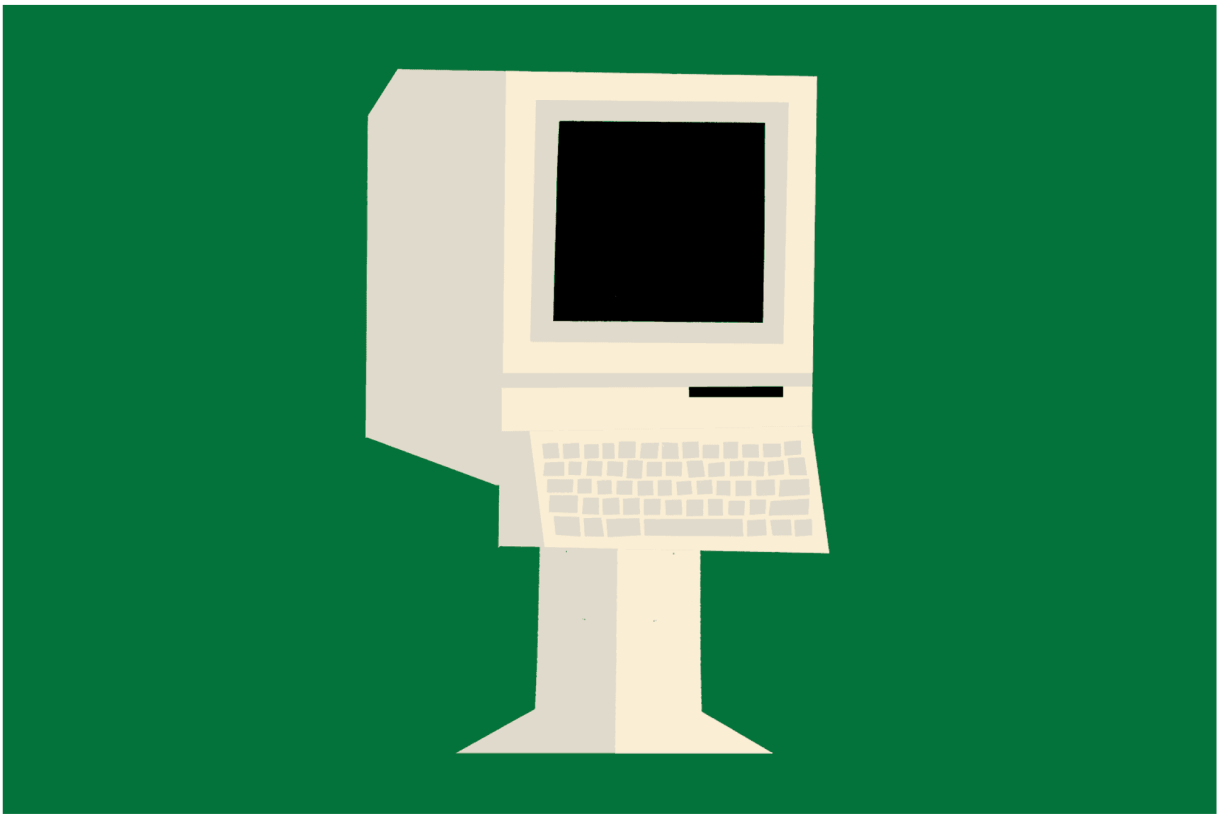
# Datenschutz, der nur ein bisschen wehtut

Das revidierte Schweizer Datenschutzgesetz schafft neue Verbindlichkeiten bei der IT-Sicherheit. Aber dieses Gesetz allein bringt noch keinen echten Fortschritt.

Von Adrienne Fichter (Text) und Adam Higton (Illustration), 29.08.2023



Erinnern Sie sich noch an die Computer der 1990er-Jahre? Damals tippte man auf Tastaturen vor graubeigen Apple-Macintosh-Ungetümen mit Diskettenlaufwerken.

Bilder solcher Computer zeigt die IT-Anwältin und Dozentin Anne-Sophie Morand ihren Studentinnen jeweils auf der ersten Folie ihrer Präsentation.

Später löst sie auf, was sie damit veranschaulichen will: «So alt ist unser Datenschutzgesetz.» Die Reaktion der Studenten: offene Münder. Das Datenschutzgesetz der Schweiz stammt noch aus dem Jahr des allerersten Browsers, 1992. Also aus den ersten Stunden des weltweiten Internets.

Am 1. September ist mit dem veralteten Gesetz Schluss. Dann tritt das totalrevidierte Datenschutzgesetz in Kraft. Dann erhält die Schweiz endlich ein Datenschutzrecht, das diesen Namen auch verdient. Die vom Parlament grosszügig gewährte Gnadenfrist für Schweizer Unternehmen ist da-

mit vorbei. Denn die Privatwirtschaft hatte seit 2020 Zeit, auf die neuen Regeln umzustellen.

