Datenschutz – was bedeutet das für Unternehmen?

Jeden Tag hinterlassen wir massenweise Daten im Internet – bewusst, mehrheitlich aber unbewusst. Daraus lassen sich sehr viele Schlüsse ziehen, manchmal auch falsche. Die Schweiz passt ihr Datenschutzgesetz an und dieses soll diese Daten vor Missbrauch schützen. Doch was ist Datenschutz genau? Wir bringen etwas Licht ins Dunkel.

>> *Milena Thalmann | White Rabbit Communications*

Der Mensch generiert pro Tag etwa 2,5 Quintillionen Bytes an Daten im Internet. Je nach Verhalten und nach Vorsicht des Nutzers zentrieren sich diese Daten stärker oder verteilen sich an mehreren Orten. Manche erkennen wir direkt als persönlich und schützenswert, andere sind es vielleicht erst auf den zweiten Blick. Kumuliert, ergeben sie ein sehr genaues Bild einer Person. Man nennt diese Person den «digitalen Zwilling».

Unser Zwilling bietet eine sehr präzise Dokumentation unserer Vorlieben, unseres Verhaltens und unserer Schwachpunkte. Dadurch sind sie sehr wertvoll für Betrachter aller Art. Oft genannte Beispiele sind: Versicherungen, Werbetreibende oder politische Akteure. Weniger bekannt sind die Algorithmen von Sozialen Plattformen, die grosszügig auf unsere Daten zugreifen und diese weiterverwerten.

Was sind das eigentlich für Daten?

Neben den Daten, die wir ganz offensichtlich erzeugen, fallen bei jeder Bewegung im Internet auch eine sehr grosse Anzahl an Meta-Daten an. Diese Daten beschreiben den Umstand einer digitalen Handlung, sprich zum Beispiel die Standortdaten, die Art des Gerätes, der genutzten Software und die zeitlichen Zusammenhänge. Daraus bilden sich Verhaltensmuster, die uns nicht nur transparent, sondern auch vorhersehbar machen.

Wenn ein Anbieter weiss, dass ich oft nach veganen Gerichten suche und eines meiner Geräte Sportdaten synchronisiert, er sieht, dass ich oft von 19 – 20 Uhr surfe und mir Instagram-Reels ansehe, dann weiss der Anbieter, wann und wo er mir Nahrungsergänzungsmittel anbieten und welchen Kontext er mir dazu geben muss. Meine Bereitschaft, etwas zu kaufen, ist initiiert, da die Information auf mich abgestimmt wurde – unabhängig vom Bedarf.

Diese Vorhersehbarkeit macht uns aber nicht nur anfällig auf Werbung oder unsere Meinungsbildung. Sie greift mitunter auch in unsere Privatsphäre ein. Dr. Silvia Knittl, Director bei PWC Deutschland stellt in einem ihrer Vorträge ganz pointiert die Frage «What, if your Digital Twin misbehaves?» – was wäre, wenn wir nicht mehr ganz so eng in Kontakt wären mit unserem digitalen Zwilling und sein Verhalten nicht ausreichend beobachten könnten?

Ein spannendes Beispiel dafür ist eine Studie, die das Google-Verhalten eines anonymen Datensatzes analysiert hat und basierend darauf antizipiert hat, welches Bild bzw. welchen digitalen Zwilling Google von der Person wahrscheinlich hat. Neben einiger wahrer Rückschlüsse wie Geschlecht und Beruf, kamen auch dramatisch falsche Bilder heraus. Während die Userin begleitend zu einem Buch Themen in Zusammenhang mit Drogenkonsum recherchierte, kam Google zum Schluss, dass sie wahrscheinlich selbst einer Abhängigkeit unterliege.

Missbrauch als Gefahr

Bei Missbrauch dieser falschen «Information» können die Folgen drastisch sein. Neben den Daten, die Internetplattformen von uns sammeln, kommen Daten dazu, die Unternehmen von uns halten und die bei Angriffen kopiert, entwendet und weitergegeben werden. Databreaches sind kein einmaliges Problem, sie kumulieren sich zu einer Bedrohung, die jeden individuell angreifbar macht. Dabei gibt es fast keine harmlosen Daten, die gestohlen werden können, aber es gibt sehr kritische Daten, die jeder Mensch bewusst schützen sollte, so wie Gesundheitsdaten, Verhaltensdaten, biometrische Daten...

Basierend auf diesen neu entstandenen Abhängigkeiten zwischen Menschen, Daten und Anbietern entstehen nun neue Gesetze, die unsere Daten besser schützen sollen und unsere Exponierung auf ein gesünderes Niveau senken wollen.

