Datenschutz: Hohe Bussgelder und Unsicherheit

Seit die neue europäische Datenschutzverordnung GDPR vor zwei Jahren in Kraft trat, wurden bereits mehrere hundert Verstösse mit Bussgeldern geahndet. Wobei der bisherige Rekord bei einer Summe von rund 200 Millionen Euro liegt. Schweizer KMU sind nach wie vor verunsichert.

Ein deutscher LKW-Fahrer musste 200 Euro Busse zahlen, weil er Dash-Cam-Aufnahmen im Internet veröffentlichte. British Airways wird voraussichtlich rund 200 Millionen Euro auf Grund schlechter IT-Sicherheits-Vorkehrungen bezahlen müssen. Fälle von GDPR-Verstössen welche mit Bussgelder geahndet werden häufen sich. Über 200 Fälle sind öffentlich bekannt. Die Tatsache, dass bis Anfang des Jahres 160'000 Verstösse angezeigt wurden und die Bescheide nicht öffentlich gemacht werden müssen, lässt auf wesentlich mehr Bussen schliessen und zeigt, dass die neuen Datenschutzvorgaben der EU ernst genommen werden.

Während internationale Grossfirmen dank grosser Rechtsabteilung, Anwälten und Beratern meist entsprechende GDPR-Projekte ins Leben gerufen und die notwendigen Massnahmen grösstenteils bereits umgesetzt haben, sind etliche Schweizer KMU nach wie vor verunsichert. Dass die Revision des Schweizer Datenschutzgesetzes bald drei Jahre nach der Präsentation des ersten Entwurfs immer noch nicht abgeschlossen ist und dadurch die EU-Datenschutzäquivalenz gefährdet ist, erhöht diese Unsicherheit noch.

Was für Schweizer KMU gilt und welche Verstösse zu den meisten Bussen führen, wird im Folgenden kurz erläutert.

Die Situation für Schweizer KMU – Schweizer Unternehmen, die eine Niederlassung in der EU haben, mit Personen im EU-Raum Geschäfte machen oder deren Verhalten beobachten (Profiling), betrifft die GDPR (EU-DSGVO) direkt. Sie müssen sich an die Vorgaben halten – und dementsprechend können auch Verstösse angezeigt und Bussen gesprochen werden. Unternehmen, für welche die EU-Regulierung nicht relevant ist, sollten sich bewusst machen, dass die kommende Revision des Schweizer Datenschutzgesetztes inhaltlich keine grossen Abweichungen von der europäischen Regulierung haben wird und ein in Kraft treten für 2021 realistisch scheint. Demnach ist für alle Schweizer Firmen, welche die Anforderungen noch nicht erfüllen, Handlungsbedarf angezeigt.

IT-Sicherheit nicht im Griff – Die bisher potenziell grössten GDPR-Bussgelder betreffen British Airways (183 Mio britische Pfund) und die Hotelkette Marriott International (99 Mio britische Pfund). Beide Bussen sind noch nicht abschliessend festgelegt und betreffen Verstösse gegen Art. 32 GDPR. In beiden Fällen geht es darum, dass Hacker grosse Mengen an persönlichen Daten stehlen konnten und nachfolgende Untersuchungen Versäumnisse im Bereich der IT-Sicherheit aufgezeigt haben. Nun ist es jedoch nicht so, dass der erwähnte Artikel eine Liste der erforderlichen IT-Sicherheitsmassnahmen enthält. Vielmehr werden *«geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten»* unter *«Berücksichtigung des Stands der Technik (…)»* gefordert. Was dies bedeutet, ist Interpretationssache.

Inwiefern getroffene Massnahmen ausreichend sind, lässt sich gerade im KMU-Bereich oft nur im Einzelfall beantworten. Dabei muss neben dem Stand der Technik und dem jeweiligen Risiko auch die Wirtschaftlichkeit der Massnahmen berücksichtigt werden. Wer aber besonders grundlegende Sicherheitsmassnahmen, wie Softwareaktualisierungen, Virenschutz, Zugriffskontrollen oder die Netzwerksicherheit vernachlässigt, dürfte klar gegen die gesetzlichen Vorgaben verstossen.

Fehlende rechtliche Grundlage für die Datenverarbeitung
Unter welchen Umständen und in welchem Mass persönliche Daten verarbeitet werden dürfen, ist in der europäischen Verordnung klar geregelt. Neben Google musste sich diesbezüglich auch bereits die österreichische Post verantworten, welche Daten zu Parteiaffinitäten von mehr als drei Millionen Österreichern sammelte. Vereinfacht gilt: Hat das Datensubjekt der Datenverarbeitung explizit zugestimmt oder ist diese für die Erfüllung eines Vertrages mit dieser Person zwingend notwendig, so ist kein Verstoss zu befürchten.

Nichteinhaltung allgemeiner Grundsätze – Auch bei Verstössen gegen die allgemeinen Grundsätze der Datenverarbeitung wurden bereits Bussen gesprochen. So wurde eine deutsche Immobiliengesellschaft mit 14.5 Mio Euro gebüsst, weil sie ein Archiv-System betrieb, welches keine Möglichkeit zur Löschung nicht mehr benötigter Daten ehemaliger Mieter vorsah. Wer Daten nur für den vereinbarten Zweck nutzt und sie auch nur so lange vorhält, wie es dieser Zweck oder ein Gesetz erfordern, verhält sich konform zu den geltenden Datenschutzbestimmungen.

Der Unsicherheit begegnen – In der aktuellen Situation stehen KMUs vor der Herausforderung die aktuelle Rechtslage und deren Bedeutung für die eigene Geschäftstätigkeit zu verstehen, sowie die die richtigen Schlüsse in Bezug auf notwendige Massnahmen zu ziehen. Für Unternehmen, welche sich einen Überblick zur aktuellen Datenschutzsituation und deren Implikationen verschaffen wollen, bietet ensec zusammen mit den Rechtsberatern von LEXR (lexr.ch) drei Pakete zu attraktiven Fixpreisen an.