## Verwässertes Vorbild

Die Vorlage für das revidierte Schweizer Gesetz ist die europäische Datenschutz-Grundverordnung (DSGVO) von 2018. Viele Elemente aus dem EU-Regelwerk finden sich fast eins zu eins im Schweizer Gesetz: das Recht auf Auskunft über die eigenen Daten und auf deren Löschung, das Prinzip Datensparsamkeit bei allen Programmen, Software und Plattformen.

Die digitalen Rechte von Einwohnerinnen der Schweiz werden also ab dem 1. September gestärkt.

Doch wie so oft beim Nachvollzug von EU-Regeln zeigen sich auch hier Schweizer Eigenheiten. Die mehrheitlich bürgerlichen National- und Ständeräte haben nur die nötigsten Pflichten für Unternehmen übernommen. Ausserdem gibt es einen grundsätzlichen Unterschied: In der Schweiz ist alles erlaubt, was nicht explizit verboten ist. In der EU gilt das umgekehrte Paradigma: Nichts ist erlaubt, ausser es wird explizit erwähnt.

Konkret: Wer in der Schweiz nicht damit einverstanden ist, dass Kunden-Hotlines biometrische Stimmenprofile von Anruferinnen erstellen, muss dem aktiv widersprechen. Ansonsten wird es einfach gemacht. In der EU hingegen müsste im gleichen Fall ein «Ja, ich will» vom Kunden eingeholt werden, bevor die Funktion aktiviert wird. Die Digitale Gesellschaft kritisiert denn auch, dass sich Schweizer Unternehmen auf allerlei «Rechtfertigungsgründe» berufen dürfen, wenn sie Daten von Nutzerinnen verarbeiten.

Dass das Parlament an der ursprünglichen Gesetzesvorlage des Bundes während mehrerer Sessionen «herumgedoktert» hat, finden viele IT-Anwälte, mit denen die Republik gesprochen hat, unproblematisch. Man habe in der EU gesehen, was funktioniere, und könne auf deren *lessons learned* aufbauen, so der Tenor.

«Das Schweizer Datenschutzgesetz ist nicht schwächer als die europäische Datenschutz-Grundverordnung», sagt etwa IT-Jurist David Rosenthal. «Wir sind aber bei den flankierenden Massnahmen, etwa bei den Datenschutzerklärungen, Verträgen oder Dokumentationspflichten, praktikabler, flexibler und weniger bürokratisch. Für viele KMU ist deren konsequente Umsetzung trotz allem eine Last.»

Unter dem alten Schweizer Datenschutzgesetz hatten unzureichende Sicherheitsvorkehrungen von Firmen kaum Folgen. Einerseits verfügte der eidgenössische Datenschutzbeauftragte lediglich über beschränkte Befugnisse. Andererseits stand den von Datendiebstählen betroffenen Bürgern nur der beschwerliche zivil- oder strafrechtliche Weg offen.

Wird also das neue Gesetz dieser Kultur der gefühlten Straflosigkeit ein Ende setzen?

Ja und nein.

## Die Verantwortung des Managements

Gemäss dem revidierten Gesetz müssen Unternehmen künftig in Cybersicherheit investieren und präventiv aktiv sein. Doch anders als in der EU wird die Verantwortung individualisiert. Das bedeutet: Unternehmen wer-

den bei Versäumnissen nicht gebüsst. Angestellte des Unternehmens dagegen können mit einer Busse von bis zu 250'000 Franken belangt werden.

Es ist fraglich, ob diese Individualisierung einer firmeninternen Fehlerkultur zuträglich sein wird. Wird etwa die Sachbearbeiterin gebüsst, die auf ein Phishing-Mail geklickt und damit ungewollt den Zugriff auf das firmeninterne Netzwerk ermöglicht hat? Fragen wie diese müssen Unternehmen nun durchdenken und intern reglementieren.

Die gute Nachricht: Das Datenschutzgesetz schreibt nicht nur Pflichten zur IT-Sicherheit für Unternehmen intern vor, es gilt auch für deren externe «Auftragsbearbeiter». Somit müssen auch IT-Lieferantinnen der Bundesverwaltung Auflagen erfüllen, die im Auftrag einer Behörde Daten bearbeiten und speichern.

Der Bundesrat möchte das Thema ausserdem zur Chefaufgabe erklären. Gemäss der Website «Onlinekommentar» – einem Portal, auf dem Fachjuristen neue Gesetze interpretieren – sollen Firmenverantwortliche beim Thema IT-Sicherheit in die strafrechtliche Pflicht genommen werden. Mit anderen Worten: Management und Verwaltungsrat müssen zukünftig gesetzlich bedingt Cybersecurity ernst nehmen. Und das ist gut so.

