STREICHENBERG

Zürich, August 2023

Vermögensverwalter und das revidierte Datenschutzgesetz – Beschränkte Auswirkungen infolge gesetzlich vorgesehener Datenbearbeitung

(Ein Leitfaden für Praktiker im Finanzdienstleistungssektor verfasst von Alexander Rabian, Melanie Käser und Mathias Stauffacher)

Datenbearbeitung aufgrund gesetzlicher Vorgabe

War unter dem bisherigen DSG die Bearbeitung von Personendaten aufgrund gesetzlicher Pflicht ein allgemeiner Rechtfertigungsgrund für die Bearbeitung von Personendaten (Art. 27 Abs. 1 aDSG), so verlangt das auf den 1. September 2023 in Kraft getretene revidierte Datenschutzgesetz (revDSG) in einigen Punkten eine differenziertere Betrachtungsweise.

Die für Vermögensverwalter wesentlichen gesetzlichen Vorgaben zur Bearbeitung von Daten über Kunden finden sich in folgenden Finanzmarktaufsichtsgesetzen (nach Art. 3 Abs. 1 FINMAG):

- Finanzdienstleistungsgesetz vom 15. Juni 2018 (FIDLEG)
- Geldwäschereigesetz vom 10. Oktober 1997 (GwG)
- Finanzinstitutsgesetz vom 15. Juni 2018 (FINIG)
- Kollektivanlagengesetz vom 23.6.2006 (KAG)
- Finanzmarktinfrastrukturgesetz vom 19. Juni 2015 (FINFRAG)

Zu all diesen Bundesgesetzen im formellen Sinn gibt es Ausführungsverordnungen (des Bundesrats, teilweise auch der Eidgenössischen Finanzmarktaufsicht FINMA), welche ebenfalls gesetzliche Grundlagen für die Bearbeitung von Personendaten darstellen.

Von den genannten Gesetzen haben das GwG und das FIDLEG die am weitesten reichenden Vorgaben zur Bearbeitung von Personendaten über «Kunden» in einem weit gefassten Sinn, d.h. Vertragsparteien und mit diesen in Beziehung stehenden Personen (z.B. wirtschaftlich Berechtigte / Kontrollinhaber, Vertreter und andere nahestehende oder geschäftlich oder persönlich verbundene Personen).

Auch für die Bearbeitung von Personendaten über Mitarbeitende des eigenen Unternehmens bestehen finanzmarktrechtliche (z.B. «Gewähr für eine einwandfreie

Streichenberg und Partner
Stockerstrasse 38
8002 Zürich
Schweiz
T. +41 44 208 2525
www.streichenberg.ch

Geschäftstätigkeit»), aber auch arbeits- und sozialversicherungsrechtliche Vorgaben.

Risikobasierte Regulierung

Das schweizerische Finanzmarktaufsichtsrecht ist u.a. dadurch gekennzeichnet, dass es für viele regulatorische Bereiche einen sogenannten «risikobasierten Ansatz» vorgibt. Dieses Grundprinzip ist auch zu beachten, wenn es darum geht zu bestimmen, welche Personendaten aufgrund gesetzlicher Vorgaben durch einen Anlageberater / Vermögensverwalter zu bearbeiten sind.

Das Gesetz (z.B. das GwG und dessen Ausführungsbestimmungen wie z.B. die GwV-FINMA) legt bei einer risikobasierten Regulierung nicht abschliessend fest, welche Personendaten bearbeitet werden müssen/dürfen. Das Gesetz verankert Prinzipien (wie z.B. das «Know your Customer»-Prinzip) und legt fest, dass das regulierte Finanzinstitut alles Notwendige (darunter auch die Bearbeitung von Personendaten) vorzukehren hat, dass sich vom Gesetz als unerlaubt oder unerwünscht erklärte Sachverhalte nicht verwirklichen. Das regulierte Finanzinstitut hat die durch ihre (bewilligte) Geschäftstätigkeit generierten Risiken unerlaubten oder unerwünschten Verhaltens zu erkennen, systematisch zu erfassen und zu steuern, d.h. effektives Risikomanagement zu betreiben.

