Kundendaten vor Datenkraken schützen. Daten werden heutzutage überall gesammelt, etwa von Konzernen wie Google und Microsoft. Dagegen nützen Datenschutzgesetze leider nicht viel. Deswegen muss man im Unternehmen die nötigen Massnahmen ergreifen, um Kundendaten und Geschäftsgeheimnisse zu schützen.

VON REGULA HEINZELMANN*

Microsoft hat eben das neue Betriebssystem Windows 10 auf den Markt gebracht. Dazu gibt es die Datenschutzbestimmung vom Juli 2015, die man vor der Installation lesen sollte. Windows 10 basiert auf einer Cloud und man kann es nicht nur für Computer, sondern auch für Tablets oder Smart Phones verwenden. Laut den Datenschutzbestimmungen generiert Windows 10 für jeden Benutzer eines Gerätes eine unverwechselbare Werbe-ID, die von App-Entwicklern und Werbenetzwerken verwendet wird. Die Kunden könnten diesen Zugriff deaktivieren, heisst es in den Bestimmungen.

Erfasst werden durch Windows 10 unter anderem Daten über Aussprache, Schreibstil (Handschrift), Spracheingabe, Informationen über Kontakte inklusive deren Namen, sowie Inhalte. Durch Deaktivieren dieser Eingabe-Personifizierung könne laut Microsoft die Datensammlung für diese Funktion beendet und die auf einem Gerät gespeicherten Daten, z.B. der Eingabeverlauf gelöscht werden.

Google speichert Inhalte. Wer Google nutzen will, muss der neuen Datenschutzerklärung vom 30. Juni 2015 zustimmen. Google erfasst gerätespezifische Informationen und nimmt Standortbestimmungen vor und speichert Inhalte. Die Standardbegründung für die Google-Datensammlung ist dem Sinn nach auch in Datenschutzerklärungen anderer Unternehmen enthalten: «Wir erfassen Informationen, um allen unseren Nutzern bessere Dienste bzw. Produkte, zur Verfügung zu stellen.»

Auch Betreiber von kostenfreien sozialen Netzwerken und sonstige Unternehmen lassen sich oft Nutzungsrechte zur Vermarktung und Weitergabe der eingestellten und veröffentlichten Inhalte einräumen und verwenden diese für Werbezwecke. In der Praxis verlieren Nutzer die Kontrolle und Übersicht darüber, was mit ihren Daten geschieht, besonders wenn sie in verschiedenen Netzwerken und Plattformen aktiv sind.

Sensible Kundendaten, die im Unternehmen verarbeitet werden, muss man vor der Datensammlerei der Internet-Konzerne wie Google, Microsoft oder Facebook schützen. Es ist Sache der Unternehmensleitung, entsprechende Richtlinien für die Angestellten zu erarbeiten und dafür zu sorgen, dass keine datenschutzrechtlichen Vorschriften verletzt werden, siehe Kasten.

DATENSCHUTZVORSCHRIFTEN FÜR UNTERNEHMEN

- Nach Datenschutzgesetz dürfen Daten nur rechtmässig, verhältnismässig und nach Treu und Glauben bearbeitet werden. Man muss darauf achten, dass sie korrekt sind.
- Bei der Datenbearbeitung muss man sich auf den Zweck beschränken, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.
- Ohne Rechtfertigungsgrund darf man Daten einer Person nicht gegen deren ausdrücklichen Willen bearbeiten oder besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgeben.
- Jede Person kann vom Inhaber einer Datensammlung kostenlose Auskunft darüber verlangen, welche Daten über sie gespeichert, verwertet und bearbeitet werden und zu welchem Zweck.
- Für Unternehmen sind angemessene technische und organisatorische Massnahmen zur Datensicherung vorgeschrieben. Einzelheiten findet man in der Datenschutzverordnung.
- Wer vorsätzlich geheime, besonders schützenswerte Personendaten oder Persönlichkeitsprofile unbefugt bekannt gibt, von denen er bei der Ausübung seines Berufes erfahren hat, wird auf Antrag mit Busse bestraft (Art. 35 DSG). Das gilt auch nach Beendigung der Berufsausübung oder während der Ausbildung.
- Für Klagen zum Schutz der Persönlichkeit muss man sich auf die Bestimmungen des ZGB (Artikel 28 ff.) beziehen (DSG Art. 15). Die klagende Partei kann insbesondere verlangen, dass die Datenbearbeitung gesperrt wird, keine Daten an Dritte bekannt gegeben oder die Personendaten berichtigt oder vernichtet werden.
- In der Regel liegt keine Persönlichkeitsverletzung vor, wenn eine betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat. Das Urheberrecht ist allerdings immer zu berücksichtigen.

