehr vorbildlich).
b.) aus scheinbar harmlosen und unverfänglichen Daten sehr konkrete Profile erstellen können (so gibt es einige Studien, die aufzeigen, dass harmlose „Likes“ Aufschluss über die Sexualität, politischen Ansichten und Religionszugehörigkeit geben können[3]).

Datenhoheit & Datensparsamkeit

Wer nicht auf Facebook & Twitter verzichten, gleichwohl jedoch nicht sein Privatleben vor den Suchmaschinen und Algorithmen der digitalen Unternehmen ausbreiten möchte, sollte sich mit den Begriffen „Datenhoheit“ und „Datensparsamkeit“ vertraut machen.

Die Datenhoheit ist die Selbstbestimmung über das, was man den Suchmaschinen sozusagen „zugesteht“. Anstatt fraglos überall allen AGB zuzustimmen, Formulare auszufüllen und wirklich jedes Quiz (mit Klarnamen und Mailadresse) mitzumachen, überlegt sich der Netz-Nutzer, welche Datenangaben sinnvoll sind, welche potenziell zu intim sind und ob die Eingabe der Daten überhaupt nötig ist.
Wer sich eine Spiele-App installieren möchte, die Zugriff auf das Adressbuch, Fotos und mehr benötigt, sollte sich fragen, wozu beispielsweise die Fotos notwendig dafür sind.
Wer auf Facebook etwas liked bzw. auf anderen Medienseiten Beiträge liked oder via Facebook kommentiert, sollte überlegen, ob die Öffentlichkeit Zugriff auf diese Information haben sollte.

Im gleichen Atemzug lässt sich der Begriff „Datensparsamkeit“ verwenden, denn während die Datenhoheit den Überblick über die Daten gewährleistet, die man nach außen hin preisgibt, geht es bei der Sparsamkeit darum, die Anzahl einzudämmen und vor allem sinnvoll unter Kontrolle zu halten.
Natürlich machen Quizze und Persönlichkeitstests Spaß, aber ist es notwendig, dafür seine Mailadresse weiterzugeben oder diese auf Facebook zu posten?

Was einmal im Netz ist, kann nie wieder gelöscht werden – das liest man immer wieder. Rein faktisch stimmt das nicht ganz, doch sobald man Daten auf Plattformen veröffentlicht, auf denen sich Informationen schnell verbreiten und streuen, desto schwieriger ist es. Es ist eine Sache, seine Daten auf einen Cloud-Speicher zu lagern, den man im Ganzen löschen lassen kann. Es ist eine andere Sache, seine Daten auf Twitter zu posten, wo Retweets, Likes und Screenshots schnell dafür sorgen, dass die Kontrolle über die Daten scheinbar zwischen den Fingern zerrinnt (auch das ist ein Grund, warum man insbesondere mit persönliche Kommentaren, Postings und Informationen sparsam umgehen sollte).

Die sozialen Netzwerke im Beruf

Dank Xing und LinkedIn, aber auch durch offizielle Unternehmensauftritte auf Facebook, Twitter und Instagram vermischt sich das Private wie nie zuvor mit dem Beruflichen.
Viele Unternehmen nutzen soziale Netzwerke auch (und vor allen Dingen), um neue Leads zu generieren und Kontaktpunkte für Kunden und die, die es werden wollen, zu bieten.
Doch die nebulösen Grenzen sorgen auch dafür, dass Unternehmen zunehmend eben den Kontrollverlust riskieren, mit dem sich auch Privatpersonen herumschlagen – nur, dass es in ihrem Fall zahlreiche Mitarbeiter gibt, deren private Nachrichten tendenziell berufliche Inhalte in sich tragen (etwa, wenn über den Chef, die Arbeitszeiten, neue Projekte oder Kollegen gesprochen wird).
Insbesondere die Digital Natives haben kaum Berührungsgrenzen mit der Informationsfreigabe auf sozialen Netzwerken, doch wenn auch empfindliche Informationen aus dem Unternehmen gestreut werden, ergibt sich dadurch ein erhebliches Risiko.

