Datenmonster Informatik

Heute werden extrem viele Daten gesammelt. Zunehmend schreckt die IT die Bevölkerung als Datenmonster. Firmen wie Google erweisen der Branche einen Bärendienst.

Von Ueli Grüter

Die Informatik lässt es zu, Daten in Mengen zu sammeln und zu verarbeiten, wie dies nie zuvor möglich war. Zudem ermöglicht es die Informationstechnologie, Datensammlungen auf einfachste Weise zu kombinieren und über Konsumenten und Einwohner eigentliche Persönlichkeitsprofile zu erstellen. Dadurch entsteht die Gefahr des gläsernen Konsumenten respektive Einwohners. Die Möglichkeiten der Informatik bedrohen damit unsere Persönlichkeit. Datenschutz soll durch Vorschriften über das Sammeln und Verarbeiten von Daten, insbesondere mit den Mitteln der Informatik, die Persönlichkeit schützen. Der Schutz von Daten ist folglich nicht der Zweck, sondern das Mittel zum Zweck für den Persönlichkeitsschutz.

Rechtliche Grundlagen

Das Sammeln und Verarbeiten von Daten ist in der Schweiz grundsätzlich erlaubt, dies jedoch in den Schranken der Datenschutzgesetzgebung. Für die Datenverarbeitung durch Private, natürliche Personen und Unternehmen sowie die Bundesorgane gilt das Bundesgesetz über den Datenschutz. Die kantonalen Datenschutzgesetze dagegen regulieren ausschliesslich die Datenverarbeitung durch die kantonalen und kommunalen Stellen. Dabei wird jedoch nur das Sammeln und Verarbeiten von Personendaten von den Gesetzen reguliert. Personendaten sind Daten, die ohne weiteres einen Rückschluss auf eine natürliche oder juristische Person zulassen. Werden also zum Beispiel bei der Online-Lizenzierung respektive Online-Registrierung von Software nur Maschinendaten wie Hersteller, Prozessor oder Arbeitsspeicher, jedoch keine Daten über Personen wie den User-Namen erfasst, fällt die Erfassung selber und die Verarbeitung der entsprechenden Daten nicht unter das Datenschutzgesetz. Eine solche Datenerfassung ist denn auch persönlichkeitsrechtlich unbedenklich.

IN KÜRZE

- Dank der IT können leicht Daten gesammelt werden.
- Das Datenschutzgesetz legt fest, wofür Daten gebraucht werden dürfen.
- Die praktische Umsetzung des Datenschutzes bereitet Probleme.
- Firmen sollten einen Mitarbeiter bestimmen, der die Einhaltung des Datenschutzes kontrolliert.

Grundsätze des Datenschutzes

Die Grundsätze des Datenschutzes sind eigentlich einfach. Probleme bereitet in der Praxis, insbesondere in der Informatik, oft deren praktische Umsetzung. Es reicht nicht, lediglich die hehren Grundsätze in Privacy-Policies auf der Homepage zu publizieren. Die Grundsätze müssen in allen Geschäftsabläufen eines Unternehmens konkret angewandt werden. Dafür ist es ratsam, in der Firma selbst eine Person zu bestimmen, die für die Umsetzung der Datenschutzgrundsätze verantwortlich ist und bei Bedarf mit externen Datenschutzspezialisten zusammenarbeitet.

Personendaten dürfen sowohl von Privaten wie von staatlichen Stellen nur erhoben werden, wenn dafür eine gesetzliche Grundlage oder ein Rechtfertigungsgrund besteht. Ein Rechtfertigungsgrund ist regelmässig die Einwilligung des Betroffenen. Zudem gilt auch im Datenschutz der universelle Grundsatz von Treu und Glauben. Dies bedeutet, dass Daten für den Betroffenen erkennbar und transparent erhoben und bearbeitet werden müssen.

Als man Daten noch mühsam von Hand oder mit der Schreibmaschine erfassen und in der Folge auf Papier archivieren musste, hat man sich zweimal überlegt, ob man eine zusätzliche Information über eine Person festhalten möchte. Mit dem Einsatz der Informatik ist die Erfassung und Archivierung von Daten äusserst einfach und günstig geworden. Damit ist der Datenhunger der Unternehmen und des Staates gestiegen. Immer mehr will man von seinen Kunden und Einwohnern wissen. Damit steigt die Gefahr, den datenschutzrechtlichen Grundsatz der Verhältnismässigkeit zu verletzen. Dieser besagt, dass Daten nur dann erhoben und verarbeitet werden dürfen, wenn dies für den entsprechenden, den Betroffenen kommunizierten Zweck notwendig und geeignet ist.

