DER GELDWÄSCHER IN DER DATENSAMMLUNG

Sabine Kilgus / Cordula Niklaus / Caroline Walser Kessel

Prof. Dr. Sabine Kilgus, LL.M., Rechtsanwältin, Titularprofessorin an der Universität St. Gallen, Präsidentin der Selbstregulierungsorganisation zur Bekämpfung der Geldwäscherei (SRO) von TREUHAND|SUISSE
Dufourstrasse 181, 8008 Zürich, Schweiz; sabine.kilgus@losinger.law, sabine.kilgus@unisg.ch, www.losinger.law

Fürsprecherin Cordula Niklaus, LL.M., Rechtsanwältin, Co-Präsidentin Datenschutzforum Schweiz (DSF)
Schifflände 5, 8001 Zürich, Schweiz; cniklaus@niclaw.ch, www.niclaw.ch

Dr. Caroline Walser Kessel, Rechtsanwältin, Präsidentin der Fachkommission der SRO Polyreg
Bellariarain 6, 8038 Zürich, Schweiz; caroline.walser@vtxmail.ch, www.walserlaw.ch

Schlagworte: ***Geldwäschereibekämpfung, Datenschutz, Persönlichkeitsrechte, Meldepflicht, Selbstregulierung Sitzgesellschaft, Transparenz, Treu und Glauben, wirtschaftlich berechtigte Person***

Abstract: *Das revidierte Datenschutzgesetz (DSG) und das mehrfach revidierte Geldwäschereigesetz (GwG) stehen in einem Spannungsfeld. Während unter dem GwG umfangreiche Daten von Kunden und hinter den Kunden stehenden wirtschaftlich berechtigten Personen erfasst und strukturiert werden müssen, ohne dass diese über alles informiert werden, sieht das DSG grundsätzlich Transparenz bezüglich der eigenen Daten und die Limitierung der Datenerfassung unter dem Gesichtspunkt der Zweckmässigkeit und Verhältnismässigkeit vor. Obwohl das GwG grosse Bereiche des DSG derogiert, sind Finanzintermediäre auch unter dem DSG gehalten, dessen Grundsätze einzuhalten und insbesondere die organisatorischen und sicherheitstechnischen Aspekte zu wahren. Dazu eröffnete das DSG die Möglichkeit, mittels Selbstregulierung der Branche, transparente Verhaltenskodices zu schaffen und durch den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten prüfen zu lassen.*

1. Einleitung

Am 1. Januar 2023 tritt in der Schweiz das revidierte Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz GwG)[1], zusammen mit den dazugehörenden Verordnungen (Geldwäschereiverordnung GwV[2] und Geldwäschereiverordnung-FINMA GwV-FINMA[3]) in Kraft. Per 1. September 2023 wird zudem das revidierte Datenschutzgesetz (DSG)[4] zusammen mit der dazugehörenden Datenschutzverordnung (VDSG, neu DSV)[5] in Kraft treten. Dies führt dazu, dass das GwG auf den 1. September 2023 bereits wieder angepasst werden musste.[6]

Diese beiden Gesetzesnovellen bilden den Anlass zu diesem Beitrag. Im Vordergrund steht das Spannungsfeld zwischen dem Bedarf an der Sicherung und Dokumentation von Daten im Rahmen der erforderlichen Sorgfalt bei Finanzgeschäften, bei der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und qualifizierten Steuerdelikten gemäss GwG, GwV und GwV-FINMA auf der einen Seite, und dem grösstmöglichen Persönlichkeitsschutz und der Transparenz der von Datenbearbeitungen betroffenen Personen gemäss DSG und VDSG auf der andern Seite. Die Thematik erhält zusätzliche Brisanz einerseits dadurch, dass nicht nur Daten des Vertragspartners selbst sowie der dahinterstehenden wirtschaftlich berechtigten Personen und Geschäftsbeziehungen erhoben werden müssen, sondern auch, dass diese Daten Gegenstand von weitreichenden

1 SR 955
2 SR 955.01
3 SR 955.033.0
4 SR 235.1
5 SR 235.11
6 In der offiziellen Sammlung des Bundesrechts ist die Version des GwG, die auf den 1. September 2023 in Kraft treten wird, bereits online verfügbar. https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/de.

Datentransfers an nationale Behörden und gegebenenfalls an ausländische Behörden im Rahmen der Amtshilfe bilden.

