Auch Schweizer Daten werden besser geschützt

Die EU-Datenschutz-Grundverordnung legt offen, in welchem Ausmass Firmen Personendaten erheben

Fast jede Schweizer Firma muss sich ans neue Datenschutzgesetz der EU halten. Dem Einzelnen verschafft es mehr Transparenz. Machen es die Firmen geschickt, resultiert daraus mehr als nur ein bürokratischer Mehraufwand.

GIORGIO V. MÜLLER

In einem noch nie da gewesenen Umfang bombardieren sie derzeit unsere E-Mail-Postfächer: Nachrichten von Firmen, die wegen geschäftlicher Beziehungen, des Kaufs eines ihrer Produkte oder einer ihrer Dienstleistungen an unsere Daten gekommen sind oder auch weil ein Wettbewerb lockte oder ein Newsletter abonniert ist. Grund der plötzlichen Aufgeregtheit ist die EU-Datenschutz-Grundverordnung (DSGVO), ein strengeres und umfassenderes Datenschutzgesetz, das ab diesem Freitag seine volle Wirkung entfalten wird.

Konsumenten werden nicht länger darüber im Dunkeln gelassen, welche Daten über sie erhoben werden. ANGEL GARCIA / BLOOMBERG

Vorsicht bei der Zustimmung

Für den Konsumenten hat diese E-Mail-Flut ihr Gutes. Schon jetzt hätten sie die Möglichkeit gehabt, von den Anbietern zu erfahren, welche Daten sie erheben, warum sie das tun und wie lange die Daten gespeichert werden. Jetzt reicht ein Mausklick, um dies zu erfahren. Dabei ist jedoch Vorsicht angebracht, denn es wird schwarze Schafe geben, die die Gelegenheit ausnützen, die Zustimmung zu neuen Diensten einzuholen oder sie von Personen zu bekommen, mit denen sie bisher noch gar nie Kontakt hatten. Auszuschliessen ist auch nicht, dass Hacker diese Chance nutzen, um als Einwilligungs-E-Mail getarnte Schadsoftware zu verbreiten. Die Verordnung legt fest, dass es nicht nur eine explizite Einwilligung des Konsumenten braucht, sondern dies zudem auf auch für Laien leicht zu verstehende Weise geschehen muss («verständliche und einfache Sprache»). Nun gibt es kaum mehr Ausreden, man habe nicht gewusst, welche heiklen Daten erfasst würden.

Je nach Unternehmen werden diese Hausaufgaben unterschiedlich erledigt. Jene, die vielleicht nur eine E-Mail-Adresse von jemand haben, bemühen sich um eine Zustimmung, diese auch künftig vorhalten zu dürfen. Bei einem Navigationsgerät für ein Fahrzeug wird es schon etwas komplexer. Hier muss der Hersteller detailliert darlegen, welche Daten erhoben werden, wofür und wo und wie lange sie gespeichert werden. Stets besteht die Möglichkeit, dies zu unterbinden. Diese Einschränkung muss indes meist mit einer Beeinträchtigung der Dienstleistung erkauft werden. In einigen Fällen ist eine Zurückweisung sogar mit der Beendigung der geschäftlichen Beziehung verbunden, wenn zum Beispiel ein Navigationsgerät oder ein Fitnessarmband den Standort des Nutzers nicht mehr erfassen darf.

Nützlicher Lernprozess

Geschäftstüchtige Firmen beweisen, dass die bürokratische Übung dazu verwendet werden kann, die Beziehungen zum Kunden zu festigen. Weil im Sinne der Transparenz und Verständlichkeit der Regeln ausdrücklich auch visuelle Informationen erlaubt sind, verbinden einige Firmen das Erforderliche mit dem Nützlichen. So hat die britische Gesellschaft Heathrow Airport ein Videofilmchen gemacht, mit dem nicht nur über die neuen Datenschutzregeln informiert wird, sondern auch auf die Vorzüge des Londoner Flughafens hingewiesen wird. Wer je einmal das kostenlose WLAN des Flughafens nutzte, wird eine solche Nachricht erhalten.

Sich durch all die vielen Details durchzuarbeiten, ist zwar mühsam, aber hilfreich. Dem einen oder anderen werden sie die Augen öffnen, wie viele persönliche Details die Firmen über ihn wissen. Wer die tollen Angebote, die erst durch die Digitalisierung möglich wurden, auch weiterhin nutzen will, wird seine Einwilligung geben. Dank diesem Lernprozess wird er dies jedoch aus einer informierten Position aus tun.

