Wer Daten nicht schützt, wird hart bestraft

Gesetz Wie eine neue EU-Verordnung uns alle stärken und absichern soll – Viele Fallstricke

Von unserem Mitarbeiter
Reinhard Kallenbach

■ **Koblenz/Region.** Mehr Rechte für Verbraucher und Geschäftskunden rund um sensible analoge und digitale Daten, zahlreiche Fallstricke für Unternehmen – dazu potenziell hohe Strafen selbst für kleine Betriebe: So in etwa lässt sich die Bandbreite der neuen Datenschutz-Grundverordnung (DSGVO) beschreiben, die am 25. Mai nach einer zweijährigen Übergangsphase nun endgültig scharf geschaltet wird. Der Bundesverband Mittelständische Wirtschaft (BVMW) appelliert an Inhaber und Geschäftsführer, sich schnellstmöglich um das Thema zu kümmern.

Existenzbedrohende Folgen

„Bis zu 20 Millionen Euro, im Extremfall bis zu 4 Prozent des Jahresumsatzes: So hoch können die Strafen sein", warnt Sarah Hennemann und rechnet vor: Zum Beispiel könnte das Bußgeld für ein Unternehmen mit einem Jahresumsatz von 800 Millionen bis zu 32 Millionen Euro betragen. Aber auch für kleine Unternehmen kann es richtig teuer werden. „Betroffenen Betrieben droht also leicht das Aus", so die Leiterin des Kreisverbands Mittelrhein des BVMW weiter. Ein Entrinnen gibt es nicht, denn die Grundverordnung wurde bereits am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht. Aus rechtlicher Sicht hatten also alle genug Zeit.

Die DSGVO ist, weil sie eine Verordnung und keine Richtlinie ist, von dem Weg durch die nationalen Parlamente der EU-Staaten ausgenommen, sie gilt direkt und unmittelbar. Sie ist ein Gesetz, das für jeden gilt, der mit personenbezogenen Daten arbeitet – also auch Privatpersonen, die über interaktive Elemente in ihrem eigenen Netzauftritt mit anderen kommunizieren, zum Beispiel dann, wenn sie einen kleinen Shop eingebaut haben. Bei einem Verstoß dürften sich die finanziellen Folgen für Privatpersonen in engen Grenzen halten. Ganz anders sieht es für Betriebe oder Freiberufler aus.

Aus Sicht des BVMW droht jetzt die Gefahr, dass sich berüchtigte Wettbewerbsvereine bewusst kleinere Betriebe vornehmen – also genau die Unternehmen, die keine eigene Verwaltung oder eine spezialisierte IT-Abteilung haben. „Im Zweifelsfall sollten sich die Inhaber nicht scheuen, einen Juristen und einen entsprechend qualifizierten IT-Spezialisten hinzuzuziehen. Unter dem Strich ist das immer noch deutlich billiger als eine Strafe", ergänzt Michael Plies, der beim BVMW unter anderem Ansprechpartner rund um das Thema Informationstechnologie (IT) ist.

Dabei ist die DSGVO keine Brüsseler Schikane für den Mittelstand. Kerngedanke ist vielmehr, Verbraucher besser zu schützen. „Es geht um das Recht auf informationelle Selbstbestimmung. Jeder Mensch soll grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen", erklärt Thomas Haschert, Fachanwalt für Arbeitsrecht und Datenschutzbeauftragter in der Kanzlei „Martini Mogg Vogt". Dabei geht es nicht nur um Name, Adresse und Geburtsjahr. „Es kommt sogar vor, das Wohn- und Vermögensverhältnisse, Angaben über das Privatleben und persönliche Einstellungen sowie Gehalt und Kreditkartennummer gespeichert oder weitergegeben wurden, ohne dass Betroffene etwas davon gewusst haben", ergänzt Kevin Müller, der als Fachanwalt für Urheber- und Medienrecht ebenfalls in der Koblenzer Kanzlei tätig ist.

Keine Ausreden mehr

Gegen diese grenzüberschreitende Praxis waren Verbraucher über nationale Datenschutzgesetze unzureichend geschützt, das DSGVO sorgt jetzt für einen „Deckel". Denn jeder, der Produkte oder Dienstleistungen in der Europäischen Union anbietet, ist dem EU-Recht unterworfen. Man kann sich also nicht mit den eigenen Geschäftsbedingungen und einem Gerichtsstand außerhalb der EU herausreden. Auch das Recht von Betroffenen, „im Netz vergessen zu werden", wird durch die Verordnung gesetzlich geregelt. Allerdings hat in diesem Punkt der Europäische Gerichtshof das Recht bereits mit seiner „Google-Entscheidung" am 13. Mai 2014 gestärkt. Damit wird klar: Die Grundverordnung zielt eigentlich auf die großen „Datenkraken". Giganten wie Google und Facebook werden also nicht geschont. Im Gegenteil. Im Zuge der Gleichbehandlung können kleine Anbieter im Netz jedoch nicht auf Gnade hoffen.

