



DAS GELDWÄSCHEREIGESETZ (GWG) IM SPANNUNGSFELD MIT DEM DATENSCHUTZGESETZ (DSG)? WAS FINANZINTERMEDIÄRE IN DER PRAXIS ZU BEACHTEN HABEN!

Eine nicht zu unterschätzende Frage, denn seit der Einführung des revidierten DSG können natürliche Personen (und nicht etwa das handelnde Unternehmen) für Verletzungen des DSG mit Bussen von bis zu CHF 250'000 bestraft werden.

Das revidierte DSG ist nun seit gut zwei Jahren in Kraft. Eine Rekapitulation für Finanzintermediäre:

1. Ausgangslage:

Unter dem GwG sind Finanzintermediäre namentlich dazu verpflichtet, umfassend Personendaten zur Identifikation des Vertragspartners, Feststellung der wirtschaftlich berechtigten Person und Angaben zu Transaktionen zu sammeln. Schliesslich besteht die Pflicht zur Erstellung eines Kundenprofils (KYC). Im Falle von Geschäftsbeziehungen mit erhöhtem Risiko (GMER) bzw. Transaktionen mit erhöhtem Risiko (TMER) unterliegen Finanzintermediäre einer nochmals gesteigerten Abklärungs- und Dokumentationspflicht. Dazu kommen umfassende Aufbewahrungspflichten gemäss GwG. In der Praxis zeigt sich denn auch immer wieder, dass insbesondere im Zusammenhang mit internationaler Kundschaft in- und ausländische Finanzintermediäre (z.B. bei der Eröffnung eines neuen Bankkontos) sowie zum Teil auch Steuerbehörden dokumentierte Informationen voraussetzen, welche weit über die gesetzlichen Verjährungs- und Aufbewahrungsfristen hinausgehen. Hierbei erwarten Kunden regelmässig, dass der Finanzintermediär diese Informationen zur Verfügung stellen kann.

Im Gegensatz dazu sieht sich der Finanzintermediär gemäss DSG mit dem (Daten)-Bearbeitungsgrundsatz der Verhältnismässigkeit und der Transparenz konfrontiert. Aus ersterem fliesst insbesondere die Pflicht zur Datenminimierung und die Verpflichtung, die Daten nur insoweit zu bearbeiten, als es für deren Bearbeitungszweck notwendig ist. Des Weiteren muss daraus eine Verpflichtung zur Löschung nach Zweckerfüllung abgeleitet werden.

Der Tenor gemäss GwG scheint, je mehr Daten desto besser. Dies steht wiederum im konzeptionellen Widerspruch zum DSG. Was bedeutet das in der Praxis?

2. Generelles Verhältnis zwischen GwG und DSG:

Bei Verletzungen der Datenbearbeitungsgrundsätze nach DSG, die der Finanzintermediär in Anwendungen der Sorgfaltspflichten des GwG begeht, wird er



sich ggf. auf den gesetzlichen Rechtfertigungsgrund gemäss Art. 31 Abs. 1 DSG berufen können. Von einer grundsätzlichen Derogation des DSG, in Anwendung des GwG, kann er aber nicht ausgehen.

Gemäss Art. 33 GwG richtet sich die Bearbeitung von Personendaten im Rahmen des GwG grundsätzlich nach dem DSG. Datenbearbeitungen im Zusammenhang mit Geldwäscherei-Verdachtsmeldungen nach Art. 9 GwG (bzw. nach Art. 305 Abs. 2 StGB), werden vom Gesetzgeber als besonders delik特 empfunden und richten sich nach Art. 34-35a GwG.

3. Praktische Umsetzung:

Für die Finanzintermediäre bedeutet dies in der Praxis nichts anderes, als dass sie die **Bearbeitungsgrundsätze** des DSG auch in Erfüllung ihrer Sorgfaltspflichten gemäss GwG einhalten müssen. Namentlich gilt das für:

