expertenReport

Leitfaden DSGVO – Thema: Mitarbeiter, Rechenschaftspflicht und Cyber

Um ein internes Datenschutzkonzept, die Rechenschaftspflicht, die Notwendigkeit einer Cyber-Risk-Versicherung und Schulungen der Mitarbeiter geht es im fünften Teil des DSGVO-Leitfadens von Sebastian Karch, Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft.

Internes Datenschutzkonzept erstellen

Wenn man sich als Unternehmer die Mühe macht, sich intensiv mit dem Datenschutzrecht zu befassen, müssen natürlich zwangsläufig dabei Entscheidungen getroffen werden: Welche Daten erhebe ich beispielsweise bei der Neu-Kundenakquise, um nicht zu viele Daten zu erheben („Datenminimierungsgrundsatz“) oder wann werden welche Daten gelöscht/gesperrt oder welche Mitarbeiter haben auf welche Daten wann Zugriff?

Sebastian Karch, Rechtsanwalt / Gesellschaftsrecht, Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft
Diese ganzen Entscheidungen zu durchdenken und zu dokumentieren kann dann „Datenschutzkonzept“ betitelt werden. Wichtig ist eigentlich nur, dass es auch gemacht wird.

Dazu gehört auch, dass „Privacy-by-Design“ und „Privacy-by-Default“ im Unternehmen etabliert werden. Das bedeutet nichts anderes als „Datenschutz durch Technikgestaltung“ beziehungsweise „Datenschutz durch datenschutzfreundliche Voreinstellungen“. Die technischen Voreinstellungen sollen also immer zu Gunsten des Kunden, das heißt zum Schutz seiner Daten, eingestellt sein.

Rechenschaftspflicht nachkommen

Nicht nur gegenüber den betroffenen Personen hat der Unternehmer Rechenschaft über die Datenverarbeitung abzugeben. Vor allem die Rechenschaftspflicht gegenüber den zuständigen Behörden ist nachzukommen, um Bußgelder zu vermeiden.

An dieser Stelle seien noch einmal die Maximalstrafen genannt. Wo vorher Bußgelder in Höhe von „nur“ bis zu 300.000 Euro verhängt werden durften, dürfen Behörden nun theoretisch bis zu 20 Millionen Euro beziehungsweise 4 Prozent des Jahresumsatzes bei „schweren“ Verstößen und bis zu 10 Millionen Euro beziehungsweise bis zu 2 Prozent des Jahresumsatzes bei „leichten“ Verstößen verhängen.

Als leichter Verstoß gilt zum Beispiel die Nichtbestellung eines Datenschutzbeauftragten, obwohl eine Pflicht zur Bestellung besteht. Als schwerer Verstoß kann eigentlich jede Verletzung der Grundsätze der DSGVO gewertet werden, also zum Beispiel wenn der Rechenschaftspflicht

(Art. 5 Abs. 2 DSGVO) nicht nachgekommen wird oder eine Datenverarbeitung ohne Rechtsgrundlage stattfindet. In Art. 5 DSGVO sind übrigens alle Grundsätze abschließend aufgezählt, die ausnahmslos und jederzeit zu beachten sind.

Bei der Verhängung von Bußgeldern haben die Behörden natürlich weiterhin mit Augenmaß zu agieren. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde bei der Erwägung des angemessenen Betrags für die Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedsstaat und der wirtschaftlichen Lage der Person Rechnung tragen (Erwägungsgrund 150 zur EU-DSGVO). Dem Willen des EU-Gesetzgebers folgend sind sie aber dazu angehalten, abschreckend und empfindlich zu ahnden.

Cyber-Risk-Versicherung abschließen?

Man kann sich zwar nicht generell dagegen versichern lassen, dass eigene Datenschutzverstöße von einer Versicherung getragen werden. Aber immerhin gibt es Cyber-Risk-Versicherungen, um sich gegen Datenschutzverstöße aufgrund von Cyberattacken auf das eigene Unternehmen versichern zu lassen. In der Regel ist der jährliche Versicherungsbeitrag ein verhältnismäßig kleiner Aufwand, um sich gegen ein großes Risiko im Unternehmen zu versichern.

Pflicht zu Mitarbeiterschulungen

Es besteht die Pflicht zur Mitarbeiterschulung. Einmal im Jahr ist ausreichend. Es empfiehlt sich aber, solche Schulungen regelmäßig durch qualifizierte Referenten durchführen zu lassen. Denn letztlich sind es die Mitarbeiter, die die häufigsten Datenschutzverstöße verursachen, nicht unbedingt die Cyber-Angriffe von außen. Der Klassiker ist hierbei das Versenden einer E-Mail mit personenbezogenen Daten des Kunden an einen falschen Empfänger. Schon ist ein Datenschutzverstoß begangen. Da hilft auch kein Standard-Disclaimer unter der E-Mail-Signatur.

Umso wichtiger ist es, dass für solch einen vorhersehbaren Datenschutzverstoß den Mitarbeitern Regelungen an die Hand gegeben werden, wie sie sich in diesem Fall zu verhalten haben: Wer muss intern darüber informiert werden? Wer ist dessen Vertretung? Wer informiert den betroffenen Kunden? Wer entscheidet, ob der Vorfall so schwer wiegt, dass die Datenschutzbehörde informiert werden muss? Stichwort: 72 Stunden Meldepflicht!

Natürlich empfehlen sich auch externe Schulungen von Dienstleistern zu diesem Thema. Am Ende muss im Unternehmen das Datenschutzniveau auf DSGVO-Standard gebracht werden. Dies ist keine einmalige Anstrengung, sondern ein dauerhafter Prozess.

https://www.experten.de/2018/09/03/dsgvo-leitfaden-thema-der-datenschutzbeauftragte/

https://www.experten.de/2018/09/06/dsgvo-leitfaden-thema-verzeichnis-und-datenschutz-folgenabschaetzung/

https://www.experten.de/2018/09/11/leitfaden-dsgvo-thema-technisch-organisatorische-massnahmen/

https://www.experten.de/2018/09/13/leitfaden-dsgvo-thema-einwilligung-auftragsdaten-und-rechte/

Bilder: (1) © photoschmidt / fotolia.com (2) © Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4945391/leitfaden-dsgvo-thema-mitarbeiter-rechenschaftspflicht-und-cyber/