Datenschutz für Versicherer: Alles im Griff?

Der Datenschutz steht mehr denn je im Blick der Öffentlichkeit. Die gesetzlichen Anforderungen sind seit dem 1. September 2023 mit Inkrafttreten des teilrevidierten Datenschutzgesetzes (DSG) wesentlich umfangreicher und komplexer. Versicherer haben in aufwändigen Projekten das revidierte Datenschutzgesetz eingeführt. Allerdings wurden aus Zeit- und Ressourcengründen viele Aspekte nur mit kurzfristigen Massnahmen adressiert. Um diesbezügliche Risiken aktiv zu managen, lohnt es sich, den Reifegrad der eigenen Implementation extern überprüfen zu lassen.

Inkrafttreten

Am 1. September 2023 ist das teilrevidierte DSG ohne Übergangsfrist in Kraft getreten. Trotz zahlreicher Angleichungen an die Europäische Datenschutzgrundverordnung (DSGVO) behält das DSG weiterhin eine eigene Grundkonzeption und weicht deshalb in diversen Punkten vom europäischen Vorbild ab.

Versicherer sind betroffen

Die Bearbeitung von Personendaten ist für Versicherer alltäglich. Datenschutz ist dementsprechend unverzichtbar. Dies gilt insbesondere für jene Versicherer, die besonders schützenswerte Gesundheitsdaten bearbeiten.

Sanktionen

Im Gegensatz zur DSGVO richten sich datenschutzgesetzliche Sanktionen in der Schweiz persönlich gegen die jeweiligen Verantwortlichen – also die involvierten Mitarbeitenden. Datenschutzverletzungen können zu empfindlichen Bussen von bis zu CHF 250’000 führen.

Meist noch kostspieliger sind allerdings die Reputationsschäden durch Datenschutzverletzungen. Es kann Jahre dauern, diesbezügliches Vertrauen im Markt zurückzugewinnen.

Lückenhafte Umsetzung

Die meisten Versicherer haben interne DSG-Implementierungsprojekte durchgeführt. Dabei sind viele von ihnen auf Schwierigkeiten gestossen, die sie bis zum Inkrafttreten des DSG nicht vollständig überwinden konnten. Dies gilt insbesondere für die Einbettung der neuen DSG-Vorgaben in das interne Kontrollsystem.

Eine weitere offene Flanke ist vielerorts die automatisierte Datenlöschung. Denn diese ist typischerweise technisch schwierig und enorm teuer, weil komplexe Abhängigkeiten zwischen Datenbeständen und -strömen bestehen. Zudem werden die IT-Systeme laufend umgestaltet und modernisiert, weshalb Legacy-Systeme zum Teil bewusst nicht «fit for purpose» gemacht wurden.

Unsere Empfehlungen

Unser «post-implementation check» klärt, ob alle DSG-relevanten Aspekte im Umsetzungsprojekt erkannt, richtig gewichtet und umgesetzt wurden. Dies schafft wertvolles Know-how und zeigt im Sinne eines kontinuierlichen Verbesserungsprozesses Möglichkeiten zur Schliessung allfälliger Lücken auf.

Generell empfehlen wir Versicherern, ihren Datenschutzrahmen laufend weiterzuentwickeln. Sie sollten diesbezügliche Verantwortlichkeiten und Prozesse verbindlich festlegen, dokumentieren und in ihr internes Kontrollsystem (IKS) einbauen.

Zudem sollte die Wirksamkeit von Datenschutzkonzepten regelmässig mit spezifischen Kennzahlen (KPI) gemessen und an den Verwaltungsrat rapportiert werden.

Dieses «Framework» muss – und das ist immer entscheidend – schliesslich auch tatsächlich gelebt werden.

Datenschutz als Daueraufgabe

Versicherer dürfen Datenschutz somit nicht als starren Anforderungskatalog betrachten, der einmal umgesetzt werden kann. Vielmehr bleibt Datenschutz eine Daueraufgabe. Denn nach der DSG-Einführung ist vor der DSG-Optimierung.

Unsere Dienstleistungen

KPMG unterstützt Sie in sämtlichen Bereichen des Datenschutzes und bietet Ihnen verschiedene Dienstleistungen an, wie zum Beispiel:

- Überprüfung der Einhaltung des Datenschutzes (Gap-Analyse);
- Überprüfung und Verbesserung des Datenschutz-Control-Frameworks;
- Messung und Reduktion der residualen Compliance-Risiken;
- Entwicklung unternehmensspezifischer Konzepte und Programme wie Löschkonzepte;
- Dokumentation der technischen und organisatorischen Massnahmen im Bereich Datenschutz;
- jederzeitige Unterstützung in sämtlichen datenschutzrechtlichen Belangen durch unseren DPO-Support-Service («Spezialisten auf Abruf»).

Unser Team aus hochqualifizierten Spezialistinnen und Spezialisten mit profunder Erfahrung in den Bereichen Datenschutz, IT-Sicherheit, Recht und Compliance, Risiko- und Projektmanagement, Audit und Zertifizierung unterstützt Sie gerne bei allen Datenschutzthemen.

Kontakt

KPMG AG
Badenerstrasse 172
Postfach
CH-8036 Zürich

kpmg.ch

Dr. Thomas Bolliger
Client Partner Privacy

+41 79 354 52 67
tbolliger@kpmg.com

Alberto Job
Director
Leiter Fachstelle Datenschutz

+41 79 326 25 89
albertojob@kpmg.com

Alexander Lacher
Partner, Financial Services,
Insurance Regulatory & Compliance

+41 58 249 33 66
alacher@kpmg.com