Der Zweck eines neuen Gesetzes oder einer neuen Verordnung bemisst sich daran, ob damit eine Verbesserung verbunden ist. Prinzipiell hätte es die DSGVO nicht gebraucht, allein in Europa gibt es seit Jahren mehr als 200 verschiedene Datenschutzgesetze. Auch in der Schweiz besteht schon seit einem Vierteljahrhundert ein solches Gesetz (das sich derzeit in der Revision befindet). Ihr Handicap ist jedoch, dass sie nur national regeln können. In Zeiten von Plattformwirtschaft und Globalisierung ist dies nicht mehr zeitgemäss und schürt höchstens einen unguten Regulierungswettlauf. Für Bruno Wildhaber vom Zürcher Kompetenzzentrum Records Management (KRM), dessen Firma sich seit Jahren mit solchen Fragen beschäftigt, erfüllt die DSGVO ihren zentralen Zweck. Wegen der gestiegenen Transparenz habe der Einzelne nun eine bessere Kontrolle darüber, was mit seinen Daten geschehe: «Es ist eine mühsame Aufgabe, nützt aber allen», sagt er.

Einerseits bedeuten die strikteren Vorschriften eine Stärkung der informellen Selbstbestimmung, eines urliberalen Guts, das es zu verteidigen gilt. Andererseits haben sie für die betroffenen Unternehmen einen Mehraufwand zur Folge. Erstaunlicherweise sind noch nicht alle bereit, wenn es ernst gilt, obwohl die Verordnung schon vor zwei Jahren in Kraft getreten ist und nur wegen der gewährten Übergangsfrist nicht sofort angewendet wurde. In den vergangenen Monaten hätten sich die Anfragen gehäuft, sagt Wildhaber: «Die Firmen sind aufgewacht, haben realisiert: Wir müssen etwas machen.» In der Schweiz gingen vor allem die kleineren Unternehmen mit viel Pragmatismus ans Werk, was auch sinnvoll sei, denn trotz der mehrjährigen Formulierung der Verordnung seien noch viele Details im Unklaren.

Eines davon ist der Datenschutzbeauftragte, der im Unternehmen dafür verantwortlich ist. Wie bei allen Compliance-Angelegenheiten liegt die juristische Verantwortung aber weiterhin beim Verwaltungsrat. Zudem braucht es einen Beauftragten nur, wenn systematisch und heikle Daten erhoben werden (Finanz- und Gesundheitsdaten fallen darunter). Der Datenschutzbeauftragte arbeitet eher wie ein interner Revisor, bei Datenschutzverletzungen schlägt er Alarm, damit die zuständige nationale Behörde benachrichtigt werden kann – und dies in 72 Stunden.

Von Kunden honoriert

Dass dies auch für kleinere Unternehmen machbar ist, zeigt das Beispiel Feintool. Schon seit Jahren habe die Firma sich mit den Auswirkungen der DSGVO beschäftigt und sie umgesetzt, vor allem hinsichtlich IT-Prozessen, zum Beispiel bei Lieferantenverträgen oder wo es sich um Personaldaten handelt, erklärt Pressesprecherin Karin Labhart. Weil fast die Hälfte der Mitarbeiter in Deutschland arbeitet, lag dies auch auf der Hand. «Wir wenden die EU-Richtlinien weitgehend auch in der Schweiz an.» Dies ist auch für Wildhaber vernünftig. Entsprechend gut sei Feintool auf die DSGVO vorbereitet, auch wenn es noch etwas «Feinabstimmung» brauche, ergänzt Labhart.

Auch beim Anlagenbauer Bühler in Uzwil (SG) seien interne und externe Projekte im Hinblick auf die DSGVO am Laufen, sagt Pressesprecher Burkhard Böndel, was einen bürokratischen Mehraufwand bedeute. So werde zum Beispiel das Einverständnis der Personen eingeholt, die den Newsletter des Unternehmens abonniert hätten.

Firmen müssen sich auch bewusst sein, dass sie bei an Dritte ausgelagerten Aufgaben (Cloud-Dienstleistungen) ihre Verantwortung für den Datenschutz nicht ebenfalls ausgelagert haben. Diverse Umfragen belegen, dass Firmen, die den Datenschutz ernst nehmen, auch von den Kunden honoriert werden.

Amerikas Datenschutz ist ein Flickenteppich

In den USA wird verstärkt über den Umgang mit persönlichen Daten diskutiert – das neue Gesetz der EU dient aber nicht als Vorbild

CHRISTIANE HANNA HENKEL, NEW YORK

Mit dem nun in Kraft getretenen Datenschutzgesetz hat die EU ein Regelwerk geschaffen, das in der einen oder anderen Form auch auf die USA und damit den derzeit weltweit wohl wichtigsten Motor der Digitalisierung Einfluss haben wird. Zum einen müssen US-Firmen, die in Europa tätig sind bzw. europäische Kunden betreuen, dem neuen Regelwerk Folge leisten. Technologiekonzerne wie Alphabet, Apple und Facebook, aber auch Industriekonzerne wie General Electric erwirtschaften oft einen bedeutenden Teil ihres Umsatzes in Europa und haben ihre Aktivitäten auf das neue Gesetz abgestimmt.