Es lässt sich damit aufgrund der abstrakt gefassten Gesetze nicht abschliessend bestimmen, welche Personendaten der Kunden, Vertragspartner, Mitarbeitenden und Dienstleistern ein reguliertes Finanzinstitut bzw. ein regulierter Finanzintermediär zu bearbeiten hat, um den gesetzlichen Pflichten nachzukommen. Die Gesetze schreiben diesbezüglich auch keine «Maximalwerte» der zu bearbeitenden Personendaten, sondern legen – wenn überhaupt – regulatorische Mindeststandards fest.

Aufgrund der risikobasierten Regulierung muss jeder Finanzdienstleister u.a. für sich selbst festlegen, welche Personendaten er bearbeiten will, damit er den gesetzlichen Vorgaben genügt. Er hat dabei erhebliche Ermessenspielräume.

Von der FINMA bewilligte Vermögensverwalter haben über ein ausgebautes Weisungswesen zu verfügen, das von den Aufsichtsträgern (FINMA und Aufsichtsorganisationen) zu genehmigen ist und den eingesetzten Prüfgesellschaften periodisch auf seine zweckmässige Ausgestaltung im Hinblick auf die Erfüllung der gesetzlichen Vorgaben geprüft wird. Geprüft wird dabei nicht das Überschreiten gesetzlicher Vorgaben zur Erfassung, Messung und Steuerung von Risiken, sondern vielmehr das Unterschreiten. Gegenstand des Weisungswesens hat auch ein dem Umfang und der Komplexität des Geschäftsbetriebs sowie den durch den Geschäftsbetrieb generierten Risiken für Anleger und insbesondere auch für die Integrität und den Ruf des Finanzplatzes angemessenes Internes Kontrollsystem («IKS») zu sein. Auch die Führung eines solchen IKS verlangt die Bearbeitung von Personendaten über Kunden, Organe, Mitarbeitende aber auch über Mitarbeitende in Schlüsselfunktionen bei Outsourcing-Partnern und sogar bei Lieferanten.

Der bewilligte Vermögensverwalter, seine mit der Geschäftsführung befassten Organe, Mitarbeitenden und externe Hilfsperson müssen stets Gewähr für eine einwandfreie Geschäftstätigkeit bieten und über einen guten Ruf verfügen. Am Unternehmen beteiligte Personen müssen gewährleisten, dass sie keinen schädlichen Einfluss auf das Gewährserfordernis ausüben. Das Gewährserfordernis verlangt die Bearbeitung von Personendaten über Mitarbeitende in einem über den Rahmen bei Unternehmen ohne entsprechendes, gesetzliches Gewährserfordernis hinausgehenden Umfang. Der genaue Rahmen muss der bewilligte Vermögensverwalter im Anwendung des risikobasierten Ansatzes festlegen. Über Mitarbeitende, die Kunden betreuen, sind zudem Personendaten über deren hinreichende Gesetzeskenntnisse und Fachwissen zu bearbeiten.

Selbst bei der Benutzung von in Erfüllung der gesetzlichen Pflichten erhobenen und damit bearbeiteten Personendaten zu Marketingzwecken dürfte sich bei Anlageberatern und Vermögensverwaltern die entsprechende Datenbearbeitung auf gesetzliche Vorgaben abstützen lassen. Mit Bezug auf das Angebot von Finanzinstrumenten legt das FIDLEG nämlich fest, dass im Rahmen der vorzunehmenden Kundensegmentierung (einschliesslich eines allfälligen Opting-in oder Opting-out), der Wahrnehmung der Informationspflichten sowie der Erfüllung der Voraussetzungen für das Anbieten von Finanzinstrumenten Personendaten von möglichen und effektiven Anlegern bearbeitet werden.

Zusammengefasst lässt sich damit festhalten, dass die riskobasierte Regulierung der Finanzdienstleistungen den Finanzinstituten und Finanzintermediären weitreichende Eigenkompetenz zu Festlegungen dazu einräumt, welche Personendaten bearbeitet werden müssen oder sollen. Der risikobasierte Regulierungsansatz schreibt auch die Bearbeitung von besonders schützenswerten Personendaten (vielleicht mit Ausnahme von sehr spezifischen Gesundheitsdaten) vor und sieht auch die Bearbeitung von Persönlichkeitsprofilen (insbesondere von Kunden, Mitarbeitenden, Schlüsselpersonen bei Outsourcing-Partnern) mit besonders schützenswerten Personendaten (z.B. Informationen über politische Aktivitäten im Rahmen der Regeln zum Umgang mit politisch exponierten Personen) vor.

