Datenschutz in der Finanzindustrie

Der Datenschutz steht mehr denn je im Blickpunkt der Öffentlichkeit. Die gesetzlichen Anforderungen sind seit dem 1. September 2023 mit Inkrafttreten des revidierten Datenschutzgesetzes (DSG) wesentlich umfangreicher und komplexer. Finanzdienstleister haben in aufwändigen Projekten das revidierte Datenschutzgesetz eingeführt. Allerdings wurden aus Zeit- und Ressourcengründen viele Aspekte nur mit kurzfristigen Massnahmen adressiert. Dies gilt insbesondere für die Einbettung des Datenschutz Control-Frameworks ins interne Kontrollsystem. Um diesbezügliche Risiken weiterhin aktiv zu managen, lohnt es sich, den Reifegrad der eigenen Implementation überprüfen zu lassen.

Inkrafttreten

Am 1. September 2023 ist das teilrevidierte DSG in Kraft getreten. Die Revision führte zu zahlreichen Angleichungen an die Europäische Datenschutzgrundverordnung (DSGVO), behält jedoch weiterhin eine eigene Grundkonzeption bei und weicht deshalb in diversen Punkten vom europäischen Vorbild ab. Das revidierte Gesetz ist ohne Übergangsfrist in Kraft getreten.

Finanzdienstleister sind betroffen

Personendaten gehören zum Alltag der Finanzindustrie. Der Datenschutz ist dementsprechend besonders wichtig. Finanzdienstleister neben Vermögenszahlen auch Hintergrundinformationen (KYC) von Kunden, die auch besonders schützenswerte Daten beinhalten können.

Sanktionen

Im Gegensatz zur DSGVO, bei der lediglich Unternehmen oder Organisationen im Fokus stehen, richten sich datenschutzgesetzliche Sanktionen in der Schweiz persönlich gegen die Verantwortlichen, also die involvierten Mitarbeitenden. Datenschutzverletzungen können zu empfindlichen Strafen von bis zu CHF 250'000 führen.

Unsere Empfehlungen

Wir empfehlen den Datenschutzverantwortlichen,
im Nachgang zur (Erst-)Implementation den Datenschutzrahmen laufend weiterzuentwickeln,
um die mittel- bis langfristige Compliance sicherzustellen.

Um Sanktionen vorzubeugen, müssen Unternehmen insbesondere ihre Datenschutz-Verantwortlichkeiten und -Prozesse verbindlich festlegen und dokumentieren. Dieses «Framework» muss tatsächlich gelebt werden. Anfänglich allenfalls bewusst in Kauf genommene Lücken sollten im Sinne eines kontinuierlichen Verbesserungsprozesses laufend überwacht und idealerweise reduziert werden.

Post-Implementation Check

Die meisten Finanzinstitute haben (oft interne) DSG-Implementierungsprojekte durchgeführt. Wurden dabei alle relevanten Aspekte erkannt und richtig gewichtet? Eine unabhängige Prüfung («post-implementation check») schafft hier Klarheit, generiert wertvolles Know-how und zeigt Möglichkeiten zur Schliessung von Lücken auf.

Datenschutz als Daueraufgabe

Finanzinstitute dürfen den Datenschutz nicht als starren Anforderungskatalog betrachten, der einmal umgesetzt werden muss. Der Datenschutz ist vielmehr ein fortwährender Prozess. Die Funktionalität der implementierten Datenschutzprozesse muss regelmässig auf Angemessenheit und Wirksamkeit überprüft und gegebenenfalls verbessert werden. Finanzinstitute sollten folglich ihre datenschutzrechtlichen Vorgaben in ihr internes Kontrollsystem (IKS) einbauen. Es empfiehlt sich, die Wirksamkeit des Datenschutzkonzepts mit spezifischen Kennzahlen («KPI») zu messen und zu rapportieren.

Risiken reduzieren

Bei der Einführung des DSG sind einige Finanzdienstleister auf Schwierigkeiten gestossen, die sie nicht bis zum Inkrafttreten des DSG überwinden konnten. Beispielhaft ist automatisierte Datenlöschung. Diese ist typischerweise technisch enorm komplex (Abhängigkeiten bei den Datenbeständen und -strömen) und dementsprechend teuer.

Zudem werden die IT-Systeme laufend umgestaltet und modernisiert. Dies kann dazu führen, dass Legacy-Systeme bewusst nicht mehr «fit for purpose» gemacht wurden. Die entsprechenden Compliance-Risiken können müssen mit kosteneffizienten und pragmatischen Konzepten bis zur Dekommissionierung übergangsweise besonders eng begleitet werden. Wir helfen dabei effektiv und effizient.

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 von unternehmensspezifischen Konzepten und Programmen 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 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. Denn nach der DSG-Einführung ist vor der DSG-Optimierung.

Kontakt

KPMG AG
Badenerstrasse 172
Postfach
CH-8036 Zürich

kpmg.ch

Alberto Job
Director
Information Management & Governance

+41 79 326 25 89
albertojob@kpmg.com

Lukas Markusich
Assistant Manager
Financial Services

+41 76 368 63 60
lukasmarkusich@kpmg.com