- **Verhältnismässigkeit (Art 6 Abs. 2 DSG):** Die Datenbearbeitung darf nicht weiter gehen, als es zur Erfüllung des Bearbeitungszwecks notwendig ist. Beispielsweise sollten Datenbanken (CRM etc.) mit Zugriffsbeschränkungen versehen sein. Unzulässig wäre auch eine flächendeckende, auf jede Kundenbeziehung angewendete, vertiefte Abklärung zur Herkunft von Vermögenswerten (Source of Funds, Source of Wealth), ohne entsprechenden Anlass aus dem GwG (GMER etc.).
- **Transparenzgebot (Art. 6 Abs. 3 DSG):** Bei der Beschaffung von Personendaten muss der Zweck der Beschaffung für die betroffene Person erkennbar sein. In diesem Zusammenhang gilt es die Informationspflicht gemäss Art. 19 DSG zu beachten. In der Praxis versuchen Verantwortliche dieser Pflicht mittels allgemeiner Datenschutzerklärungen (bspw. durch verfügbar machen auf der Webseite) nachzukommen.
- **Zweckbindung (Art. 6 Abs. 3 DSG):** Personendaten dürfen nur insoweit bearbeitet werden, als dass es mit dem Beschaffungszweck zu vereinbaren ist. Beispielsweise dürfen Daten, die zum Zwecke der Identifizierung des Vertragspartners erhoben wurden, nicht per se zu Marketingzwecken verwendet werden (Zustellung Newsletter etc.). Ist der Zweck erfüllt, müssen die Daten gelöscht werden. In Anbetracht der eingangs erwähnten Erwartungshaltung gegenüber Finanzintermediären, Daten auch noch Jahrzehnte nach deren Erhebung zur Verfügung zu haben, kann diese Vorgabe in der Praxis Probleme bereiten.
- **Datenrichtigkeit (Art. 6 Abs. 5 DSG):** Der Finanzintermediär hat dafür zu sorgen, dass die bearbeiteten Daten richtig sind. Er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Beispielsweise müssen Adressänderungen oder neue Telefonnummern von Kunden nachgeführt werden. Meldungen über solche Änderungen müssen verlangt oder vereinbart werden.
- **Datensicherheit (Art. 8 DSG):** Der Finanzintermediär hat durch geeignete technische und organisatorische Massnahmen für die Datensicherheit besorgt zu sein. Aus technischer Hinsicht hat er seine Server beispielsweise mit Firewalls zu schützen oder gespeicherte Daten zu



verschlüsseln. Aus organisatorischer Sicht hat er seine Mitarbeiter namentlich zu schulen und Weisungen zu erlassen.

4. Weitere Pflichten gemäss DSG:

Mit den folgenden Ausführungen sollen die grundlegenden Pflichten gemäss DSG, inklusive allfälliger Sanktionen bei Verletzung, aufgezeigt werden.

In Erfüllung ihrer Sorgfaltspflichten gemäss GwG, müssen Finanzintermediäre nebst den erwähnten Bearbeitungsgrundsätzen des Weiteren eine mögliche Pflicht zur Erstellung eines **Bearbeitungsverzeichnisses** (Art. 12 DSG) prüfen. Damit ist ein Überblick über sämtliche Datenbearbeitungen innerhalb des Unternehmens zu verstehen. Insbesondere sind darin Angaben über die Identität des Verantwortlichen, den Bearbeitungszweck und eine Beschreibung der Kategorien betroffener Personen und bearbeiteter Personendaten sowie zum Empfänger der Daten zu machen. Für KMU hat der Bundesrat eine Erleichterung bzw. eine Enthebung zur Pflicht der Erstellung eines Bearbeitungsverzeichnisses vorgesehen (Art. 12 Abs. 5 DSG). Ein Blick auf die Sanktionsbestimmungen des DSG (Art. 60 ff. DSG) zeigt jedoch, dass ein Unterlassen dieser Pflicht keine direkten Sanktionen nach sich zieht. Aus Gründen der Übersichtlichkeit, Kontrolle und angesichts potentieller Auskunftsbegehlen durch Betroffene, ist eine Führung des Bearbeitungsverzeichnisses jedoch auch für KMUs zu empfehlen.

Im Gegensatz zur Datenschutz-Grundverordnung der EU (DSGVO) steht es Finanzintermediären unter dem DSG grundsätzlich frei, eine **Datenschutzberaterin** zu ernennen oder nicht. Ein Datenschutzberater sollte den Entscheidungsträgern in Fragen des Datenschutzes beratend und unterstützend zur Seite stehen und keinesfalls selber entscheiden. Nicht zuletzt sollte damit in der Praxis eine persönliche Haftung der Datenschutzberaterin vermieden werden können. Relevante (gesetzliche) Vorteile bringt die Ernennung einer Datenschutzberaterin indes nicht. Einziger Vorteil gemäss DSG ist die mögliche Umgehung der Konsultationspflicht mit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) im Rahmen einer Datenschutz-Folgenabschätzung (Art. 23 Abs. 4 DSG).

Eine **Datenschutz-Folgenabschätzung** gemäss Art. 22 DSG müssen Finanzintermediäre immer dann in Betracht ziehen, wenn eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Zu denken ist hier insbesondere auch an KI-gestützte Anwendungen zur Bearbeitung von Personendaten. Mit der Datenschutz-Folgenabschätzung sollen einerseits Risiken erkannt und bewertet und andererseits mitigierende Massnahmen aufgezeigt werden. Gemäss Art. 22 Abs. 4 DSG sind private Verantwortliche namentlich dann von der Pflicht zur Erstellung einer Datenschutz-Folgeabschätzung ausgenommen, wenn sie gesetzlich zur Bearbeitung der Daten verpflichtet sind. Dies gilt folglich insbesondere für Datenbearbeitungen durch Finanzintermediäre im Rahmen des GwG. Die Verletzung der Pflicht zur Erstellung einer Datenschutz-Folgeabschätzung zieht wiederum keine direkten Sanktionen gemäss DSG nach sich (vgl. Art. 60 ff. DSG).