Besonderes Augenmerk der letzten Gesetzesnovellen des GwG liegt dabei auf der Kenntnis der an Finanztransaktionen beteiligten juristischen Personen. Gefordert wird grösstmögliche Transparenz hinsichtlich der Eigentümer- und Beherrschungsverhältnisse an diesen juristischen Personen, und falls zutreffend, auch bezüglich allfälliger Strukturen, die durch mehrere juristische Personen gebildet werden. Diese Transparenzanforderungen zielen darauf ab, zu wissen, welche *natürliche* Person schliesslich hinter einer juristischen Person, Gesellschaft oder Struktur steht (sog. «ultimate beneficial owner»). Diese Person ist soweit als möglich nicht nur zu kennen, sondern zu identifizieren. Ausgenommen sind einzig juristische Personen, deren Beteiligungstitel an einer Börse kotiert sind. Diese Transparenzanforderungen widersprechen nicht nur fundamental der gesellschaftsrechtlichen Konzeption der Aktiengesellschaft («Société anonyme») und dem Konzept von Inhaberaktien, sondern auch den grundsätzlichen Anforderungen der datenschutzrechtlichen Gesetzgebung und dem Recht auf Privatsphäre.

Damit ergeben sich Zielkonflikte – maximale Transparenz versus Recht auf Privatsphäre und Kontrolle über die eigenen Daten –, die sich nicht konzeptionell, sondern, wenn überhaupt, nur anhand von Interessenabwägungen zwischen den Transparenz verlangenden Stellen und der Wahrung verfassungsmässiger Rechte der von den Transparenzbestimmungen Betroffenen lösen lassen.

Konkret steht im Rahmen der verschärften Geldwäschereibestimmungen Folgendes zur Debatte: Prüfung und Abklärung betreffend Personen, die hinter juristischen Personen stehen, Abklärungen bezüglich der Provenienz ihres Vermögens («source of wealth») und bezüglich der aktuellen Tätigkeiten und Finanzflüsse («source of funds») anhand allgemein zugänglicher öffentlicher Quellen und Daten, sowie Erkundigungen direkt bei den Kunden sowie bei vertrauenswürdigen Personen und Datenbanken, welche mit dem im Datenschutzgesetz definierten Persönlichkeitsschutz und der informationellen Selbstbestimmung kollidieren können. Grundsätzlich gilt das GwG zwar als Rechtfertigungsgrund für Datenerhebungen und Datenbearbeitungen, indem bei einer korrekten Umsetzung der Pflichten gemäss Art. 3–9 GwG keine widerrechtliche Persönlichkeits- oder Datenschutzverletzung vorliegt. Es müssen jedoch dabei auch indirekte Wirkungen beachtet werden, wie bspw. Auskunftsrecht und Rechtschutz der durch die Untersuchungen und Abklärungen betroffenen Dritten (bspw. Vertragspartner von Kunden und/oder wirtschaftlich berechtigten Personen oder diesen nahestehenden Personen), oder generell Zugang zu den erhobenen Daten und nach der Meldung erfolgten Datenweitergabe ins Ausland. Dadurch, dass immer mehr und immer detailliertere Daten erhoben werden müssen, namentlich was die Abklärungen betr. Geschäftstätigkeit und Herkunft des Vermögens betrifft, werden die Informationen immer aussagekräftiger; damit wird es aus der Optik des Persönlichkeitsschutzes auch gefährlicher, wenn sie in falsche Hände geraten. Besonderes Augenmerk ist dabei der in Angriff genommenen Revision von Empfehlung 24 der «Groupe d'action financière» (GAFI)[7] zu widmen, wonach die Staaten verpflichtet werden sollen, ein zentrales Register der wirtschaftlich Berechtigten an allen juristischen Personen, operativen Gesellschaften und Sitzgesellschaften, zu errichten. Dies vor dem Hintergrund, dass das revidierte Datenschutzgesetz – wie die DSGVO – den Schutz der juristischen Person aufgegeben hat.

2. Wesentliche Aspekte des GwG und des nGwG

2.1. Transparenz bezüglich Personen

Das Geldwäschereigesetz regelt seit seinen Anfängen die Anforderungen an die Anwendung der notwendigen Sorgfaltspflichten bezüglich Identifikation des Vertragspartners und Feststellung des wirtschaftlich Berechtigten (Art. 3 und 4 GwG). Mit jeder Gesetzesrevision wurden die Anforderungen verschärft und die Ausarbei-

[7] Englisch: Financial Action Task Force (FATF) mit Sitz in Paris bei der OECD.