Anwendbarkeit der Grundprinzipien des revDSG

Die folgenden grundlegenden gesetzlichen Prinzipien zum Datenschutz gelten auch, wenn der Datenbearbeiter für die Datenbearbeitung den Rechtfertigungsgrund der gesetzlich vorgesehenen Datenbearbeitung hat:

- Rechtmässigkeitsprinzip (Art. 6 Abs. 1 revDSG): Bei einem bewilligten Vermögensverwalter durch weitreichende gesetzliche Grundlagen sowie durch überwiegende private oder öffentliche Interessen in einem weiten Rahmen erfüllt;
- Zweckmässigkeitsprinzip (Art. 6 Abs. 1 revDSG): Die Daten dürfen ohne die Einhaltung weitergehender Bestimmungen des revDSG nur zu den gesetzlichen Zwecken verwendet werden. Diese reichen allerdings sehr weit.
- Verhältnismässigkeitsprinzip (Art. 6 Abs. 2 revDSG): Die Daten dürfen nur soweit nötig für den vorgesehenen Zweck bearbeitet werden. Die risikoba-

sierte Regulierung setzt hier einen weiten Rahmen und gibt dem Vermögensverwalter einen eigenen Ermessensrahmen.

- Treu und Glauben (Art. 6 Abs. 2 revDSG): Die Erfüllung gesetzlicher Vorgaben ist stets eine Datenbearbeitung nach Treu und Glauben. Dieser Grundsatz limitiert die Datenbearbeitung auf eine sachgerechte Anwendung eines risikobasierten Ansatzes, erlaubt dabei aber weitreichendes Eigenermessen des Datenbearbeiters;
- Transparenzgebot / Informationspflicht (Art. 6 Abs. 3 revDSG / Art. 19 ff. revDSG): Die bearbeiteten Daten werden für einen erkennbaren Zweck beschafft. Dieses Erfordernis wird mit einfacher Information von Kunden, Anlegern etc. erfüllt.
- Datenschutzfreundliche Voreinstellungen (Art. 7 revDSG; «Privacy by Design/Default»): Dieser Grundsatz wird durch die anwendbaren Aufsichtsgesetze in einem sehr weiten Rahmen relativiert. Oft stehen datenschutzfreundliche Voreinstellungen zu den Zielen und Zwecken der Regulierung in Widerspruch;
- Datenrichtigkeit (Art. 6 Abs. 5 revDSG): Die anwendbaren Aufsichtsgesetze sehen vor, dass der bewilligte Vermögensverwalter von der Richtigkeit der bearbeiteten Personendaten überzeugt ist. Die vorsätzliche oder fahrlässige Bearbeitung von Personendaten tangiert das Erfordernis der Gewähr für eine einwandfreie Geschäftstätigkeit. Teilweise sehen Finanzmarktaufsichtsgesetze die risikobasierte Überprüfung von Aktualität und Richtigkeit bearbeiteter Personendaten vor;
- Datensicherheit (Art. 8 revDSG): Das Weisungswesen hat angemessene Vorgaben zur Datensicherheit vorzusehen.

Verzeichnis der Bearbeitungstätigkeiten (Art. 12 revDSG):

Welche Bearbeitungstätigkeiten mit Bezug auf Personendaten ein Vermögensverwalter vornimmt, ergibt sich aus seinem Weisungswesen. Dieses hat die Datenbearbeitungen aufzuführen, ausser wenn das Unternehmen weniger als 250 Personen beschäftigt und nicht besonders schützenswerte Personendaten bearbeitet werden oder ein Profiling mit hohem Risiko durchgeführt wird.

Da Vermögensverwalter im Rahmen ihrer gesetzlichen Pflichten, insbesondere nach dem GwG, regelmässig besonders schützenswerte Personendaten bearbeiten und unter Umständen sogar Profilierung mit hohem Risiko durchführen, ist es beim jetzigen Kenntnistand empfehlenswert, ein Verzeichnis der Datenbearbeitungstätigkeiten zu führen.