Die Lösung: Aufklärung statt Verbot

In meinem Beruf gehören die sozialen Netzwerke zum Alltag. Ich poste für cloud world auf Facebook, Twitter, LinkedIn und Xing und bin auch privat in entsprechenden Datenschutz- und Cloud-Gruppen unterwegs. Für mich wäre es also kontraproduktiv, wenn man mir meinen Zugang auf Arbeit sperren würde.
Dafür weiß ich allerdings, was ich über meine Arbeit und mein Unternehmen posten darf und auch, wie ich mich gegenüber Kollegen, Kunden und Kollaborateuren verhalten soll.
Klären Sie Ihre Mitarbeiter darüber auf, was akzeptables Verhalten ist und welche Informationen geteilt werden dürfen und welche intern bleiben sollen. Viele Mitarbeiter wissen gar nicht, dass eine lapidare Beschwerde über die Launen des Chefs auf Facebook auch weitreichende Konsequenzen für das Unternehmen haben könnte. Geben Sie klare Richtlinien vor und lassen Sie diese notfalls auch vertraglich absichern. Denken Sie jedoch daran, dass vertragliche Klauseln vor allem dann wirksam sind, wenn sie auch noch einmal im persönlichen Gespräch (oder bei einem Workshop zum Thema) klar definiert und besprochen werden.

4. Personengebundene Daten: Mehr Schutz, mehr Regeln

Wenn es um sensible Datensätze geht, gehören personengebundene Daten nicht nur dazu, sondern bilden geradezu die Königsklasse, die mit besonderer Sorgfalt behandelt werden muss.

Doch was sind eigentlich personengebundene Daten?

Alle Daten, die direkten Rückschluss auf eine Person geben können, werden als „personengebundene Daten“ bezeichnet. Dazu gehören allerdings nicht nur offensichtliche Angaben wie Name, Adresse und Geburtsdatum, sondern selbst scheinbar nebensächliche Infos wie Hobbies, Erkennungsmerkmale, die IP Adresse und sogar Arbeitszeiten. Auch Daten, die alleine unverfänglich sind, aber in der Kombination Hinweise auf die Person geben können, gehören dazu.

Besonders sensible personengebundene Daten sind darüber hinaus Informationen über Krankheitsverläufe und andere eher privat/intime Daten. Diese müssen zusätzlich abgesichert werden, weshalb es gerade in diesen Bereichen (Krankenpflege, Ärzte, Anwälte) spezielle Software-Angebote von Dienstleistern gibt, die die sehr spezifischen Anforderungen nach der deutschen Gesetzeslage erfüllen.

Wer einem Dienstleister personengebundene Daten zur Weiterverarbeitung überlässt (sei es zur Speicherung, Analyse, etc.), muss eigentlich die Eigentümer dieser Daten (Kunden, Mitarbeiter, etc.) darauf hinweisen und es muss zudem durch sie eine aktive Erlaubnis erfolgen. Das bedeutet, dass der Eigentümer wissen muss, was mit seinen Daten geschieht und an welche Dienstleister sie weitergeleitet werden. Darüber hinaus muss er seine Erlaubnis dazu geben (etwa mit einem Häkchen, dass die entsprechenden Bestimmungen als „Akzeptiert“ markiert).
Gemäß des aktuellen Datenschutzgesetzes[4], das auch europaweit gilt (jedoch schon etwas angestaubt ist), dürfen die gesammelten Daten übrigens nicht ohne Wissen des Besitzers für andere Zwecke genutzt werden als in den Datenschutzhinweisen angegeben. Daher ist der spontane Verkauf von Kundendaten oder aber das Nutzen der Daten für andere als die angegebenen Zwecke rechtswidrig.

Alternativ ist auch ein Vertrag zur Auftragsdatenverarbeitung (ADV-Vertrag) gültig. Wann so ein Fall vorliegt und wie so ein Vertrag aussehen kann, wird vom Bayrischen Landesamt für Datenschutzaufsicht vorgegeben[5]. Dieser gilt quasi als Alternative zu der aktiven Zustimmung der Nutzer, geht jedoch auch mit einigen erhöhten Vorkehrungen und Prüfungen einher.