Informationspflicht verschärft

Auf die erheblich gestiegenen Informationspflichten verweist Elmar Kloss: „Wo früher keine Information des Betroffenen notwendig war, weil sich Art, Umfang und Zweck der Datenverarbeitung aus der Situation ergab, verlangt das neue Recht stets eine ausdrückliche und umfassende Information. Durch die neuen Informationspflichten soll das Zweckbindungsprinzip stärker betont werden, und Unternehmen müssen sich vorab Gedanken über Rechtsgrundlagen und Speicherfristen machen", erklärt der Fachanwalt für IT-Recht in der Kanzlei Dr. Caspers, Mock & Partner. Er ergänzt, dass „selbst datenschutzkonform arbeitenden Unternehmen ein Bußgeld droht, wenn nicht vorab eine rechtskonforme Dokumentation zum Nachweis der Rechtmäßigkeit der Datenverarbeitung erstellt wurde." Und Dirk Lindloff, der in der gleichen Kanzlei unter anderem als Fachanwalt für IT- und Datenschutzrecht tätig ist, macht deutlich, dass die Verordnung auch mit einem wesentlich erhöhten bürokratischen Aufwand verbunden ist. Und Rechtsanwalt Gabriel Litzenberger (Kanzlei Fromm) empfiehlt: Auf jeden Fall sollten Betroffene einen detaillierten Fragenkatalog aufstellen und am besten mit juristischem Beistand penibel abarbeiten.

Aber nicht nur aus rechtlicher Sicht hat die DSGVO ihre Tücken. Denn jeder, der Netzauftritte oder Datenbanken betreibt, muss seine Netzstrukturen so sichern, dass Dritte nicht so einfach illegal auf diese zugreifen und die gestohlenen Daten nutzen können – oder gar auf die Rechner der Kunden gelangen, die Verkäufer und Dienstleister eigentlich schützen sollten. Die sogenannte SSL-Verschlüsselung ist somit Pflicht (SSL ist das Kürzel für Secure Socket Layer). Diese „sichere Sockelschicht" sorgt dafür, dass sensible Daten verschlüsselt übertragen werden. Dass dies der Fall ist, können auch Laien erkennen – und zwar an der kleinen Darstellung eines Hängeschlosses in der Adresszeile. „Die meisten Unternehmen haben die Übergangsfrist genutzt, ihre Präsenzen im Netz entsprechend umzustellen. Wer das noch nicht gemacht hat, sollte das möglichst sofort angehen", erklärt Immanuel Bär, Mitgründer des Polcher IT-Sicherheitsunternehmens ProSec.

Klassische Missbrauchfälle

Ein klassischer Fall für Datenmissbrauch ist der allzu sorglose Umgang mit Daten und Fotos in allen Medienkanälen. Da kann es schnell passieren, dass einmal freigegebenes Material einfach weiterverwendet wird, ohne dass die Betroffenen informiert werden – beispielsweise wenn sich ein Gast, der bei einer Hausmesse fotografiert wird, ohne seine Einwilligung in einer Produktwerbung wiederfindet. Auf ein alltägliches Beispiel hatte Thomas Kehr, Anwalt bei Dornbach, bereits zu Beginn der Übergangsfrist hingewiesen (die RZ berichtete): Wenn Kunden, obwohl sie widersprochen haben, weiterhin mit E-Mails oder Werbepost „zugeschüttet" werden, kann dieses Versäumnis schnell ein Fall für die Datenschutzbeauftragen der Länder werden. Die Beweislast liegt nicht beim Verbraucher, sondern beim Unternehmen.

Ein weiteres Beispiel sind Akquiselisten, über die Firmen lange potenzielle Kunden angesprochen haben, obwohl keine Zustimmung der Kunden für die Verwendung sensibler Daten vorlag. Dieser Praxis hat bereits das Bundesdatenschutzgesetz einen Riegel vorgeschoben. Das zeigt: Schon in der Zeit vor dem DSGVO waren hohe Geldstrafen möglich.

Kleinbetriebe als Hauptziel

Die Hauptgefahr ist jedoch das Netz: Hacker nehmen immer öfter auch Seiten kleinerer Betreiber ins Visier. Sie steuern Schwachpunkte wie semiprofessionelle Shopsysteme an. „Das Schlimme ist, dass der Geschädigte nicht nur einen zerstörten Auftritt hat, sondern auch noch in Regress genommen werden kann, weil er Daten nicht ausreichend geschützt hat", warnt Michael Vogelbacher. Der Fachanwalt von der Kanzlei Advokat pro in Oberhonnefeld ergänzt: „Einen internen oder externen Datenschutzbeauftragten müssen Unternehmen immer dann bestellen, wenn sie mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Rhein-Zeitung Koblenz
vom 01.03.2018