Neue Datenschutzgesetz-gebung – Erfahrungen mit der Umsetzung

Seit dem 1. September 2023 ist das revidierte Schweizer Datenschutzgesetz in Kraft. In den vergangenen Monaten haben wir eine grössere Anzahl von Finanzdienstleistern bei der Umsetzung der neuen Vorschriften begleitet. Unser Fazit bis heute: Die Umsetzung lässt sich in der Regel und für das Gros der Änderungen mit vertretbarem Aufwand bewerkstelligen. Unterschätzen sollte man die Thematik allerdings nicht und generell können wir festhalten, dass sich einige Neuerungen einfacher umsetzen lassen als andere. Welche Themen dabei besonders im Fokus stehen, erläutern wir nachfolgend anhand unserer bisherigen Praxiserfahrung mit dem neuen Datenschutzgesetz.

Einordnung[1]

	Banken / Wertpapierhäuser	**Asset Management-Institute** (Fondsleitungen, Verwalter von Kollektivvermögen)	**Vermögensverwalter / Trustees**	**Übrige Finanzintermediäre** (SRO-Beaufsichtigte)
Anwendbarkeit	Ja	Ja	Ja	Ja
Relevanz	Hoch	Normal	Hoch	Hoch

[1] Es handelt sich um eine stark vereinfachte Darstellung, welche eine rasche erste Einordnung der Thematik ermöglichen soll. Jedes Institut sollte die Relevanz und den konkreten Handlungsbedarf individuell-konkret bestimmen.

Sich einen Überblick verschaffen

Es ist absolut unerlässlich, dass sich der Finanzdienstleister zu Beginn einen Überblick über die Datenbearbeitungen in seinem Betrieb verschafft und sich entsprechend Gedanken zu Rollen und Verantwortlichkeiten macht. Ohne eine solche generelle Übersicht wird eine regelkonforme Umsetzung der Vorschriften zwangsläufig scheitern. Ob ein formelles Bearbeitungsverzeichnis vorgeschrieben respektive sinnvoll ist, ist im Einzelfall individuell zu entscheiden. In den Projekten hat es sich aber bewährt, bereits bei nur leicht komplexeren Verhältnissen ein Verzeichnis zu erstellen (z.B., wenn mehrere Arten von Dienstleistungen angeboten werden). Das Verzeichnis kann dann als Basis für die weiteren Umsetzungsarbeiten verwendet werden.

Qualifizierung von Beziehungen mit Kooperationspartnern

Die Qualifizierung der Beziehungen zwischen dem Finanzdienstleister und seinen jeweiligen Kooperationspartnern (z.B. Banken, IT, Research-Dienstleister, Corporate Services, Berater) hat sich als besonders herausfordernd erwiesen. Das mit dem revidierten Datenschutzgesetz neu eingeführte Rollenmodell, mit dem «Verantwortlichen» und gegebenenfalls einem «Auftragsbearbeiter», ist nur auf den ersten Blick einfach umzusetzen. So qualifiziert entgegen einem allgemeinen Sprachverständnis folgend, nicht jedes Auftragsverhältnis, welches die Bearbeitung von Personendaten mitbeinhaltet, als Auftragsbearbeitung im Sinne des Datenschutzgesetzes.

In der praktischen Umsetzung ist somit bei sämtlichen Bearbeitungen von Personendaten, die nicht ausschliesslich durch den Finanzdienstleister durchgeführt werden, zu prüfen, wer «Verantwortlicher» ist, und ob zusätzlich eine Auftragsbearbeitung vorliegt.

In unseren Projekten haben wir gute Erfahrungen damit gemacht, sich direkt mit den Kooperationspartnern auszutauschen, um im Detail zu verstehen, welche Personendaten wie und in welchem Umfang bearbeitet werden.

