Grant Thornton

Neues Datenschutzgesetz per 1. September 2023

Das neue Datenschutzgesetz tritt per 1. September 2023 in Kraft – die Frist rückt näher. Was sollten die Finanzdienstleister die kommenden 3 Monate tun, um die Umsetzung voranzutreiben? Wo liegen die grössten Herausforderungen?

Boris Hofer, Director, Regulatory & Compliance im Gespräch mit Bettina Neresheimer, Head Marketing & Communication diskutieren diese und andere brennende Fragen rund um die Implementierung des neuen Datenschutzgesetzes.

Bettina Neresheimer: Am 1. September 2023 tritt die neue Datenschutzgesetzgebung in Kraft, was bedeutet dies für Finanzdienstleister?
Boris Hofer: Praktisch sämtliche Unternehmen und somit auch Finanzdienstleister bearbeiten Personendaten (z.B. Kundendaten, Daten von Mitarbeitenden). Entsprechend werden sie von den neuen Vorschriften betroffen sein. Je nach Grösse, Geschäftsmodell etc. bestehen aber natürlich signifikante Unterschiede.

Bettina Neresheimer: Inwiefern?
Boris Hofer: Zur Beantwortung dieser Frage muss man sich einzelne Neuerungen im Detail anschauen. Ein Beispiel: Neu bestehen Vorschriften dazu, wie eine Beziehung zwischen zwei Unternehmen zu regeln ist, wenn eines dieser Unternehmen Personendaten im Auftrag des anderen bearbeitet, z.B. durch eine Auslagerung von IT-Servicedienstleistungen. In diesem Zusammenhang spricht man von sogenannten Auftragsbearbeitungen. Anzahl und Komplexität solcher Kooperationen sowie ein Auslandsbezug können zu mehr oder weniger Anpassungsbedarf führen. Bearbeitet ein Finanzdienstleister hingegen sämtliche Personendaten ausschliesslich «inhouse», so besteht diesbezüglich kein Handlungsbedarf.

Bettina Neresheimer: Wie beurteilst du den Umsetzungsstand bei den einzelnen Finanzdienstleistern und für welche Unterstützung werdet ihr zurzeit angefragt?
Boris Hofer: Wir stellen grosse Unterschiede fest. Die meisten Unternehmen müssen nicht bei 0 beginnen. Vermögensverwalter, welche die Compliance-Funktion ausgelagert haben, verfügen in der Regel bereits über ein Rahmenwerk, auf welchem aufgebaut werden kann. Schliesslich haben grössere Finanzdienstleister die Umsetzung oft im Rahmen umfangreicher Projekte vorangetrieben. Entsprechend werden wir aktuell sowohl für initiale Bedarfsanalysen, für Umsetzungsprojekte als auch für die Beurteilung von bereits implementierten Datenschutzrahmenwerken angefragt.

> «Wir empfehlen Unternehmen sich initial einen ersten Überblick darüber zu verschaffen, wo und wie es von den neuen Vorschriften betroffen sein könnte.»

Bettina Neresheimer: Viele Finanzdienstleister fragen sich: «Wo soll ich beginnen»?
Boris Hofer: Eine gute Frage. Wir empfehlen Unternehmen einerseits, sich initial einen ersten Überblick darüber zu verschaffen, wo und wie es von den neuen Vorschriften betroffen sein könnte. Dies bedingt Kenntnis über Art und Umfang der bearbeiteten Personendaten im Unternehmen. Unsere Erfahrungen zeigen, dass mit diesem «initialen Risikoprofil» bereits einigermassen abgeschätzt werden kann, ob respektive wo grössere Anpassungen anfallen werden und wie rasch diese

Arbeiten durchzuführen sind. Andererseits sollte innerhalb des Unternehmens eine verantwortliche Person identifiziert werden, welche sich der Thematik annimmt, respektive die Umsetzung der neuen Vorschriften koordiniert und sicherstellt. Wir sehen es relativ oft bei unseren Kunden, dass hierfür die Kompetenzen der Compliance Funktion entsprechend ausgebaut werden. Ab einer gewissen Unternehmensgrösse respektive Komplexität ist dann aber eine eigene Fachstelle üblich.

Bettina Neresheimer: Wie geht es danach weiter?
Boris Hofer: Das erstellte «initiale Risikoprofil» liefert zwar einen guten Überblick. Es reicht aber in der Regel noch nicht aus, um sich wirklich komfortabel zu fühlen und die entsprechenden Risiko- und Umsetzungsentscheide zu fällen. Wir empfehlen daher allen Finanzdienstleistern – unabhängig von deren Grösse und dem initial geschätzten Risiko – systematisch zu ermitteln, welches «Delta» zu den neuen Vorschriften besteht. Nur so wird eine verlässliche Entscheidungsgrundlage geschaffen.

Bettina Neresheimer: Dies klingt eher kompliziert und insbesondere für kleinere Finanzdienstleister allenfalls sehr aufwändig…
Boris Hofer: …die Herausforderung liegt in der Tat darin, dass das Resultat der Analyse nicht vorweggenommen werden sollte, auch wenn dies ab und zu verlockend sein mag. Es führt somit unseres Erachtens kein Weg an einer fundierten Analyse vorbei. Ohne entsprechende Erfahrung und Expertise besteht aber tatsächlich das Risiko, dass zu viel oder zu wenig abgeklärt wird.

