Schon seit vielen Jahren gibt es in Österreich eines der schärfsten Datenschutzgesetze. Bisher gab es aber kaum Sanktionen bei Verstößen; diesen wurde selten und wenn, dann nicht besonders intensiv nachgegangen. Die wenigen bekannt gewordenen Fälle wurden medial kaum verarbeitet und konnten daher keine abschreckende Wirkung zeigen.

Dies hat sich durch die Datenschutzgrundverordnung (DSGVO) seit dem 25. Mai dieses Jahres grundlegend geändert. Die maximalen Strafandrohungen von bis zu 4% des Konzernumsatzes oder 20 Mio. EUR ließen doch viele Menschen aufhorchen und brachten sie dazu, sich mit dem Thema Datenschutz ernsthaft und genau auseinanderzusetzen, was als sehr positiv zu bewerten ist. Leider klagen die Datenschutzbehörden europaweit, dass sie ressourcenmäßig massiv unterausgestattet sind und daher ihre alten und neuen Kontrollfunktionen kaum wahrnehmen können.

Durch die neue Gesetzgebung der DSGVO haben Konsumenten nun wesentlich bessere und schärfere Werkzeuge, um ihre Rechte an den eigenen Daten durchzusetzen. Bei vielen Unternehmen – vor allem bei den vielen Klein- und Mittelbetrieben in Österreich - hat die DSGVO jedoch zu blanker Panik geführt. Die hohen Strafdrohungen gepaart mit unpräzisen Formulierungen trieben und treiben viele an den Rand der Verzweiflung. Besonders Gruppen, die bisher kaum mit digitaler Datenverarbeitung zu tun hatten - wie Vereine und handwerkliche Betriebe - waren und sind damit überfordert.

Einer der größten Kritikpunkte an der DSGVO ist der große Interpretationsspielraum. Ohne juristische und auch technische Fachkenntnisse ist eine Umsetzung des Gesetzestextes in die Praxis kaum möglich. Unternehmen suchten aus Angst vor den drakonischen Strafdrohungen die Hilfe von Beratern und Juristen, die jedoch auch wenig Klarheit und vor allem keine Sicherheit schaffen konnten. Diese Unsicherheit führte oftmals zu überschießenden Reaktionen, was wohl jeder von uns kurz vor dem Inkrafttreten der DSGVO anhand der vielen Newsletter-Bestätigungsaufforderungen in seinem Posteingang zu spüren bekommen hat.

Die Digital Society begrüßt einerseits in vollem Umfang die neuen Rechte für die Betroffenen, die die DSGVO bringt. Gleichzeitig fordern wir aber auch, dass es mehr Rechtssicherheit für Unternehmen geben muss. Vor allem Kleinbetriebe wie Handwerker brauchen klare, einfache Vorgaben, wie sie die DSGVO in der Praxis mit geringem Aufwand einhalten können und nicht Gefahr laufen, von den Strafen der DSGVO getroffen zu werden.

Leider wurde in Österreich vom Gesetzgeber die Zeit nicht genutzt, durch das Datenschutz-Anpassungsgesetz ein wenig mehr Klarheit in die Thematik zu bringen. Das Gesetz wurde beschlossen, ohne die Begutachtungsfrist abzuwarten. Später wurde versucht dieses Versäumnis durch das Datenschutz-Deregulierungsgesetz zu reparieren, das aber nicht mehr Klarheit brachte, sondern nur die Aufforderung an die Datenschutzbehörde, mehr aufzuklären und zu verwarnen und weniger zu strafen. Es braucht aber keine Regelung für „Verwarnung statt Strafen“, sondern Klarheit, was ein Unternehmen genau zu tun hat.

Datensicherheit

Es gibt in Österreich genau einen einzigen Bereich, in dem die Kriminalität steigend ist, und zwar im Bereich der sogenannten „Cyberkriminalität“ und des damit verbundenen Internetbetrugs. Sicherheit spielt für den Datenschutz eine wichtige Rolle. Ohne Sicherheitsmaßnahmen gibt es keinen wirksamen Datenschutz. Aus diesem Grund ist Datensicherheit auch ein integraler Bestandteil der DSGVO. Denn ist die Sicherheit von IT-Systemen nicht gewährleistet, so sind auch die in ihnen gespeicherten personenbezogenen Daten nicht vor unbefugtem Zugriff geschützt.