Lückenhaft ist das Gesetz hingegen, was die Informationspolitik betrifft. Werden Betroffene nicht über Datendiebstähle informiert, hat dies keinerlei Konsequenzen. Die bisherige Praxis von Unternehmen verspricht in dieser Hinsicht nichts Gutes, wie der Datendiebstahl bei den Medienunternehmen NZZ und CH Media durch die Ransomware-Gruppe Play zeigt. Dabei unterliessen es die Unternehmen, ehemalige Angestellte darüber zu informieren, dass deren AHV-Nummern, Postadressen und Bankkontonummern gestohlen wurden und frei im Darknet verfügbar waren.

Die NZZ erteilte lediglich eine allgemeine Auskunft über die gestohlenen Daten, etwa, dass es sich dabei um Personalien und Lohnausweise handelte. Der Sprecher des eidgenössischen Datenschutzbeauftragten, Nicolas Winkelmann, stellt hingegen klar fest: Die NZZ müsse Betroffene informieren, wenn sie Bescheid über die individuellen Details pro Person wisse.

Es liegt auf der Hand, weshalb die NZZ sich windet. Sie will den Aufwand von Massenanfragen vermeiden. Und: Der Medienkonzern hat auch nichts zu befürchten. Vertuschung und Nichtinformation werden – anders als in der EU – auch unter dem revidierten Schweizer Datenschutzgesetz nicht sanktioniert. Unternehmen dürfen also bei Datenlecks ihre Kundinnen im Dunkeln lassen.

Damit bleibt nur noch eine Institution, die in diesem Punkt das Recht durchsetzen kann: der eidgenössische Datenschutzbeauftragte Adrian Lobsiger. Seine Rolle wird per 1. September aufgewertet, er erhält mehr Ressourcen und Kompetenzen. Neu kann er Verfügungen aussprechen und verlangen, dass unsichere IT-Produkte sofort gestoppt werden. Gut möglich, dass Lobsiger bald ein Exempel statuiert, um die Öffentlichkeit für die neue Ära wachzurütteln. Doch angesichts der schieren Masse von täglichen Datenschutzverstössen im digitalen Zeitalter wird auch er sich nur um die «grossen Fische» kümmern können.

Darüber hinaus bleibt nur noch ein Korrektiv übrig: die vierte Gewalt.

Solange Medien weiterhin schonungslos über Datenschutzverstösse berichten und Sicherheitslücken aufdecken, werden Unternehmen allein aus Gründen der Reputation die neuen Datenschutzregeln ernster nehmen

müssen. Der Grossteil möchte das Vertrauen ihrer Kundschaft nicht aufs Spiel setzen. Dies stellt auch Anwältin Anne-Sophie Morand in ihrer Arbeit fest: «Die Unternehmen wollen gesetzeskonform sein. Niemand möchte bei diesem Thema einen Imageschaden riskieren.»

## Konsumentinnen müssen ihre Rechte einfordern

Viel wichtiger als die Ahndung von Verstössen ist das Verhalten der Konsumenten: Ein guter Schutz der Privatsphäre muss von mündigen Kundinnen eingefordert werden. In Zeiten, in denen Unternehmen künstliche Intelligenzen mit grossen Massen von Daten trainieren, ist nicht nur das explizite Einverständnis der Konsumenten für solches Modelltraining wichtig, sondern auch die Zusicherung der Firmen, dass die entsprechenden Daten gut geschützt sind.

Der Markt spielt in diesem Punkt nicht wirklich: Firmen lagern die Verantwortung zu oft an Konsumentinnen, Kunden und Nutzerinnen aus. «Schwachstelle Mensch» heisst das im Jargon, damit gemeint ist beispielsweise das Fehlverhalten von Usern.

Die zahlreichen Datenlecks bei Behörden wie etwa beim Bundesamt für Polizei oder bei der Kantonspolizei Bern, die gefühlt jede Woche publik werden, zeigen ausserdem einen Systemfehler bei Beschaffungen. IT-Sicherheit ist ein anstrengender Prozess, der nie abgeschlossen ist. Doch gerade beim Outsourcing von Projekten an externe IT-Dienstleister nehmen die Behörden ihre Aufsichtspflicht kaum wahr. Dies stellt der Bundesrat selber fest: «Eine wesentliche Lücke im Management der Informationssicherheit der Bundesverwaltung und der Armee sind heute die fehlenden Kontrollen und Audits.»

Doch auch hier gibt es eine gute Nachricht: Am 1. Januar 2024 tritt das neue Informationssicherheitsgesetz in Kraft, das alle Lieferanten des Bundes strenger in die Pflicht nehmen und das Nationale Zentrum für Cybersicherheit des Bundes aufwerten wird.

Bleibt zu hoffen, dass es damit zur Korrektur kommen wird. Solange IT-Sicherheit und Datenschutz nicht angemessen in Produkte eingepreist werden, ist das Datenschutzrecht lediglich ein Instrument für Pflästerli-Politik.