Des Weiteren müssen Finanzintermediäre die Voraussetzungen im Zusammenhang mit einer allfälligen **Bekanntgabe von Personendaten ins Ausland** (Art. 16 ff. DSG) kennen. Personendaten dürfen immer dann ins Ausland transferiert werden, wenn die ausländische Gesetzgebung einen angemessenen Schutz bietet bzw. dem Schweizer Datenschutzniveau entspricht. Welche Länder diese Voraussetzungen erfüllen wird vom Bundesrat festgelegt und im Anhang 1 der Datenschutzverordnung (DSV) publiziert. Möchte ein Finanzintermediär Daten in ein Land bekanntgeben, das



nicht auf der genannten Liste steht (insbesondere Länder ausserhalb EWR), muss ein geeigneter Datenschutz gemäss Art. 16 Abs. 2 lit. a-e DSGVO durch anderweitige Massnahmen gewährleistet sein. Namentlich durch: Einen völkerrechtlichen Vertrag, entsprechende Datenschutzklauseln in einem Vertrag, Standardvertragsklauseln (SCC) oder verbindliche unternehmensinterne Datenschutzvorschriften (BCR). Art. 17 DSGVO regelt Ausnahmen von den Vorschriften gemäss Art. 16 DSGVO. Beispielsweise dürfen Personendaten ins Ausland bekannt gegeben werden, wenn die betroffene Person in die Bekanntgabe eingewilligt hat oder die Bekanntgabe in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages steht. Wer die Bestimmungen im Zusammenhang mit der Bekanntgabe von Personendaten ins Ausland verletzt, kann auf Antrag mit Busse bestraft werden (Art. 61 DSGVO).

Nach Art. 24 DSGVO sind **Datensicherheitsverletzungen (Data Breach)**, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder Grundrechte der betroffenen Person führen, dem EDÖP zu melden. Finanzintermediäre haben zudem aufsichtsrechtliche Meldepflichten zu beachten (insbesondere FINMA). Im Gegensatz zur DSGVO wird eine unterbliebene Meldung gemäss DSGVO nicht direkt sanktioniert (vgl. Art. 60 ff. DSGVO).

Der Finanzintermediär muss sich für jede Datenbearbeitung mit Einbezug von Dritten der Rollenverteilung zwischen **Verantwortlichem** und **Auftragsbearbeiter** bewusst sein. Der Verantwortliche ist derjenige, der über Zweck und Mittel der Datenbearbeitung entscheidet. Er bestimmt also, warum und auf welche Art Daten bearbeitet werden und trägt die Hauptverantwortung für die Rechtmässigkeit dieser Bearbeitung. Der Auftragsbearbeiter hingegen bearbeitet die Personendaten niemals für eigene Zwecke, sondern ausschliesslich im Auftrag und auf Weisungen des Verantwortlichen (Bspw. Cloud Provider). Der Verantwortliche muss sicherstellen, dass die Zusammenarbeit mit dem Auftragsbearbeiter vertraglich geregelt ist und den Anforderungen des DSGVO entspricht.

Nach Art. 60 DSGVO wird zudem mit Busse bestraft, wer **Informationspflichten** gegenüber Betroffenen bei der Beschaffung von Personendaten nicht einhält, das **Auskunftsrecht** betroffener Personen nicht wahrt oder **Mitwirkungspflichten** im Rahmen von Untersuchungen des EDÖP verletzt.

Haben Sie weitere Fragen zu diesem Thema? Oder benötigen Sie Hilfe bei der Umsetzung in ihrem Unternehmen? Zögern Sie nicht, uns zu kontaktieren!

Our locations:
Mandaris AG
St. Alban-Anlage 46
CH-4052 Basel
Tel. +41 61 285 17 17

Mandaris AG
Selnastrasse 3
CH-8001 Zürich
Tel. +41 43 344 33 55

Mandaris AG
Chamerstrasse 174
CH-6300 Zug
Tel. +41 41 500 01 15

Mandaris Group (Malta)
Ltd.
Forni Complex 1E, Level 2,
Pinto Wharf,
Valletta Waterfront
Floriana, FRN 1913
Malta
Tel. +356 2779 1900



The Author:

Dominik Wasmer

MLaw, TEP, DAS Compliance Management (HSLU)
CAS Datenschutz (Universität Zürich)

Vice President, Legal & Compliance Officer

dominik.wasmer@mandaris.com

Phone: +41 61 285 17 17