expertenReport

Größter Umbruch im Datenschutzrecht

Auf die Versicherungsmakler kommt 2018 einiges an neuen Gesetzesregelungen zu. Auch das Thema Datenschutz muss angepackt werden. Eine große Tageszeitung titelte gar sinngemäß: „größter Umbruch im Datenschutzrecht aller Zeiten“. So weit würde der Verfasser zwar nicht gehen, aber unstreitig gibt es für deutsche Unternehmer erhöhten Handlungsbedarf. Es bedarf einer guten Compliance-Strategie, um das neue Datenschutzniveau zu erreichen.

Den 25. Mai 2018 im Kalender rot anstreichen

Am 25. Mai 2018 läuft die zweijährige Umsetzungsfrist ab, die der EU-Gesetzgeber allen Unternehmern gewährt, um sich auf den neuen Datenschutzstandard in der EU einzustellen. Mit Ablauf dieser Umsetzungsfrist gibt es keine Ausreden mehr für diejenigen Unternehmer, die sich bis dahin noch nicht mit der EU-Datenschutz-Grundverordnung (DSGVO) beschäftigt haben. Gleichzeitig mit Ablauf dieser Frist tritt ebenfalls ein neues Bundesdatenschutzgesetz (BDSG) in Deutschland in Kraft.

> Sebastian Karch, Rechtsanwalt / Gesellschaftsrecht, Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft
> Auch der Versicherungsmakler, wie alle Unternehmer in Deutschland, steht in der Pflicht zur Einhaltung des Datenschutzes.

Ziel (Art. 1 DSGVO) und Grundsätze (Art. 5 DSGVO) der DSGVO

Datenschutz ist Grundrechtsschutz! Das Ziel der DSGVO ist der Schutz der „personenbezogenen Daten“ aller EU-Bürger. Der EU-Gesetzgeber will ein einheitliches Datenschutzniveau in den Mitgliedstaaten etablieren. Skandale, wie die Datensammelwut sozialer Netzwerke und die Speicherung von Fluggastdaten, waren Auslöser der Datenschutzreform. Dabei haben deutsche Unternehmer einen klaren Standortvorteil, da der Datenschutz nach aktuellem BDSG (zumindest theoretisch) schon sehr hoch ist und von der DSGVO im Vergleich zu anderen Mitgliedstaaten nur wenig angehoben wird. Datenschutzverstöße sollen auch großen Unternehmen richtig wehtun. Daher sind Bußgelder von bis zu 20 Millionen Euro möglich.

Zur Erreichung des Ziels muss jeder Unternehmer folgende DSGVO-Grundsätze leben: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht.

Dabei gilt natürlich weiterhin der Gesetzesvorbehalt, das heißt, es ist alles verboten, was nicht ausdrücklich durch Gesetz oder Einwilligung des Betroffenen erlaubt ist. Das Problem bei der Umsetzung der DSGVO ist, dass sie keinen Maßnahmenkatalog enthält, den der Unternehmer einfach abarbeiten kann. Vielmehr ist jeder Unternehmer angehalten, die Datenschutzgrundsätze eigenverantwortlich in seinem Unternehmen zu implementieren. Es ist also keine einmalige Anstrengung des Unternehmers gefordert, sondern die Etablierung einer konkreten Compliance-Strategie.

4 Punkte für eine gute Compliance-Strategie

1. Datenschutzbeauftragter (Art. 37 DSGVO)

Es gilt eine Pflicht zur Bestellung eines Datenschutzbeauftragten (DSB) im Unternehmen, wenn die „Kerntätigkeit“ in der umfangreichen Verarbeitung besonderer Kategorien von Daten (unter anderem Gesundheitsdaten und biometrische Daten) besteht.

Die gute Nachricht für Versicherungsmakler ist, dass nur durch die Ausübung des Berufs an sich keine Bestellpflicht ausgelöst wird. Die weniger gute Nachricht ist, dass die „Kerntätigkeit“ im oben genannten Sinne durch die Erfüllung der Pflichten aus dem Versicherungsmaklervertrag recht schnell betroffen sein dürfte. Für einzelne Makler mag es hier einen gewissen Argumentationsspielraum geben, aber jedem muss klar sein, dass die Entscheidung, keinen DSB zu bestellen, teuer werden kann. Denn sollte die Datenschutzbehörde im Nachhinein zu dem Ergebnis kommen, dass die Bestellpflicht gegeben ist, kann die Nichtbestellung von der Behörde mit bis zu 10 Millionen Euro sanktioniert werden. Bei Zweifeln über die Bestellpflicht ist der sicherste Weg also die freiwillige Bestellung eines DSB.