Da Sie als Auftraggeber die Verantwortung über den Schutz der personengebundenen Daten haben, liegt es an Ihnen, sicher zu gehen, dass der Anbieter die vereinbarten Sicherheitsvorkehrungen auch einhalten kann.
Das kann im kleinen Rahmen rein schriftlich erfolgen (wenn etwa weniger als 19 Mitarbeiter manuell personengebundene Daten verarbeiten oder weniger als 9 Mitarbeiter die Daten elektronisch verarbeiten[6]). Bei einer größeren Anzahl an Mitarbeitern, die mit den Daten in Kontakt kommen, müssen auch regelmäßige Prüfungen bzw. Audits unternommen werden.

Wie das aktuelle Urteil[7] (Stand 10/15) um das Safe Harbor-Abkommen gezeigt hat, sind dabei nicht nur besondere Sicherheitsmaßnahmen von Belang, sondern auch der Standort des Unternehmens bzw. der Hardware.
Wie Rechtsanwalt Thomas Schwenke in seinem Blog[8] erklärt und wie bereits im vorigen Kapitel erwähnt, ist der Standort Grundvoraussetzung für den ADV-Vertrag, da dieser nur dann gültig ist, wenn der entsprechende Dienstleister in einem Land mit ausreichendem Datenschutzniveau sitzt bzw. dort seine Rechner hat.

Zu diesen Ländern gehören:
- Länder innerhalb der EU
- Länder innerhalb der EWR
- Sichere Drittländer: Schweiz, Kanada, Argentinien, Andorra, Färöer, Guernsey, Israel, Isle of Man, Jersey, Australien, Neuseeland, Uruguay

Vor der Entscheidung, dass das Safe Harbor-Abkommen mit den USA ungültig sei, konnten sich amerikanische Unternehmen – die sich eigentlich nicht zu den sicheren Drittländern zählen dürfen – auf das Abkommen berufen. Mittlerweile wird allgemein geraten, nach den EU-Standardvertragsklauseln[9] zu gehen, die jedoch im Kontext von Safe Harbor ähnlich kritisch bewertet werden können.
Schwenke empfiehlt daher, sich entweder auf Anbieter aus sicheren Ländern zu beziehen, Nutzer aktiv zur Datenverarbeitung zustimmen zu lassen oder aber eindeutige ADV-Verträge auszuhandeln. Das könnte jedoch unter Umständen schwer werden, da die meisten US-Unternehmen (aktuell) noch gar keine anbieten.
Ein nicht unerhebliches Stichwort in diesem Kontext dürften die sogenannten „Binding Corporate Rules“ sein. Darin enthalten ist ein Audit mit einer nationalen Datenschutzbehörde, das so als unabhängige Prüfung der bestehenden Sicherheitsvorkehrungen gilt und so zwei Fliegen mit einer Klappe schlägt. Einen – zugegeben etwas angestaubten – Vorschlag hat die EU Kommission übrigens 2008 als PDF[10] veröffentlicht.

Ausnahmen

- Eine Ausnahme dieser Fälle tritt beispielsweise dann ein, wenn das Leben des Nutzers bewahrt werden muss (etwa, wenn es um das Weitergeben von Krankeninformationen bei einem medizinischen Vorfall geht).

- Weniger weltbewegend, dafür nicht weniger relevant ist der Ausnahmefall der Vertragserfüllung durch die Weitergabe der Daten. Bestellt man beispielsweise ein Produkt auf einer deutschen Online-Seite, das Produkt wird aber von einem amerikanischen Händler vertrieben, kann der Shop die Adressdaten an den Händler schicken, damit der Auftrag erfüllt werden kann.