tung verfeinert, indem bspw. tiefer gehende Abklärungen, namentlich bezüglich Beherrschungsverhältnisse nicht nur bei Sitzgesellschaften, sondern auch hinsichtlich der hinter operativen Gesellschaften stehenden natürlichen Personen, vorzunehmen sind. Das hängt mit dem über die Jahre erweiterten Zweck des GwG zusammen. Zweck des GwG ist heute nicht mehr nur die Bekämpfung der Geldwäscherei i.S.v. Art. 305bis StGB[8], sondern auch die Bekämpfung von Terrorismusfinanzierung i.S.v. Art. 260^{quinquies} StGB (und damit auch von kriminellen Organisationen i.S.v. Art. 260ter StGB) und der qualifizierten Steuerhinterziehung (Art. 305bis Abs. 1bis StGB). Damit ändert sich auch der Charakter und der Zweck der eingeholten Informationen: Da Terrorismusfinanzierung auch aus legalen (und versteuerten) Mitteln erfolgen kann, ist der Fokus vermehrt auf den Kontext der Geschäftsbeziehung, d.h. der Herkunft des Vermögens und die Finanzflüsse, zu legen. Ähnliches gilt für den Kampf gegen Steuerhinterziehung. Auch diesbezüglich sind detaillierte Kenntnisse über Strukturen und Finanzflüsse nötig, um allfällig strafbares Verhalten eruieren zu können.

Eine stärkere Kontextualisierung und gegebenenfalls die Erstellung eines eigentlichen Kundenprofils verlangt nicht zuletzt der risikobasierte Aufsichtsansatz, wonach die Kundenbeziehungen in Geschäftsbeziehungen mit «normalen» und solche mit «erhöhten» Risiken einzuteilen sind.

Schliesslich fordert Art. 4 nGwG, der am 1. Januar 2023 in Kraft tritt, nicht nur die Feststellung der wirtschaftlich berechtigten Person mit den nach den Umständen gebotenen Sorgfalt, «sondern eine Überprüfung deren Identität, um sich zu vergewissern, wer die wirtschaftlich berechtigte Person ist.» Damit einhergehend wird verlangt, dass Nachidentifikationen vorzunehmen sind, wenn Zweifel an der Richtigkeit der Angaben bestehen, bspw. wenn sich diese aufgrund veränderter Verhältnisse ändern (Art. 5 und 6 GwG) und die erhaltenen Daten periodisch und risikoadäquat zu aktualisieren.

2.2. Transparenz bezüglich Herkunft des Vermögens und Zweck der Geschäftsbeziehung

Art. 6 GwG verlangt eine eigentliche Provenienzforschung hinsichtlich der Herkunft des Vermögens («source of wealth») und damit zusammenhängend des Sinns und Zwecks der gewünschten Geschäftsbeziehung («source of funds»), die überdies die Klassifizierung in Geschäftsbeziehungen (und Transaktionen) mit normalem Risiko und solche mit erhöhtem Risiko ermöglichen. Nur wenn diese engmaschig beobachtet werden, können ungewöhnliche Transaktionen, ungewöhnliche Geldflüsse und generell die Risikoeinstufung der Geschäftsbeziehung unter dem Gesichtspunkt des Risikos für Geldwäscherei, aber auch für Terrorismusfinanzierung oder Steuerhinterziehung ermittelt oder erkannt werden. Die so ermittelten Daten über die Kundenstruktur können als eigentliche Persönlichkeitsprofile i.S.v. des DSG bezeichnet werden.[9]

2.3. Umfassende Informationspflichten bezüglich der gesammelten Daten

Dass diese Daten sorgfältig, richtig, aber umfassend ermittelt und von den Finanzintermediären gespeichert, verwaltet und periodisch aktualisiert werden müssen, ist konsequent, stützt sich doch die Meldepflicht (Art. 9 GwG) und auch das Melderecht (Art. 305ter Abs. 2 StGB) bei Verdacht auf Geldwäscherei, Terrorismusfinanzierung oder schweres Steuerdelikt auf eben diese Daten, die ihrerseits im Rahmen der Meldung an die Meldestelle zur Bekämpfung der Geldwäscherei (MROS oder Meldestelle) weitergeleitet werden (Art. 9 GwG oder Art. 305ter Abs. 2 StGB). Diesfalls sind die Finanzintermediäre gehalten, die Daten, die die Meldung begründen, in einem separaten Ordner zu halten (Art. 34 Abs. 1 GwG). Dieser ist während fünf Jahren zu führen und anschliessend zu vernichten (Art. 34 Abs. 4 GwG).

---

[8] Schweizerisches Strafgesetzbuch, SR 311.0. Unter Geldwäscherei werden dabei Handlungen und Unterlassungen verstanden, die dazu dienen, dass Vermögenswerte, die aus einer schweren Straftat, einem Verbrechen i.S.v. Art. 10 StGB, stammen, nicht mehr als solche erkennbar sind.