Spionage über Smart-Geräte. Dass Smart Phone Apps häufig den Sinn haben, die Nutzer auszuspionieren, ist schon lange bekannt. Auch andere Smart-Geräte, z.B. Fernseher, sind heute mit Videokamera und Mikrophon ausgerüstet. Sobald sie mit dem Internet verbunden sind, können die Zuschauer überwacht werden, sogar mit Gesichtserkennung. Deshalb sollte man Smart-Geräte nur mit dem Internet verbinden, wenn es unbedingt notwendig ist. Bei Smart-Bildschirmen kann man auch den Zugang zur Kamera vorsichtig zukleben.

Smart-Geräte sollte man bei einem vertrauenswürdigen Unternehmer besorgen, der garantieren kann, dass das Gerät nicht vorher manipuliert wurde. Auch für mobile Geräte ist ein Antiviren-Scanner notwendig. Mobile Geräte mit

sensiblen (Kunden-)Daten soll man niemals verleihen oder unbeaufsichtigt lassen. Es ist sehr zu empfehlen, für berufliche Zwecke andere Smartgeräte zu verwenden als für private.

Betriebliche Fitnessprogramme – Daten sind Privatsache. Häufig bieten Arbeitgeber Fitnessprogramme an. Die Arbeitgeber dürfen aber Daten über die Angestellten nur bearbeiten, soweit sie deren Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind (OR Art. 328b). Der Arbeitgeber darf also nicht mittels Fitnessprogrammen Gesundheitsdaten über die Angestellten sammeln. Medizinische Daten gelten nach Datenschutzgesetz (DSG) als besonders schützenswerte Personendaten. Für ihre Bearbeitung ist eine freiwillige und ausdrückliche Einwilligung erforderlich.

Dazu ist auch zu prüfen, welche Gesundheitsapps man den Angestellten anbietet. «Der gläserne Konsument ist gleichzeitig ein gläserner Patient. Ihr Körper gehört nicht mehr Ihnen allein.» Diese Sätze findet man in dem Buch von Markus Morgenroth «Die wahre Macht der Datensammler.» Das Beratungsunternehmen ePrivacy hat rund 730 Gesundheits-Apps getestet. 78 Prozent der Apps konnten Drittpersonen nicht daran hindern, die Daten abzufangen. Bei 45 Prozent der Apps waren selbst hochsensible Daten nicht einmal verschlüsselt. Am besten stellt man für die Fitnesskontrolle Geräte zur Verfügung, die nicht mit dem Internet verbunden sind. Mit einer Computerschnittstelle (USB/WIFI/WLAN) können die Nutzer die Daten in ihren Privatgeräten verarbeiten und den Zugriff bestimmen.

WEITERE INFORMATIONEN

Offizielle Seiten:

- http://www.edoeb.admin.ch
- http://www.melani.admin.ch/
- Datenschutzerklärungen
- http://www.google.ch/intl/de/policies/privacy/
- http://www.microsoft.com/privacystatement/de-de/core/default.aspx
- Studie über medizinische Apps
- http://www.onetoone.de/ePrivacy-Studie-Nur-die-wenigsten-Apps-sind-sicher-26209.html

LEKTÜRE

- «Sie kennen dich! Sie haben dich! Sie steuern dich! Die wahre Macht der Datensammler», Markus Morgenroth, Droemer Knaur, 2014. www.droemer-knaur.de
- Ich glaube, es hackt! Tobias Schrödel, Springer Spektrum. http://ich-glaube-es-hackt.de/

* **Regula Heinzelmann** ist Juristin und freischaffende Journalistin in Dietikon und Berlin. **www.heinzelmann-texte.ch**