Daten sollen also so isoliert wie möglich gehalten werden und einem Zweck zugewiesen werden, ohne von diesem abzuweichen, so dass der Erzeuger der Information in der Kontrolle bleiben kann. Folglich sind alle Unternehmen, die personenbezogene Daten speichern, verarbeiten und versenden, angehalten, sich um die Sicherung, den sicheren Transport und die verantwortungsvolle Verbreitung zu kümmern – damit keiner einen falschen Nutzen aus diesen ziehen kann. Neben der bekannten DSGVO (DatenSchutzGrundVerOrdnung) in der EU tritt per September 2023 auch in der Schweiz die reformierte Datenschutzverordnung in Kraft.

Brennende Fragen – spannende Antworten

Wir haben uns mit vier Fachpersonen über diverse Aspekte des Datenschutzes unterhalten.

Das Interview führten wir mit:

- **Sabine Fercher (SF)** ist Anwältin und Gründerin von Fercher Compliance LLC
- **Johannes Troppmann (JT)** ist Managing Director & GRC Pionier bei IS4IT Schweiz AG
- **Slobodan Mikulovic (SM)** ist Datenschutzbeauftragter sowie Geldwäschebeauftragter bei der DATA Security AG
- **Philipp Bachmann (PB)** ist COO, Sales & Channel Manager sowie Mitglied der Geschäftsleitung bei der SEPPmail AG

1 In Ihren eigenen Worten: Was schützt der Datenschutz genau?

SF: Der Mensch als selbstbestimmtes Individuum mit seiner eigenen Persönlichkeit wird geschützt, wie wenn er Kleider tragen dürfte und sich nicht ständig nackt betrachten lassen müsste. Seine psychische Integrität soll so verpackt sein, dass diese nicht Manipulationen ausgesetzt ist.

JT: Der Datenschutz schützt den Menschen und nicht das Unternehmen. Das ist das Erste was Unternehmen immer falsch verstehen. Als Datenschutzbeauftragter sage ich immer «Wir schützen keine Unternehmensdaten, sondern Daten von Menschen, die wir irgendwie erhalten haben, da wir ethisch und per Gesetz dazu verpflichtet sind.»

SM: Der Datenschutz regelt den Umgang mit Daten und soll sicherstellen, dass nur befugte Personen Daten für bestimmte Zwecke verarbeiten dürfen.

PB: Der Datenschutz schützt das Individuum. Das Gesetz räumt uns ein Recht ein, dass wir dringend brauchen, um weniger Manipulation und mehr Transparenz im digitalen Raum zu erhalten.

Sabine Fercher:

«Unternehmen könnten in der Isolation landen.»

2 Welche Unterschiede erfahren Unternehmen, die bereits in einem regulierten Umfeld sind, gegenüber jenen, die keinen Standardregularien unterliegen?

SF: Je nach Unternehmen und Umfeld, ist es klar ein Wettbewerbsvorteil, Standardregularien zu unterliegen. Das streng regulierte Umfeld achtet bereits bei der Erarbeitung von technischen Lösungen auf «Privacy by Design» und «Privacy by Default» und erlaubt einen einfacheren Marktzugang in ein unterreguliertes Umfeld. Je mehr das Verständnis für den Datenschutz wächst, umso schwieriger wird es, datenschutzrechtlich mangelhafte technische Lösungen zu vermarkten.

JT: Das hängt davon ab, wie weit sie das Thema Datenschutz bzw. Datensicherheit bis dato ernst genommen und umgesetzt haben. Denn für Unternehmen, welche sich dem Thema angenommen haben, ändert sich gar nichts. Für diejenigen, welche das Thema stiefmütterlich behandeln haben, ändert sich das Risikopotenzial.

3 Wie aufwendig ist die Umsetzung eines Datenschutz-Prozesses?

PB: Die Umsetzung von Datenschutz-Prozessen nimmt einige Monate in Anspruch. Natürlich kann man davon ausgehen, dass ein wenig digitalisiertes mittelständisches Unternehmen etwas weniger Aufwand hat als ein Grossbetrieb. Wobei viele grosse Unternehmen die «Privacy-by-Design»-Ansprüche schon länger in ihre Prozesse eingebaut haben, während der Mittelstand bisher oft weggeschaut hat.