Es ist nicht notwendig, dass bei elektronischer Bearbeitung von Personendaten im Weisungswesen detaillierte und akribische Listen über jedes bearbeitete Datenmerkmal geführt werden («Listen mit Datenfeldern»). Gerade bei der Umsetzung eines risikobasierten Ansatzes bei der Bearbeitung von Personendaten zu regulatorischen Zwecken werden ja auch nicht schematisch über alle Kunden, wirtschaftlich Berechtigte / Begünstigte oder Vertreter identische Datenmerkmale bearbeitet. Auch muss das Verzeichnis der Bearbeitungstätigkeiten kein separates, vom Weisungswesen getrenntes Dokument sein, sondern ist zweckmässigerweise ins Weisungswesen integriert.

Datenbekanntgabe ins Ausland (Art. 16ff. revDSG)

Die Datenbekanntgabe ins Ausland ist nicht per se untersagt. Die Datenbearbeitung auf im Ausland gelegenen Servern und Datenspeichern ist damit für Vermögensverwalter weiterhin möglich.

In Anhang I zur revidierten Datenschutzverordnung (revDSV) sind die Staaten und Territorien aufgeführt, die nach der Beurteilung des Verordnungsgebers ein angemessenes Datenschutzniveau aufweisen. Neben den EWR-Staaten wird auch zahlreichen anderen Staaten ein angemessenes Datenschutzniveau attestiert. Nicht aber den U.S. Die Datenbearbeitung auf in den USA stehenden Servern ist somit nur eingeschränkt erlaubt.

Informationspflicht bei der Beschaffung von Personendaten (Art. 19ff. revDSG)

Zur Transparenz der Datenbearbeitung gehört grundsätzlich auch die Pflicht, die betroffene Person angemessen über die Bearbeitung von Personendaten zu informieren. Art. 19 revDSG knüpft für die Informationspflicht bei der Datenbeschaffung an. Vermögensverwalter beschaffen Informationen über Kunden etc. im Rahmen ihrer gesetzlichen Pflichten (insbesondere nach dem GwG) nicht nur beim Kunden, sondern nutzen auch andere Datenquellen (z.B. zur Plausibilisierung der beim Kunden erhobenen Daten). Dass diejenigen Daten, die der Vermögensverwalter vom Kunden direkt erhält, bearbeitet werden, ergibt sich ja von selbst.

Nach Art. 20 revDSG entfällt die Informationspflicht über die Datenbeschaffung soweit entsprechende Datenbearbeitungen gesetzlich vorgesehen sind. Dies gilt insbesondere auch für die Bearbeitung von Kundendaten und Personendaten über Mitarbeitende. Mit Bezug auf Kunden entfällt die Informationspflicht in weiten Teilen auch infolge des Berufsgeheimnisses. Auch wenn die Personendaten in nach Art. 16 revDSG zulässiger Weise ins Ausland bekanntgegeben werden (z.B. dort auf einem Server gespeichert werden), sind die betroffenen Personen darüber nicht spezifisch zu informieren.

Eine umfassende und detaillierte Datenschutzerklärung gegenüber Kunden und Mitarbeitenden ist damit für Vermögensverwalter, die ein traditionell ausgerichtetes Geschäft betreiben, nicht notwendig. Es ist aber gleichwohl im Rahmen der allgemeinen Transparenzvorgaben sinnvoll, Kunden im Rahmen der allgemeinen Informationspflichten über die weitreichende, gesetzlich vorgesehene Datenbearbeitung zu informieren. Wichtig ist, dass der Vermögensverwalter in dieser Information festhält, dass sein Unternehmen der Datenbearbeiter ist.

Wer als Vermögensverwalter aber in weitergehendem Umfang Personendaten bearbeitet, wie z.B. Personendaten von Stellenbewerbern, ist gesetzlich verpflichtet, diese Personen über Art, Umfang und Dauer der Datenbearbeitung zu informieren.