EU-Gesetz als Referenzpunkt

Zum andern hat die EU mit dem Regelwerk einen Referenzpunkt geschaffen für die laufenden Diskussionen in den USA zu den Themen Datensicherheit und Privatsphäre. In Amerika hat man bisher einen recht lockeren Umgang mit persönlichen Daten gepflegt. Amerikaner sind es gewohnt, dass ihre Adressen in die Hände Dritter gelangen und ihre Briefkästen dann mit persönlich adressierten Werbebriefen gefüllt werden. Eine generell recht geringe Regulierungsdichte in diesem Bereich hat nicht zuletzt den Aufstieg jener Technologiekonzerne erleichtert, deren Geschäftsmodell auf dem Verkauf zielgenauer Werbung basiert, wie etwa Facebook (mit seinen Social-Media-Töchtern Facebook, Whatsapp und Instagram) oder der zum Alphabet-Konzern gehörende Suchmaschinenbetreiber Google. Auch Betreiber elektronischer Marktplätze wie Airbnb und Uber haben vom generell lockeren Umgang in den USA im Bereich Datenschutz und Privatsphäre profitiert.

Zwei jüngere Vorkommnisse haben jedoch das Thema in die Öffentlichkeit gezerrt. Zunächst der umfangreiche Diebstahl von Daten bei der Kreditdaten-Firma Equifax; das Unternehmen verfügt über eine umfangreiche Datensammlung, die genutzt wird, um die Kreditwürdigkeit von rund 800 Mio. Individuen zu bestimmen. Im September 2017 gab das Unternehmen bekannt, persönliche Daten von über 145 Mio. Individuen seien gestohlen worden. Unter diesen Daten befanden sich die in den USA sehr wichtige und oft zu Betrugszwecken entwendete Sozialversicherungsnummer, samt Adresse, dem vollen Namen, dem Geburtsdatum und in einigen Fällen auch der Fahrausweisnummer.

Das zweite Ereignis, das das Thema Daten ins Gedächtnis der Öffentlichkeit rief, war die Cambridge-Analytica-Affäre; sie brachte ans Licht, dass sich die gleichnamige Firma für politische Beratung Zugang zu persönlichen Daten von über 80 Mio. Facebook-Nutzern verschaffen konnte. Die Affäre hat den US-Kongress dazu bewogen, Facebook-Konzernchef Mark Zuckerberg gleich zu zwei Anhörungen einzuladen. Facebook muss sich mittlerweile den Vorwurf gefallen lassen, nicht nur mit den Daten der Nutzer fahrlässig umzugehen, sondern auch über die Verbreitung von Fake-News sowie als Plattform für ausländische politische Kräfte die Demokratie des Landes zu gefährden.

Mehr Intelligenz ausserhalb des Hirns
Kommentar auf Seite 13

Die Fälle Equifax und Facebook haben vielen Amerikanern vor Augen geführt, dass sie oft nicht wissen, welche Daten die diversen Unternehmen über sie zusammengetragen haben und wie und ob die Firmen diese weiterleiten. Auch ist vielen erst jetzt bewusst geworden, dass die Unternehmen es vielfach nicht vermögen, Kundendaten vor dem unbefugten Zugriff Dritter zu schützen. Vor diesem Hintergrund werden die Datenschutzbemühungen der Europäer und besonders die Auswirkungen des nun in Kraft getretenen EU-Datenschutzgesetzes mit grossem Interesse verfolgt.

Amerika selbst verfügt sehr wohl über Gesetze, die den Umgang der Firmen mit persönlichen Daten ihrer Kunden regeln. Dabei handelt es sich allerdings um einen womöglich zu löcherigen und in Teilen veralteten Flickenteppich an landesweit oder auch nur in einzelnen Gliedstaaten geltenden, während Jahrzehnten erlassenen Gesetzen. Zudem gibt es spezifische, nur für einzelne Branchen geltende Regelungen wie etwa für die Finanzbranche oder für den Umgang mit Patientendaten. Kritiker monieren, die vorgesehenen Bussen und Sanktionen seien zu niedrig bzw. zu schwach. Die Konsumentenschutz- und Wettbewerbsbehörde FTC, die gerade in Sachen Datenschutz den Unternehmen versucht auf die Finger zu schauen, fordert seit Jahren ein umfassendes Gesetzeswerk, das landesweit und branchenübergreifend gültig ist. Ein entsprechender Vorstoss der Regierung Obama verlief aber im Sande.

Sorge um Standortnachteile

Im Nachgang zur Affäre um Cambridge Analytica und Facebook haben zwei Senatoren Ende April mit der Social Media Privacy Protection and Consumer Rights Act of 2018 einen Gesetzesvorschlag eingebracht, der sich speziell auf Online-Plattformen und soziale Netzwerke bezieht. Ähnlich wie nun in der EU werden den Kunden umfangreiche Rechte in Bezug auf ihre Daten eingeräumt. Der Gesetzesvorschlag ist aber nicht so umfassend wie das EU-Gesetz. Auch sieht er nicht drakonische Strafen vor. Generell steht man dem EU-Gesetz in den USA kritisch gegenüber. Es bestärkt zwar viele in der Ansicht, die USA benötigten ein modernes Datenschutzregelwerk. Man will aber kein bürokratisches Monster schaffen, das Innovation und Wettbewerbsfähigkeit des Standorts USA beschädigt.