- Die EU-Kommission[11] nennt darüber hinaus auch noch den Fall des öffentlichen Schutzes (etwa im Kampf gegen Kartelle, etc.). Dieser Punkt dürfte jedoch für Unternehmen zu 99,99% irrelevant sein.

5. Checkliste: Worauf muss ich bei den AGB und Datenschutzhinweisen achten?

Wer die AGB und Datenschutzhinweise nicht liest, der verliert die Kontrolle über seine Daten und deren Verwertung.
Die immer wieder populären Postings auf Facebook, in denen Nutzer sich dagegen aussprechen, sind nutzlos und rein rechtlich nicht von Belang. Wer nicht möchte, dass Facebook nichts mit den persönlichen Daten macht, der soll Facebook nicht nutzen.
Mit der folgenden Checkliste möchte ich zumindest ein paar Hinweise geben, worauf man insbesondere im Umgang mit persönlichen oder personengebundenen Daten achten sollte, wenn man sich durch die AGB liest.

Datenschutz

Wer hat Zugriff auf meine Daten?
- Gibt es Dienstleister, die der Anbieter auch beauftragt und inwieweit kann mir garantiert werden, dass meine Daten auch bei diesem Dienstleister sicher sind?
- Hat der Anbieter unverschlüsselten Zugriff auf meine Daten?

Wo werden Sie gelagert? (Serverstandort)
- Gehört der Serverstandort zu den sicheren Ländern, in denen ein hinreichendes Datenschutzniveau gewährleistet werden kann?
- Gibt es verteilte Server, so dass die Daten quasi „gespiegelt“ abgesichert werden und so bei Auswahl eines Servers nicht verloren gehen?
- Wie sind die Sicherheitsvorkehrungen innerhalb des Rechenzentrums (auch analog)?
- Wo befindet sich das Unternehmen?

Wie werden sie geschützt? (Verschlüsselung, u.a.)
- Welche Sicherheitsmaßnahmen werden vorgenommen, um meine Daten abzusichern?
- Gibt es unterschiedliche Maßnahmen für unterschiedliche Handhabung (etwa Zugriff via Smartphone)?
- Kann der Anbieter diese Maßnahmen nachweisen (Audits, ADV-Vertrag, etc.)?

Was passiert mit meinen Daten bei einer Testversion?
- Werden die Daten anschließend unwiderruflich gelöscht?

Kündigung

Wann kann gekündigt werden?
- Gibt es Kündigungsfristen (etwa drei Monate vor Ablauf der Vertragslaufzeit?
- Kann jederzeit gekündigt werden?
- Wird der Vertrag automatisch verlängert?

Was passiert mit meinen Daten, wenn ich gekündigt habe?
- Habe ich Zugriff auf meine Daten nach der Kündigung?
- Habe ich die Gelegenheit, alle Daten auf meine Systeme zurückzuführen?
- Werden meine Daten anschließend unwiderruflich gelöscht, damit der Anbieter keinen Zugriff mehr auf sie hat (gerade hier halten sich manche AGB vage und erklären, dass sie es sich vorbehalten, die Daten zu löschen. Handelt es sich aber um sensible Daten, müssen Sie vertraglich darauf bestehen, dass die Daten gelöscht werden).

Werde ich über eine Sperrung des Kontos oder einer Löschung meiner Daten informiert?
- Wenn nein, was geschieht mit meinen Daten?

Unterliegen meine Daten irgendwelchen Aufbewahrungsfristen?
- Wenn ja, welche Garantien habe ich?
- Gelten diese auch nach der Kündigung?
- Kann ich auch nach der Kündigung auf die Daten zugreifen?

Verwendung persönlicher (Profil/Konto-) Daten

Datennutzung
- Wie werden meine Daten genutzt?
- Welche meiner Daten werden wofür verwendet?
- Kann ich die unwiderrufliche Löschung meiner Daten anfordern?
- Kann ich einsehen, welche meiner Daten gesammelt wurden und wie diese verwendet wurden?
- Was passiert mit meinen Daten nach Löschung meines Kontos?