Das ist leichter gesagt als getan. Datensicherheit betrifft ja nicht nur Daten in gut geschützten Rechenzentren, sondern mittlerweile auch Alltagsgegenstände. Das „Internet der Dinge“ verwandelt fast jede technische Gerätschaft in eine potentielle Gefahrenquelle. Denken Sie an Autos, die schon lange voll digital gesteuert werden. Es gab schon mehrmals Fälle, wo in Autos aus der Ferne digital eingebrochen werden konnten und nicht nur Daten abgegriffen, sondern auch aktiv in die Funktionen eingegriffen wurde. Wie lustig es ist, wenn mitten in der Fahrt plötzlich nichts mehr funktioniert und man das Auto nur mehr ausrollen lassen kann, können Sie sich vorstellen. Wir haben in Österreich zwar unsere §57a-Begutachtung, das Pickerl. Aber dort wird nur geprüft ob die Bremsen in Ordnung sind, aber nicht, ob es in der Bremssoftware eine Schwachstelle gibt.

Oder nehmen Sie intelligente Lautsprecher, die immer beliebter werden, mit denen wir auf einfache Art mit Geräten in unserem Haushalt kommunizieren können, die aber auch dauernd zuhören, was wir sagen. Solche Umgebungen können uns das Leben tatsächlich erleichtern und werden uns in Zukunft im Pflegebereich länger ein selbstbestimmtes Leben bieten können (Stichwort *Ambient Assisted Living*). Aber wir müssen uns auch hier Gedanken über die Sicherheit dieser Systeme machen, und zwar sowohl aus Datenschutzsicht wie auch hinsichtlich der Sicherheitsaspekte.

Diese Thematik zieht sich durch viele Bereiche. Gerade werden überall Smartmeter von den Energieversorgern installiert, die Daten über unser Verhalten sammeln und uns den Strom abdrehen können. Kraftwerksteuerungsanlagen sind teilweise auch über das Internet erreichbar und damit potentiell steuerbar. Und natürlich sind auch unsere Telekommunikationsnetze potentiell verwundbar. Wie verwundbar digitalisierte Nationen geworden sind wurde erst vor kurzem in der Ukraine vor Augen geführt, wo Hacker einen flächendeckenden Stromausfall verursachten.

Datensicherheit betrifft also nicht nur unsere persönlichen Daten, sondern auch den Kern unseres „digitalen Lebens“, unsere digitale Infrastruktur. Für die Zukunft wird es immens wichtig, dass Geräte, die über das Internet erreichbar sind, bereits per Design sicher sind, indem sie sichere Voreinstellungen aufweisen *(Security by Design, Security by Default)*. Derzeit werden Sicherheitsmechanismen – wenn überhaupt - oft erst nach der Fertigstellung eines Produkts hinzugefügt, quasi aufgepfropft, da Sicherheit in der Entwicklung natürlich Geld kostet und nur als notwendiges Übel gesehen wird. Genau hier muss die Politik ansetzen und diese Prinzipien einfordern. Und sie muss das ohne Wenn und Aber tun. Sicherheitslücken für einen Bundestrojaner offenzuhalten, gefährdet die Allgemeinheit und verschlechtert die Sicherheitslage, anstatt sie zu erhöhen. Ohne Sicherheit riskieren wir unsere Daten – aber auch Menschenleben.

Über die Digital Society

Die Digital Society ist eine gemeinnützige, parteiunabhängige NGO, die es sich zum Ziel gesetzt hat die digitale Welt zu verbessern und durch aktive Gestaltung der Zukunft bei der Digitalen Transformation zu helfen. *Unsere Vision* **ist eine freie digitale Welt, von der alle Mitglieder unserer Gesellschaft profitieren.**