Weitergehende Informationspflichten haben aber auch insbesondere diejenigen Vermögensverwalter, die ein stark oder bloss teilweise auf eine Web-basierte Kommunikation und Dienstleistungserbringung abgestütztes Geschäftsmodell betreiben. Die Einbindung von Web-Applikationen in die Vermögensverwaltung verlangt

die Bearbeitung von Personendaten (z.B. elektronische Aufzeichnungen über die Nutzung der Web-Applikation), die nicht durch gesetzliche Vorgaben abgedeckt ist, sondern sich aus dem spezifischen Geschäftsmodell und den entsprechenden vertraglichen Vereinbarungen ergeben. Solche Vermögensverwalter bearbeiten Personendaten in einem über die gesetzlichen Vorgaben hinausgehenden Rahmen und haben entsprechend weitergehende Informationspflichten, die eine umfassende Datenschutzerklärung notwendig machen.

Unveränderte Weitergeltung haben die Bestimmungen betreffend den Einsatz von sogenannten «Cookies» auf Websites. Hier gilt weiterhin eine Informationspflicht. Ein Zustimmungserfordernis besteht nach dem revDSG nicht.

Auftragsdatenbearbeitung für Banken

Im Rahmen der Delegation von formellen Pflichten nach dem GwG bearbeiten bewilligte Vermögensverwalter regelmässig Personendaten auch im Auftrag der «delegierenden» Banken («Delegation» nach VSB). Dabei liegt eine Auftragsbearbeitung von Personendaten vor, die gleichzeitig eine eigene, gesetzlich vorgegebene Datenbearbeitung des Vermögensverwalters darstellt.

Da es sich hier über deckungsgleiche Bearbeitungen von Personendaten handelt, die der Vermögensverwalter nach gesetzlichen Vorgaben selbst auch bearbeiten muss, sind beim Vermögensverwalter keine besonderen Vorkehren für die Auftragsdatenbearbeitungen notwendig.

Bearbeitet der Vermögensverwalter Personendaten und leitet diese an die auftraggebenden Banken weiter, was bei der «Delegation» der formellen Sorgfaltspflichten nach der VSB, aber auch bei weiteren Datenbearbeitungen nach dem Weg (z.B. Erarbeitung des KYC) der Normallfall ist, so muss der betroffene Kunde entsprechend informiert werden. Dies kann im Rahmen der allgemeinen Kundeninformation in genereller Weise erfolgen.

Datenbekanntgabe an Dritte, insbesondere Auftragsdatenbearbeiter

Lässt der Vermögensverwalter Personendaten durch Dritte im In- oder Ausland bearbeiten, so stellt er in den entsprechenden Verträgen sicher, dass die Datenbearbeitung durch den Auftragsbearbeiter nur in einer Weise erfolgt, die für den Vermögensverwalter geltenden Regeln entspricht. Dazu sollten die Verträge geeignete Datenschutzklauseln enthalten.

Insbesondere hat der Vermögensverwalter durch geeignete Klauseln auch sicherzustellen, dass der Auftragsbearbeiter die nötigen Vorkehren zum Schutz des Berufsgeheimnisses getroffen hat. Es gelten hier die aufsichtsrechtlichen Vorgaben der FINMA zur Auslagerung.

Informationspflicht bei automatisierter Einzelentscheidung (Art. 21 revDSG)

Risikoklassierungen nach GwG oder bezüglich der Anlagetätigkeiten nach FIDLEG (Einstufung aufgrund von Fragebogen) stellen auch dann keine «automatisierten Einzelfallentscheidungen» im Sinne des revDSG dar, wenn IT-Systeme dazu Resultate liefern. Aufgrund regulatorischer Vorgaben besteht eine persönliche Verantwortung der zuständigen Personen zur Festlegung entsprechender Entscheidungen. Die eingesetzten «Automaten» sind bloss Hilfsmittel.

Datenschutz-Folgenabschätzung (Art. 22 revDSG)

Diese Pflicht entfällt, wenn die Datenbearbeitung aufgrund gesetzlicher Vorgabe erfolgt (Abs. 4).