Zumindest in den Fällen, in denen eine Auftragsbearbeitung vorliegt, ist eine Sichtung und gegebenenfalls Anpassung des Vertrags zwischen dem Finanzdienstleister und seinem Kooperationspartner notwendig. Letzteres kann im Einzelfall wiederum herausfordernd sein, vor allem dann, wenn unterschiedliche Ansichten bezüglich der Notwendigkeit von Anpassungen respektive deren Ausgestaltung bestehen.

Datensicherheit

Finanzinstitute müssen technische und organisatorische Massnahmen treffen um Personendaten angemessen zu schützen. Die Verordnung zum Gesetz enthält einen umfangreichen Katalog solcher technischen und organisatorischen Massnahmen. Abgesehen davon, dass Verletzungen der Datensicherheit gravierende Auswirkungen haben können, zu denken ist hierbei z.B. an den Verlust von Kunden- oder Mitarbeiterdaten: Wer die Mindestanforderungen an die Datensicherheit verletzt, macht sich unter Umständen strafbar.

In der praktischen Umsetzung haben wir in einem ersten Schritt jeweils abgeklärt, welche Massnahmen zur Datensicherheit bereits bestehen und haben diese dokumentiert. Wo IT-Dienstleistungen an Dritte ausgelagert wurden, dies war bei der überwiegenden Anzahl der von uns begleiteten Institute zumindest teilweise der Fall, haben wir diesen Schritt wann immer möglich gemeinsam mit diesen Dienstleistern vorgenommen.

Bei der Beurteilung der Angemessenheit der Massnahmen ist wiederum die Komplexität der Verhältnisse zu berücksichtigen. Auch hier konnten IT-Dienstleister in der Regel wertvollen Input liefern. Der Beizug von Spezialisten ist aber teilweise unabdingbar.

Umsetzung der Informationspflichten

Für Finanzdienstleister, welche einen guten Überblick über die stattfindenden Datenbearbeitungen, den Beizug von Dritten und die vorhandenen Massnahmen zur Datensicherheit haben, ist die Umsetzung der Informationspflichten danach mit vertretbarem Aufwand möglich. Da eine Verletzung der Informationspflichten zu einer Busse führen kann, ist eine sorgfältige Herangehensweise aber unbedingt zu empfehlen.

In Regel werden die Informationspflichten in einer oder mehreren (z.B. separat für Kunden, Mitarbeitende, Besucher der Webseite etc.) Datenschutzerklärungen formalisiert. Falls eine Webseite vorhanden ist, ist es sinnvoll die Datenschutzerklärung dort zu veröffentlichen. Zusätzlich sollte in Verträgen und/oder AGB's darauf hingewiesen werden, dass die Datenschutzerklärung auf der Webseite des Finanzdienstleiters zu finden ist.

Falls keine Webseite vorhanden ist, muss die Datenschutzerklärung den betroffenen Personen in anderer Art und Weise zur Kenntnis gebracht werden. Die Information, dass die Erklärung beim Unternehmen grundsätzlich vorhanden ist, ist nicht ausreichend.

Fazit

Finanzdienstleister, welche sich noch nicht mit den Bestimmungen des neuen Datenschutzgesetzes auseinandergesetzt haben, sollten dies zeitnah in Angriff nehmen. Abwarten ist keine Option. Die hierzu notwendigen Arbeiten sind zwar mit Aufwand verbunden, können aber durch eine gute Planung, eine klare Zuteilung von Rollen und Verantwortlichkeiten und falls notwendig unter Beizug der notwendigen Fachexpertise effizient umgesetzt werden.

Haben Sie Fragen zum neuen Datenschutzgesetz und/oder zur konkreten Umsetzung? Gerne unterstützen Sie unsere Spezialisten vom Regulatory & Compliance FS Team. Wir freuen uns auf Ihre Kontaktaufnahme.

Boris Hofer
Director, Regulatory & Compliance FS
Grant Thornton AG
T +41 43 960 72 63
E boris.hofer@ch.gt.com

Yasmine Schwager
Assistant, Regulatory & Compliance FS
Grant Thornton AG
T +41 43 960 72 46
E yasmine.schwager@ch.gt.com