Drittparteien
- Werden meine Daten an Drittparteien zur Weiterverarbeitung geleitet?
- Ist klar formuliert, wofür meine Daten von den Drittparteien genutzt werden?
- In welchen Ländern sind diese Drittparteien ansässig und wie erfolgreich können meine Daten dort geschützt werden?

Quellennachweise & weiterführende Links

1.) Aufbewahrungspflicht für Daten der Buchhaltung
https://de.wikipedia.org/wiki/Aufbewahrungspflicht

2.) Rene Buest zum Sinn und Unsinn der Cloud Made in Germany
http://clouduser.de/analysen/sinn-und-unsinn-von-cloud-siegeln-zertifikaten-verbanden-und-initiativen-8124

3.) So kann Facebook Profile aus Likes erstellen
http://www.engadget.com/2015/01/13/facebook-like-psychometric-research/

4.) Das aktuell geltende europäische Datenschutzrecht
http://www.bmi.bund.de/DE/Themen/Gesellschaft-Verfassung/Datenschutz/Datenschutzrecht-EU/datenschutzrecht-eu_node.html

5.) Hinweise zur Auftragsdatenverarbeitung vom Bayrischen Landesamt für Datenschutzaufsicht (PDF)
https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/BayLDA_Auftragsdatenverarbeitung.pdf

6.) Ausnahmefälle für rein schriftliche Nachweise des Datenschutzes seitens des Dienstleisters
https://www.datenschutzbeauftragter-info.de/fachbeitraege/auftragsdatenverarbeitung/

7.) Das aktuelle Urteil des Europäischen Gerichtshofes zum Safe Harbor-Abkommen (PDF)
http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117de.pdf

8.) Blogbeitrag von Rechtsanwalt Thomas Schwenke zum Vorgehen nach dem Safe Harbor-Urteil
http://rechtsanwalt-schwenke.de/was-bedeutet-das-safe-harbor-urteil-des-eugh-fuer-sie/

9.) Wie sehen die EU-Standardvertragsklauseln aus?
https://www.datenschutzbeauftragter-info.de/auftragsdatenverarbeitung-was-sind-eu-standardvertragsklauseln/

10.) Binding Corporate Rules (PDF)
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_de.pdf

11.) Ausnahmen für die Auftragsdatenverarbeitung ohne Zustimmung der Nutzer bzw. ADV-Verträge (PDF)
http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=URISERV:l14012

Coverbild by poppicnic @ Pixabay

Über cloud world

cloud world ag ist der zentrale und neutrale Marktplatz für Cloud-Produkte und -Dienstleistungen im deutschsprachigen Raum und wurde 2013 in Pfäffikon, Schweiz) gegründet. Mit den Top-Domains cloud.de / .ch / .at / *.li ist cloud world der Anlaufpunkt für Cloud-Interessenten, -Experten und -Anbieter, der das Thema Cloud im deutschsprachigen Raum vorantreibt und eine erfolgreiche Werbe-Plattform für Anbieter bietet, die wiederum Anwendern durch Transparenz und Neutralität Vertrauen schafft.

Neben einem Directory, das SaaS-, PaaS- und IaaS-Produkte sowie cloudrelevante Services listet, bietet cloud world Informationen und Ratgeber rund um die Cloud an (Info-Center, Blog, Newsletter und kostenlose Leitfäden). Darüber hinaus können Anwender einzelne SaaS-Produkte in zielgruppenspezifischen Bundles zu attraktiven Kondition direkt über den Marktplatz beziehen.
cloud world ist auch an den deutschen Standorten Berlin und Karlsruhe vertreten.

Ihre Ansprechpartnerin

Juliane Waack
Online-Editor
Tel. +49 (0) 30 2589-4537
Mobil +49 (0) 174 188 05 31
E-Mail juliane.waack@cloud.de
Web http://blog.cloud.de/
Twitter: https://twitter.com/Jules_McCloud
LinkedIn: https://de.linkedin.com/pub/juliane-waack/96/3ab/78
Xing: https://www.xing.com/profile/Juliane_Waack