Meldung von Verletzungen der Datensicherheit (Art. 24 revDSG) – Vorgehen nach FINMA-Mitteilung

Vermögensverwalter üben eine beaufsichtigte Tätigkeit aus. Die gesetzlichen Vorgaben zum Umgang mit Verletzungen der Datensicherheit im revDSG sind daher teilweise sehr stark durch die aufsichtsrechtlichen Vorgaben der Bewilligungsbehörde FINMA übersteuert. Insbesondere bei Cyber-Attacken auf sog. kritische Aktiven (dazu gehören auch IT-Systeme) sind die Vorgaben der FINMA-Aufsichtsmitteilung 05/2020[1] einzuhalten. Die primär zu orientierende Stelle ist hier die AO. Im laufenden Bewilligungsverfahren ist auch die FINMA zu orientieren.

«Bloss» interne Verletzungen der Datensicherheit (z.B. Zugriff auf Kundendaten durch dazu nicht befugte Mitarbeitende) müssen dem EDÖB gemeldet werden, wenn dies voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Dieses hohe Risiko besteht allerdings in der Praxis nur dann, wenn ein «Datenabfluss nach aussen» droht. In solchen Fällen ist jedoch ohnehin primär der zuständige Aufsichtsträger zu informieren. Eine Information des EDÖB ist mit dem Aufsichtsträger abzustimmen.

Die Vorgehensweise ist in den Grundzügen im Weisungswesen zu regeln.

Auskunftsrecht (Art. 25 ff. revDSG)

Hier geht es namentlich um das Verhältnis des datenschutzrechtlichen Auskunftsrechts zu Auskunfts- und Rechenschaftspflichten nach dem FIDLEG. Aufgrund des im FINIG verankerten Berufsgeheimnisses dürfen Personendaten nicht an andere Personen als die jeweilige Geheimnisherrin bekanntgegeben werden, soweit keine sonderrechtlichen Bekanntgabepflichten bestehen. Die Aufsichtsgesetze sehen zudem weitere Gründe für die Verweigerung, Einschränkung oder Verzögerung (Art. 26 Abs. 2 revDSG) der Auskunftserteilung vor. Dazu gehören Auskünfte über die

[1] https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf?sc_lang=de&hash=87CF9E3048AAF9E70606ABB74184D2EB

Erfüllung der Meldepflicht nach GwG und anderer aufsichtsrechtlicher Meldepflichten, Verschwiegenheitspflichten aufgrund behördlicher Anordnungen sowie das Verbot des tipping-off nach in- und ausländischer Rechtsordnung (z.B. auch in Steuersachen).

Vor dem Hintergrund dieser zahlreichen möglichen Beschränkungen des Auskunftsrechts, lässt sich aus guten Gründen darlegen, dass das FIDLEG bei der Anlageberatung und Vermögensverwaltung den Auskunftsrahmen festlegt. Bei finanzintermediären Tätigkeiten nach dem GwG ist die Verweigerung, Einschränkung oder bloss Verzögerung der Auskunft Folge des präventiv-strafprozessualen Charakters des GwG. Das Auskunftsrecht darf nicht genutzt werden, die Ziele des GwG (Prävention und Bekämpfung von Geldwäscherei und Terrorismusfinanzierung) zu gefährden. Im Zweifelsfall hat der bewilligte Vermögensverwalter die Auskunft nach dem revDSG einzuschränken oder gar zu verweigern. Darüber ist im Einzelfall zu entscheiden.

Einschränkungen:

Die vorstehenden Ausführungen gelten nur eingeschränkt, wenn

A. Daten betreffend natürliche Personen für andere Zwecke als die Erbringung von Dienstleistungen der Vermögensverwaltung, der Anlageberatung, der Entgegennahme und Weiterleitung von Aufträgen über Finanzinstrumente sowie das Angebot von Finanzinstrumenten (z.B. im Rahmen einer Online-Registrierung für einen Newsletter für Nicht-Kunden) erhoben werden;

B. die Datenbearbeitung nicht nur in den Geltungsbereich des revDSG, sondern auch in denjenigen des Datenschutzrechts der Europäischen Union, insbesondere der DSGVO fällt. Hierzu ist allerdings festzuhalten, dass nach hiesiger Auffassung die Annahme und die Betreuung von im EWR ansässigen Kunden im Rahmen der passiven Dienstleistungsfreiheit (Erwägungsgründe 111 Satz 2 MiFID II und 43 Satz 2 MiFIR) nicht zu einer Anwendbarkeit der DSGVO führt.

***