[9] Caroline Gaul/Michael Isler/David Vasella, in: Hsu Peter/Flühmann Daniel (Hrsg.), Basler Kommentar zum GwG, Basel 2021, N 14 zu Art. 33 GwG (nachfolgend zit. BSK GwG-AUTOR).

Die MROS hat dann die Aufgabe zu entscheiden, ob aufgrund der Daten ein genügender Anfangsverdacht besteht, so dass die Daten an die Strafuntersuchungsbehörden weitergeleitet werden müssen. Andernfalls werden die Daten der Meldung während zehn Jahren gespeichert (Art. 28 Abs. 1 MGwV)[10], damit sie zur Verfügung stehen, falls zu einem späteren Zeitpunkt ähnliche Meldungen bzw. Meldungen mit einem Bezug zu dieser ursprünglichen Meldung auftauchen oder aber eine ausländische Behörde im Kampf gegen Geldwäscherei auf dem Weg der Amtshilfe von der MROS Informationen verlangen kann.

Kommt es zu einer Meldung, darf der Kunde oder Dritte, namentlich allfällige wirtschaftlich Berechtigte, nicht über die erstattete Meldung informiert werden (Art. 10a nGwG). Das ändert sich erst, wenn die MROS oder später die Strafuntersuchungsbehörde mittels Verfügung eine Vermögenssperre anordnen und der Kunde entsprechend informiert werden darf (Art. 10a GwG).

Mit der Revision von 2021, die auf den 1. Januar 2023 in Kraft getreten ist, wird nun aber der Kreis der Personen, die über eine Meldung informiert werden dürfen, stark erweitert: Nicht nur, dass wie bis anhin andere Finanzintermediäre, die sich auch um das meldepflichtige Dossier gekümmert haben, informiert werden dürfen – typischerweise die meldende Bank, die den externen Vermögensverwalter über die Meldung informiert – vielmehr dürfen alle nationalen Behörden und Selbstregulierungs- bzw. Aufsichtsorganisationen und im Rahmen der konsolidierten Aufsicht (ausländische) Muttergesellschaften und deren Aufsichtsbehörden über die erfolgte Meldung informiert werden – alles mit dem Ziel, dass sich die Kenntnisse über die Geschäftsbeziehung und die involvierten Personen flächendeckend verbreiten (siehe unten 4.4.).

2.4. Aktionärsregister

Ein weiterer Schritt zur Verstärkung der Transparenz ist bereits weit fortgeschritten in der Vorbereitung. Art. 24 der Empfehlungen der GAFI sollen so ausgelegt werden, dass jedes Land ein Register zu führen hat, in dem die wirtschaftlich Berechtigten aller juristischen Personen, auch der operativen, nicht nur von Sitzgesellschaften, eingetragen werden. Es ist heute davon auszugehen, dass ein solches Register, das in einzelnen EU-Staaten schon besteht, wohl generell etabliert werden muss. Ungeachtet der Frage, ob ein solches Register zur Bekämpfung der Geldwäscherei wirklich notwendig ist, bleibt strittig, nicht zuletzt aus datenschutzrechtlichen Überlegungen, *wer* das Register führt bzw. führen soll, *wer* Einsicht und Zugriff hat bzw. haben soll und darf. Denn in diesem Register soll der «ultimate beneficial owner» eingetragen werden, also die natürliche(en) Person(en), die letztlich eine juristische Person oder Struktur kontrolliert. Ebenfalls zu Diskussionen Anlass gibt die Frage, ob es weiterhin Ausnahmen für kotierte Gesellschaften geben soll.

All diese Punkte verdienen es, unter dem Aspekt des Datenschutzes und im speziellen unter dem revidierten schweizerischen Datenschutzgesetz, beleuchtet zu werden, erklärt doch Art. 33 GwG schon bisher und auch unter dem revidierten DSG lapidar, dass sich die Bearbeitung von Personendaten nach dem Datenschutzgesetz richtet.

3. Wesentliche Aspekte des DSG

3.1. Grösstmöglicher Persönlichkeitsschutz bei der Datenbearbeitung

Im revidierten Datenschutzgesetz, welches per 1. September 2023 in Kraft treten wird, sind die bisherigen allgemeinen Grundsätze der Datenbearbeitung weiterhin zu beachten.[11] Es handelt sich insbesondere um die Rechtmässigkeit, die Transparenz, die Zweckmässigkeit, die Verhältnismässigkeit, die Richtigkeit der Daten sowie die Datensicherheit (vgl. dazu Art 6 nDSG). Im Unterschied zur DSGVO braucht es für die Daten-

[10] Verordnung über die Meldestelle für Geldwäscherei, SR 955.23.