SF: Die Umsetzung des Datenschutzes ist auch ein prinzipienbasiertes Unternehmenskulturthema und eine nicht endende Aufgabe. Das Managen vom Datenschutz basiert auf Pfeilern, die je in einzelnen Prozessen eingeführt werden:
1) Datenschutzerklärung, womit erhoben und publiziert werden muss, wofür Personendaten genutzt werden.
2) Inventar, womit ein Verständnis für den Standort der Daten evaluiert wird.
3) Vertragsmanagement und Klärung der Rollenzuteilung, mit der Unterstützung von vielen Mustern, der Auditrechte, aber auch Notifikation unter den Parteien.
4) Krisenmanagement inklusive Zuteilung der Verantwortlichkeiten bei möglichen Vorfällen und Sicherstellung der Notifikation von Behörden – gegebenenfalls auch der Betroffenen.

SM: Das hängt oft auch noch davon ab, welche Hilfsmitteln zum Einsatz kommen. Wer mit einem erfahrenen Datenschützer zusammenarbeitet und einen strukturierten Schutzprozess mit Softwareunterstützung startet, schafft sich ressourcenseitig sicher einen massiven Zeitvorsprung.

4 Sind nur Daten betroffen, die das jeweilige Unternehmen selbst bearbeitet?

SF: Der Datenschutz kennt die Rolle des Betroffenen, des Verantwortlichen und des Verarbeiters. Der Verantwortliche, vereinfacht derjenige, dem die betroffene Person die Daten zuerst anvertraut, ist verantwortlich. Er muss alle Betroffenen informieren, was er mit den Daten macht und eine Einwilligung einholen, wenn er Daten an Verarbeiter – insbesondere in nicht anerkannte Drittländer – übertragen will. Ein tunesischer IT-Support mit Zugriffsrechten für Laptops in Deutschland bearbeitet Daten, sobald er auf dem Laptop Personennamen sehen könnte. Die betroffene Person muss vom Verantwortlichen informiert sein und der Verantwortliche muss vom Verarbeiter – dem IT Supporter – das vertraglich abgesicherte Zugeständnis haben, dass dieser sich an EU-Datenschutzvorschriften hält. Der Verantwortliche muss dies auch prüfen und den Verarbeiter auditieren.

JT: Es gibt zwei massgebliche Rollen, welche auch namentlich aus der DSGVO übernommen wurden: Den «Verantwortlichen» und den «Auftragsverarbeiter», sprich die Daten welche ein Verantwortlicher (z. B. eine Bank) einem «Auftragsverarbeiter» (z. B. einem IT-Haus oder einer Marketingfirma) zum Verarbeiten der personenbezogenen Daten übergibt. Interessant ist: entgegen der DSGVO haften aber nach dem neuen DSG «alle Mitwirkenden», wobei nach der DSGVO die Auftragsverarbeiter nur beschränkt haften.

Johannes Troppmann:

«Datenschutz ist das fundamentale Grundrecht jedes Menschen auf individuelle Selbstbestimmung.»

5 Mit welchen Folgen müssen Unternehmen rechnen, die den Datenschutz nicht priorisieren?

JT: Entgegen der Vorgehensweise in der EU sind im neuen DSG der Schweiz ausschliesslich natürliche Personen haftbar und keine juristischen.

Somit muss das Unternehmen (ausser dem Aufbau des Datenschutzkonzeptes als Auflage) per se mit keinen «Folgen» rechnen, dafür die verantwortlichen Personen. Wer dies nun genau ist, ist noch nicht klar, aber ich rechne damit, dass die Geschäftsführung und der Verwaltungsrat an erster Stelle stehen.

Fortsetzung Interview auf Seite 12

SF: Unternehmen ohne Priorisierung vom Datenschutz gleiten ins Abseits wegen mangelnder Wettbewerbsfähigkeit. Weiter führt es zur Isolation, weil das Unternehmen für potenzielle Geschäftspartner ein zu grosses Risiko darstellt. Bei Verletzung des Datenschutzes kann es existentiell werden. Innerhalb der EU werden die Unternehmen bestraft, in der Schweiz das Individuum. Die «kleine» Schweizer Busse von bis zu CHF 120'000 pro Fall – ab September 2023 – könnte demnach sehr wohl Wirkung entfalten. Gemäss enforcementtracker.com sind bis August 2022 1,6 Milliarden Euro Bussgelder bei 1214 Fällen erhoben worden. Amazon, WhatsApp, Google und Facebook waren 2021 die höchstgebüssten Unternehmen.

PB: Das Bewusstsein der Nutzer steigt und die Rechte sind nun deutlich formuliert. Daher werden Unternehmen ohne aktiven Datenschutz Mühe haben, Kunden zu finden. Wir haben in der Vergangenheit erlebt, wie der Missbrauch von personenbezogenen Daten zu einer Verzerrung unserer «echten» Welt geführt hat. Nun wird es Zeit, dies zu stoppen.