Das wohl prominenteste Beispiel Verletzung dieses Grundsatzes ist der Fall der zweckfremden Verwendung von Umzugsdaten der Schweizerischen Post. Der Grundsatz der Zweckbindung besagt, dass Daten nur für den Zweck erhoben und bearbeitet respektive gebraucht werden dürfen, der bei der Erhebung der Daten den Betroffenen kommuniziert wurde. Die Schweizerische Post hat die neuen Adressen der Leute, die umgezogen sind und dies der Post gemeldet haben, aber ungefragt an Unternehmen weitergegeben, die die Daten mit ihren eigenen Stämmen abgeglichen haben. Die Post hat ihr Vorgehen damit begründet, dass es durch diese Massnahme zu weniger Fehlzustellungen komme. Da diese Drittverwendung den Betroffenen jedoch nicht oder zu wenig deutlich kommuniziert wurde und diese darum davon ausgehen mussten, dass ihre Daten lediglich für Nachsendungen verwendet werden, wurde der datenschutzrechtliche Grundsatz der Zweckbindung verletzt. Kommuniziert wurde also ein anderer Zweck als derjenige, zu dem die Daten dann noch zusätzlich verwendet wurden. Zwischenzeitlich hat die Post ihre Praxis in Absprache mit dem Eidgenössischen Datenschutzbeauftragten geändert. Die Betroffenen können nun ihr explizites Einverständnis für die Verwen-

dung zum Datenabgleich bei Dritten geben. Problematisch ist nun aber, dass ein Nachsendeauftrag mit Einverständnis der Drittverwendung nichts kostet, währenddem bei der Verweigerung eine Gebühr für die Nachsendung erhoben wird.

Falls die übrigen datenschutzrechtlichen Grundsätze erfüllt sind, das heisst also Daten rechtmässig erhoben und bearbeitet wurden, ist auch der Grundsatz der Integrität der Daten einzuhalten. Der Grundsatz der Integrität verlangt, dass die bearbeiteten Daten richtig und, soweit es der Zweck verlangt, auch vollständig sind. Unrichtige Daten sind auch nachträglich zu korrigieren.

Persönlichkeitsschutz durch Datensicherung

Im Zeitalter der Informatik ist Datenschutz im wesentlichen Datensicherung. Die Datenlecks bei Banken und Telekommunikationsunternehmen zeigen dies immer wieder exemplarisch. Wenn ein entsprechendes Leck auftritt, fühlen sich die Kunden wie nackt und in ihrer Persönlichkeit verletzt. Der Imageschaden der Unternehmen ist enorm. Das Gesetz verlangt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Diese Massnahmen haben die Vertraulichkeit, die Verfügbarkeit, die Integrität und Authentizität der Daten zu sichern. Sie müssen verhältnismässig sein und dem Stand der Technik entsprechen. Je intimer die Daten, desto höher sind die Anforderungen an die Sicherheit. Da das Gesetz wenig konkret ist, müssen die Massnahmen zur Datensicherung entsprechend der individuellen Situation in einem Unternehmen definiert und umgesetzt werden.

Auskunftsrecht

Wenn man testen will, ob in einem Unternehmen die Vorschriften der Datenschutzgesetzgebung systematisch und lückenlos umgesetzt werden, kann man dies mit einem einfachen Auskunftsbegehren nach Art. 8 DSG tun. Falls das Unternehmen innert Frist mit den gesetzlich verlangten Informationen antwortet, kann man mindestens davon ausgehen, dass Datenschutz bei der entsprechenden Firma kein Fremdwort ist. Die Resultate solcher Anfragen variieren stark und es ist erstaunlich, dass auch grosse Unternehmen mit der Auskunftspflicht immer wieder Mühe bekunden. Erstaunlich ist dies auch insofern, als die Verletzung von Art. 8 DSG strafrechtlich geahndet werden kann.

Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Der Inhaber der Sammlung muss ihr alle über sie vorhandenen Daten einschliesslich der verfügbaren Angaben über die Herkunft der Daten, den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie die Kategorien der bearbeiteten Personendaten, die an der Sammlung Beteiligten und den Datenempfänger mitteilen. Die Auskunft ist in der Regel schriftlich, in Form eines Ausdrucks oder einer Fotokopie sowie kostenlos zu erteilen. Vom Betroffenen kann zudem als Nachweis seiner Identität die Kopie einer Identitätskarte oder eines Passes verlangt werden. Ohne diesen Nachweis könnte das Persönlichkeitsrecht des effektiv Berechtigten verletzt werden.

Damit die Auskunftspflicht erfüllt werden kann, ist in einem Unternehmen eine entsprechende Ansprechperson zu bestimmen und sind die technischen Vorkehrungen zu treffen, dass die erforderlichen Daten innert der gesetzlichen Frist von 30 Tagen zusammengestellt und übermittelt werden können.

Umsetzung des Datenschutzes im Unternehmen

Was braucht es, um die Grundsätze des Datenschutzes in einem Unternehmen umsetzen zu können? Je nach Budget ist es wohl ratsam, vorab einen im Bereich Datenschutz spezialisierten Rechtsanwalt beizuziehen, um mit ihm die datenschutzrechtlich relevanten Bereiche zu ergründen. Danach ist ein Datenschutz-Reglement (auch: Privacy-Policy) zu erstellen, das alle organisatorischen und technischen Massnahmen erfasst. Dabei ist es wichtig, dass die Massnahmen auf die konkreten Umstände im Unternehmen abgestimmt werden. Schlussendlich ist es unerlässlich, eine Person zu bestimmen, die für die Umsetzung der Massnahmen und deren laufende Kontrolle verantwortlich ist.

Konsequenzen der Verletzung von Datenschutzbestimmungen

Was passiert, wenn ein Unternehmen die Vorschriften des Datenschutzes verletzt? Bis anhin waren die rechtlichen Konsequenzen vernachlässigbar, weil der Eidgenössische Datenschutzbeauftragte zur Durchsetzung des Datenschutzgesetzes entweder keine griffigen Kompetenzen hatte oder diese nicht wahrnahm. Zudem hat praktisch nur das Unterlassen der Auskunftspflicht strafrechtliche Konsequenzen. Zivilrechtlich hat sowieso nie jemand interveniert, weil das Kostenrisiko für den einzelnen Betroffenen in der Regel zu gross ist. Der grösste Schaden, der einem Unternehmen bis anhin entstand, war der Imageschaden, der im Bereich Datenschutz nach wie vor enorm sein kann. Nur schon aus diesem Grund empfiehlt es sich, die Grundsätze des Datenschutzes streng einzuhalten und unternehmensintern die dafür notwendigen regulatorischen, organisatorischen und technischen Massnahmen zu treffen. Seit einiger Zeit ist auch der Eidgenössische Datenschutzbeauftragte – neben seinen europäischen Kollegen – entschlossener in der Durchsetzung des Datenschutzgesetzes geworden, hat er doch vor kurzem Google wegen dessen Online-Dienst «Street View» beim Bundesverwaltungsgericht eingeklagt. ■

LESER FRAGEN, RECHTSANWALT GRÜTER ANTWORTET

Rechtsanwalt Ueli Grüter steht den LeserInnen des Swiss IT Magazine für kurze Fragen zu Informatik und Recht auch unter informatikrecht@gsplaw.ch und 043 430 32 70 unentgeltlich zur Verfügung. Fragen von allgemeinem Interesse werden in anonymisierter Form publiziert.

DER AUTOR

Ueli Grüter, LL.M., ist Rechtsanwalt in Zürich und Luzern und Dozent an der Hochschule Luzern mit Spezialgebiet Kommunikations- und Technologierecht. In der Serie «Informatikrecht für die Praxis» führt Grüter in 13 Folgen kurz und verständlich durch die rechtlichen Grundlagen in der Informatik und zeigt die rechtlichen Stolpersteine. Mit der letzten Folge erscheint die Serie dann auch als E-Book.

DATENSCHUTZGRUNDSÄTZE

- Rechtmässigkeit
- Treu und Glauben
- Verhältnismässigkeit
- Zweckbindung
- Integrität
- Sicherheit

Mehr zum Eidgenössischen Datenschutzbeauftragten unter www.edoeb.admin.ch.