2. Technisch-organisatorische Maßnahmen (TOMs), Art. 32 DSGVO

Der Unternehmer hat Schutzmaßnahmen zu treffen, damit die personenbezogenen Daten seines Kunden nicht verloren gehen oder unbefugten Dritten in die Hände fallen. Dafür ist es ausreichend, dass ein „angemessenes“ Schutzniveau eingerichtet wird, welches an den Risiken im Falle des Datenschutzverstoßes festzumachen ist. Die Verschlüsselung ist hierbei ein vorzugswürdiges Mittel. Eine Pflicht zur Verschlüsselung gibt es indes nicht. Wird sich gegen die Verschlüsselung entschieden, sollte dies unbedingt mit guten Argumenten dokumentiert werden. Weiterhin sollen die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sichergestellt werden. Überdies soll gewährleistet werden, dass die Daten auch nach eventuellen Zwischenfällen wieder rasch verfügbar sind. Dies alles soll stets auf dem aktuellen Stand der Technik erfolgen. Was unter „Stand der Technik“ genau zu verstehen sein soll, ist allerdings unklar.

3. Verarbeitungsverzeichnis (Art. 30 DSGVO) und Folgenabschätzung (Art. 35 DSGVO)

Das Verarbeitungsverzeichnis ist der Dreh- und Angelpunkt der Datenschutz-Compliance. Der Verfasser empfiehlt dringend, bis zum 25. Mai ein Verarbeitungsverzeichnis anzulegen. Dies ist Pflicht! Das Verfahrensverzeichnis kann in schriftlicher oder elektronischer Form angelegt werden und muss folgende Pflichtangaben enthalten: Name und Kontaktdaten des Verantwortlichen und gegebenenfalls des Datenschutzbeauftragten, Zwecke der Verarbeitung, Beschreibung der Kategorien betroffener und personenbezogener Daten, Auskunft, ob die Daten in ein Drittland übermittelt werden, Löschfristen sowie eine Beschreibung der getroffenen TOMs. Die Datenschutz-Folgenabschätzung steigert das Niveau noch einmal. Hier trifft den Unternehmer die Pflicht zur Vorab-Analyse, wenn die Datenverarbeitung ein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen darstellt. Wann dies in der Praxis der Fall sein soll, sollte eigentlich mittels einer sogenannten Black List von Behördenseite zur Verfügung gestellt werden. Diese liegt aktuell jedoch noch nicht vor, sodass noch unklar ist, wann die Pflicht definitiv greift.

4. Rechte der Betroffenen

Gegenüber ihren Kunden müssen Versicherungsmakler diese über deren Rechte transparent informieren, etwaigen Auskunftsansprüchen „unverzüglich“ nachkommen, gegebenenfalls die Daten berichtigen und Löschungsansprüchen nachgekommen werden. Der Löschungsanspruch sollte allerdings stets in eine „Sperrung“ der Daten abgewandelt werden, um sich später noch gegen etwaige Ansprüche wegen Falschberatung wehren zu können.

Fazit

Auch der Versicherungsmakler, wie alle Unternehmer in Deutschland, steht in der Pflicht zur Einhaltung des Datenschutzes. Dabei stellt der Versicherungsmaklervertrag stets die Rechtsgrundlage für die Verarbeitung dar (Art. 6 Abs. 1 Buchst. b) DSGVO). Zudem sollten Einwilligungen in die Verarbeitung der Daten von den Kunden eingeholt werden und geprüft werden, ob

mit Dienstleistern ein Auftragsdatenverarbeitungsvertrag (ADV) abzuschließen ist. Die Dokumentation aller datenschutzrechtlichen Anstrengungen ist zu empfehlen. Ein Verarbeitungsverzeichnis muss unbedingt erstellt werden.

Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft, Mail

Bilder: (1) © ra2 studio / fotolia.com (2) © Kanzlei Michaelis Rechtsanwälte Partnerschaftsgesellschaft (3) © experten-netzwerk GmbH

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4944730/groesster-umbruch-im-datenschutzrecht/