Slobodan Mikulovic:

«Keine Angst vor dem Datenschutz.»

Philipp Bachmann:

«Das Bewusstsein der Nutzer steigt.»

6 Welche Tricks gibt es, um Datenschutz schnell einzuführen?

JT: Keine. Es braucht eine gewisse Grunddokumentation und die Einführung der Prozesse, welche dann durch Schulungen auch von den Mitarbeitern gelebt werden müssen.

Es ist sinnvoll, hier pragmatisch zu bleiben und keine 100-Seiten-Abhandlungen mit juristischen Details zu jeder Richtlinie zu verfassen. Aber der «Datenschutzberater» (so wird die Rolle neu heissen) wird die Verantwortlichen im Unternehmen beraten, was sie tun und lassen sollten und die Umsetzung der Massnahmen prüfen.

SF: Verwaltungsratsbeschluss, Risikoevaluation und top-down abgesegneter Projektplan sind der Start. Ein geübter Projektmanager erkennt die zahlreichen Stakeholder und bindet diese gemäss RACI (responsible, accountable, consulted, informed) korrekt ein. Klar wird oft in der Praxis nur das sogenannte «window dressing» gemacht. Hierzu dient der Webauftritt mit der Datenschutzerklärung und der Angabe der verantwortlichen Person für Datenschutzthemen.

SM: Ich kenne einen Super-Trick: keine Angst haben vor dem Datenschutz. Denn im Grossen und Ganzen ist es, wie bereits von allen Parteien hier erwähnt, ein Wettbewerbsvorteil, ein Kundenversprechen und eine Strategie für eine verantwortungsvolle Zukunft. Also ein Teil jedes Unternehmensfundaments. In ein paar Jahren fragt niemand mehr «Macht ihr Datenschutz?», so wie heute niemand fragt «Macht ihr Buchhaltung?».

7 Werden die neuen Gesetze helfen, dass auch die User selbst mehr auf den Schutz ihrer Daten achten?

SM: Ja, ich gehe davon aus, dass aufgrund der Bekanntgabe und daraus resultierender Kommunikation die Sensibilisierung aller steigen wird. Das haben wir in Deutschland erlebt und in der Schweiz wird es auch bald so sein.

SF: In der Schweiz wird mit dem Fokus auf die Individualbestrafung und der Einführung eines neuen Berufsgeheimnisses, das für alle gilt, ein Umdenken stattfinden. Spätestens wenn die ersten Fälle strafrechtlich verfolgt werden. Dies obliegt den kantonalen Behörden. Es bleibt abzuwarten, welche Kantone Vorreiter werden. Eine einheitliche Anwendung ist schweizweit kaum denkbar.

JT: Nein. Gesetze sind das letzte Mittel und es ist traurig, dass es so weit kommen musste, um den Datenschutz zu «erzwingen». Aber dieser verpflichtet Menschen und Unternehmen, personenbezogene Daten von Dritten zu schützen und nicht seine eigenen.

Es wäre wünschenswert, dass die Menschen auch eine Schlussfolgerung für sich selbst daraus ziehen würden, aber dafür ist noch sehr viel Sensibilisierungsarbeit notwendig, um dieses kognitiv zu verankern. Denn die Digitale Welt – vor allem Soziale Medien – fördern genau das Gegenteil.

PB: Es bleibt zu hoffen. Denn letztlich gibt es ja so einiges zu schützen, wenn man sich mal ansieht, wie intensiv wir digitale Dienste nutzen und welche Spuren wir dabei hinterlassen.

Fazit

Wie so viele Massnahmen, die im Zusammenhang mit Cyber Sicherheit stehen, ist auch der Datenschutz ein Thema welches «Change» in Firmen fordert. Es sind nicht nur die IT Prozesse betroffen, sondern auch die Menschen, die sich ihrer Verantwortung bewusst werden müssen und die Firmenkultur, die es zulassen muss verantwortungsvoll zu handeln. Datenschutz ist Compliance, Führung und Kundenversprechen in einem. Es sind aber auch alle Nutzer gefragt, ihre Rechte einzufordern. <<

Die Autorin

Milena Thalmann ist Marketing- und Kommunikationsexpertin für die IT-Branche. 2020 gründete sie zusammen mit ihrem Geschäftspartner die Agentur White Rabbit Communications. Durch diverse Engagements in ihrer Laufbahn, unter anderem für die Swiss Cyber Security Days oder Dreamlab Technologies, verfügt sie über solide Einblicke in die IT Sicherheitsbranche.

www.whiterabbitcom.ch