Bild iStockphoto/maginima

Neues Datenschutzgesetz – welche Massnahmen müssen Unternehmen jetzt ergreifen?

Am 1. September trat das neue schweizerische Datenschutzgesetz in Kraft. Dieses bringt Veränderungen für Firmen aller Branchen und Grössen mit sich. Wer sich noch nicht mit der Thematik auseinandergesetzt hat, sollte sich sputen. Worauf man besonders achten sollte, fragte «Fokus» bei David Schwaninger nach, Rechtsanwalt und Partner bei der Blum & Grob Rechtsanwälte AG.

David Schwaninger
Rechtsanwalt & Partner bei Blum & Grob Rechtsanwälte AG

Ab sofort gilt es ernst: Seit dem 1. September 2023 sind Unternehmen in der Schweiz angehalten, den Vorschriften des neuen Datenschutzgesetzes nachzukommen. Gemäss Einschätzungen von Fachleuten könne man davon ausgehen, dass sich ein Grossteil der Unternehmen noch nicht mit der neuen Gesetzgebung auseinandergesetzt hat – und viele Betriebe dementsprechend nicht wissen, welche neuen Regeln sich daraus für sie ergeben. «Diesen Unternehmen kann man nur raten, dass sie jetzt schnellstmöglich die essenziellsten ‹Quick Fixes› umsetzen, um die Compliance zur neuen Gesetzgebung sicherzustellen und mögliche negative Konsequenzen zu minimieren», betont David Schwaninger. Als Rechtsanwalt und Partner bei der Blum & Grob Rechtsanwälte AG unterstützt er Firmen unterschiedlichster Branchen und Grössen in diesem Prozess.

Wie gehen Schwaninger und sein Team dafür vor? «Wir analysieren gemeinsam mit dem Kundenunternehmen, wo es hinsichtlich des Datenschutzes noch Lücken gibt – und stopfen diese», führt der Rechtsanwalt aus. Wichtig sei, dass Schweizer Firmen verstehen, wie sie aufgrund der neuen Gesetzgebung die Wahrung des Datenschutzes ihrer Kundinnen und Kunden verstärken und aktiver vorantreiben müssen. «Beispielsweise wurde eine erweiterte Informationspflicht eingeführt», erklärt Schwaninger. Diese schreibt Unternehmen unter anderem vor, dass sie betroffene Personen bei der Beschaffung von Personendaten proaktiv darüber informieren, zu welchem Zweck diese bearbeitet werden und, falls diese Daten ins Ausland gehen, wohin. Hierzu versteht der Gesetzgeber kein Pardon: «Die Verletzung der neuen Informationspflicht ist ein Straftatbestand, was auch für den Einsatz ungenügender Massnahmen für die Wahrung der Datensicherheit gilt.» Die Strafen können substanziell sein und haben vor allem für die individuelle Person im Betrieb, die für die Verfehlung verantwortlich ist, Konsequenzen. So ist etwa das Verhängen hoher Geldbussen möglich.

In der eigenen Hand

Die gute Nachricht lautet gemäss David Schwaninger aber, dass Betriebe viel selbst unternehmen können, um eine gute «Data Governance» zu etablieren. In einem ersten Schritt sei es ratsam zu analysieren, über welche Personendaten ein Betrieb verfügt, wofür diese Informationen verwendet, wo die Personendaten gespeichert sowie welche konkreten Massnahmen zur Datenschutz-Compliance ergriffen werden. Es lohnt sich, hierzu eine Bestandsaufnahme vorzunehmen und diese samt allfälligen ergriffenen Massnahmen schriftlich festzuhalten. Dies macht es zudem einfacher, betroffene Personen bei der Beschaffung über die Verwendung ihrer Personendaten zu informieren. Es sei zudem wichtig, die Regelungen mit Dienstleistern zu klären, die im Namen des eigenen Unternehmens Personendaten bearbeiten, wie beispielsweise den Erbringern von Cloud-Diensten. Denn manche dieser Anbieter können in Staaten ansässig sein, die aus Sicht des Schweizer Gesetzgebers keinen ausreichenden Datenschutz bieten. Aufgrund der Komplexität der resultierenden Fragen ist es sinnvoll, das Thema mit einem Rechtsexperten näher zu betrachten.

Akut wird die Datenschutzthematik auch im Worst Case – dann nämlich, wenn ein Unternehmen gehackt wurde. «Dass es zu einem Sicherheitsvorfall gekommen ist, man vielleicht Opfer eines Ransomware-Angriffs wurde oder Daten verloren gegangen sind, ist per se noch kein Straftatbestand», legt David Schwaninger dar. Allerdings kann ein solcher Fall unter Umständen einer Meldepflicht unterliegen, sodass eine Firma allenfalls mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und sogar mit den betroffenen Personen Kontakt aufnehmen muss. In einem solchen Fall müssen möglichst rasch die zentralen Fragen geklärt werden: Sind der EDÖB sowie Kundinnen und Kunden in Kenntnis zu setzen? Wie geht man am besten dabei vor? Und wie ist es eigentlich zum Vorfall gekommen?

In der Vergangenheit haben David Schwaninger und sein Team Firmen auch in solchen Situationen unterstützt. «Wir erbringen natürlich keinen technischen Support – obschon wir auf Wunsch den Kontakt zu den entsprechenden Fachleuten herstellen können – sondern kümmern uns um die juristischen Belange eines Cyberangriffs.» Auch bei der Krisenkommunikation können die Expertinnen und Experten von Blum&Grob wertvolle Hilfe leisten. «Wir achten darauf, dass sich unsere Klientinnen und Klienten möglichst nicht haftbar machen und sind auch zur Stelle, wenn es um Rückfragen sowie das Festlegen der weiteren Strategie geht.»

Über die Blum & Grob Rechtsanwälte AG
Blum&Grob ist eine renommierte Schweizer Wirtschaftskanzlei mit über 50 Mitarbeitenden. Das in Zürich ansässige Unternehmen zählt sowohl mittelständische als auch grosse in- und ausländische Unternehmen, Organisationen, Start-ups und Privatpersonen zu seinen Klienten und berät diese in allen Bereichen des Wirtschaftsrechts.

www.blumgrob.ch

Blum & Grob
RECHTSANWÄLTE