Bettina Neresheimer: Bei welchen Anpassungen ist mit dem grössten Umsetzungsaufwand zu rechnen?
Boris Hofer: Dies ist abhängig vom Risikoprofil und der Grösse des Unternehmens und allenfalls bereits Bestehendem. So verfügen beispielweise viele Finanzdienstleister bereits über eine Datenschutzerklärung, die als Basis dient und angepasst werden kann. Unabhängig davon sind die Sichtung der Verträge mit Kooperationspartnern oder die Umsetzung der Datensicherheit sicher zeitnah in Angriff zu nehmen, da Anpassungen in diesen Bereichen meist nicht von heute auf morgen zu bewerkstelligen sind.

Bettina Neresheimer: Worauf gilt es bei der Umsetzung der Vorschriften zur Datensicherheit besonders zu achten?
Boris Hofer: Das ist eigentlich ein eigenständiges Thema, zumal sich die Datensicherheit nicht ausschliesslich auf den Schutz von Personendaten bezieht. Ein grosser Teil der Personendaten steht heute in digitaler Form zur Verfügung. Im Besonderen beim Schutz von elektronischen Daten ist Vorsicht geboten, denn nachdem der Schutzbedarf bestimmt ist, gilt es technische und organisatorische Massnahmen zu implementieren, welche den Schutz der Personendaten sicherstellen. Dabei muss sichergestellt werden, dass die Daten lediglich Berechtigten Personen zugänglich sind (Vertraulichkeit), dass die Daten zur Verfügung stehen, wenn sie benötigt werden (Verfügbarkeit), die Daten nicht verändert werden können (Integrität) und nachvollzogen werden kann, wann die Daten von wem bearbeitet wurden (Nachvollziehbarkeit).

Im Speziellen das Thema Nachvollziehbarkeit, könnte einigen Herstellern von Applikationen, welche Personendaten beinhalten, Kopfzerbrechen bereiten.

Bettina Neresheimer: Kannst Du das näher erklären?
Boris Hofer: Applikationen sind in der Regel relativ gut darin, die Nachvollziehbarkeit, von Datenveränderungen zu protokollieren. Anders sieht es beim Lesen von Daten aus. Lesezugriffe werden nicht immer standardmässig protokolliert.

Mit Christopher Oehri und seinem Team verfügt Grant Thornton über ausgewiesene Spezialisten in diesem Bereich, die für Fragen gerne zur Verfügung stehen.

Bettina Neresheimer: Deine Gedanken zum Thema «Bussen» in der neuen Datenschutzgesetzgebung?
Boris Hofer: Der im Vergleich zur jetzigen Gesetzgebung stark ausgebaute Bussenkatalog sollte nicht unterschätzt werden. Zwar sind nicht sämtliche Verletzungen der neuen Datenschutzgesetzgebung in diesem Katalog enthalten und fahrlässiges Handeln sollte generell nicht zu einer Busse führen. Mit einer guten Vorbereitung und einem guten Rahmenwerk lässt sich das Risiko also bereits begrenzen. Da die maximalen Bussen mit CHF 250'000 sehr hoch und diese Bussen grundsätzlich persönlicher Natur sind, kann es sich ein Unternehmen nicht leisten, diesen Aspekt der neuen Datenschutzgesetzgebung komplett zu ignorieren. Verurteilungen von eigenen Mitarbeitenden liegen sicher nicht im Interesse eines Finanzdienstleisters.

Bettina Neresheimer: Für die Umsetzung bleiben noch gut drei Monate Zeit. Reicht das oder wo siehst Du allenfalls Engpässe?
Boris Hofer: Finanzdienstleister, die noch nicht mit der Umsetzung begonnen haben, sind sicher gut darin beraten, nicht weiter zuzuwarten. Wird zeitnah gestartet, so scheint die rechtzeitige Umsetzung auch bei Unternehmen mit etwas komplexeren Verhältnissen noch möglich. Für sämtliche Unternehmen gilt nun aber «je früher desto besser».

Bettina Neresheimer: Zum Abschluss noch eine persönliche Frage: Was ist für Dich das Spannende am Datenschutz?
Boris Hofer: Datenschutz betrifft ein Unternehmen in seiner Gesamtheit und kann nicht isoliert, z.B. als rein rechtliche Thematik oder als alleinige Herausforderung der Informationssicherheit betrachtet werden. Ich gehe sodann von aus, dass sowohl Bedeutung wie auch Komplexität des Datenschutzes noch zunehmen werden. Wenn man sich beispielsweise die rasanten Entwicklungen im Bereich des maschinellen Lernens (Stichwort: Künstliche Intelligenz) anschaut, wird bereits klar, dass hier noch einiges kommen wird. Die funktionsübergreifende Umsetzung der Datenschutzanforderungen unter Berücksichtigung der verschiedenen Interessen und mit Blick auf die Zukunft sind somit und zumindest für mich das Spannende an Projekten in diesem Bereich.

Bettina Neresheimer: Vielen Dank für das Interview!

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

Weiterführende Informationen zum Thema «Neues Datenschutzgesetz»:

Neues Datenschutzrecht per 1. September 2023 – Wichtigste Neuerungen im Überblick

Die Totalrevision des schweizerischen Datenschutzgesetzes