[11] Der neue Wortlaut ist unter https://www.fedlex.admin.ch/eli/cc/2022/491/de abrufbar.

bearbeitung durch Private auch künftig grundsätzlich keine explizite Einwilligung oder eine Rechtfertigung, solange diese allgemeinen Grundsätze entsprechend berücksichtigt werden, die betroffene Person der Bearbeitung der Daten nicht explizit widerspricht und keine besonders schützenswerte Daten Dritten bekannt gegeben werden.[12]

3.2. Rechtmässigkeit, Verhältnismässigkeit und Zweckmässigkeit

Das revidierte Datenschutzgesetz hält in Art. 6 nDSG am etablierten Grundsatz fest, dass Personendaten rechtmässig bearbeitet werden müssen, was auch deren Beschaffung beinhaltet. Im Weiteren hat die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen, und die Bearbeitung muss verhältnismässig sein. *Das bedeutet, dass nur soviel Daten wie nötig und so wenig wie möglich beschafft und bearbeitet werden sollen*. Weiter dürfen Personendaten nur zu einem bestimmten Zweck beschafft werden, der gleichzeitig für die betroffene Person erkennbar sein muss, und die Daten dürfen nur so bearbeitet werden, dass es mit dem bestimmten Zweck vereinbar ist.

Wer Personendaten bearbeitet, ist sodann verpflichtet, sich über die Richtigkeit dieser Daten zu vergewissern. Es sind dabei alle angemessenen Massnahmen zu treffen, damit Daten berichtigt, gelöscht oder vernichtet werden, welche im Hinblick auf den Zweck der Beschaffung oder der Bearbeitung unrichtig oder unvollständig sind (vgl. insbesondere Art. 6 Ziff. 5 nDSG).

3.3. Datensicherheit

Wer Daten bearbeitet ist verpflichtet, mittels geeigneten technischen und organisatorischen Massnahmen sicherzustellen, dass die zwingenden Grundsätze bei der Datenbearbeitung eingehalten und umgesetzt werden können. Diese Massnahmen müssen dabei dem aktuellen Stand der Technik, der Art und dem Umfang der Bearbeitung sowie dem durch die Bearbeitung möglichen Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person entsprechen. Zudem müssen auch geeignete Voreinstellungen sicherstellen, dass die Bearbeitung auf das dem Bearbeitungszweck entsprechende Mindestmass beschränkt ist (vgl. Art. 7 nDSG).[13]

Sowohl der Verantwortliche wie auch der Auftragsbearbeiter sind zur Gewährleistung der Datensicherheit verpflichtet. Zudem müssen die getroffenen Massnahmen auch ermöglichen, allfällige Verletzungen der Datensicherheit zu vermeiden (vgl. Art. 8 nDSG). Es ist dabei zu beachten, dass nur diejenigen Personen Zugang zu den Daten haben, die diese auch für die Erfüllung ihrer Aufgabe benötigen (sog. «need to know»), und zwar sowohl persönlich und analog wie auch digital. Es müssen unternehmensintern entsprechende Weisungen erlassen und verteilt werden, und die Personen sind entsprechend zu schulen. Allenfalls muss auch ein Bearbeitungsreglement erstellt werden.

3.4. Betroffenenrechte (Information, Auskunft, Berichtigung, Löschung)

Das revidierte DSG sieht neu grundsätzlich gegenüber allen von einer Datenbearbeitung Betroffenen eine Informationspflicht vor. Eine Ausnahme von dieser Informationspflicht besteht, sofern die betroffene Person bereits entsprechend informiert wurde oder wenn die Datenbearbeitung aufgrund einer gesetzlichen Bestimmung erfolgt. Bei der gesetzlich vorgesehenen Beschaffung und Bearbeitung muss jedoch klar geprüft werden, ob diese auf die Erfüllung der gesetzlichen Pflicht beschränkt bleibt, oder ob darüber hinaus weitere Daten erhoben werden oder bereits vorhandene Daten noch für andere Zwecke bearbeitet werden, was wie-

[12] BSK GwG-Gaul/Isler/Vasella, N 3 zu Art. 33 GwG.

[13] Siehe auch Eidg. Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, das neue Datenschutzgesetz aus Sicht des EDÖB, Stand 7. Oktober 2022, S. 3 f.; https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2022/leitfaden_ndsg.pdf.download.pdf/Leitfaden%20Das%20neue%20Datenschutzgesetz%20aus%20Sicht%20des%20ED%C3%96B_20221009.pdf

derum zu einer erneuten Informationspflicht führen würde. In der Regel kann diese Information auch mittels einer Datenschutzerklärung (DSE) erfolgen, die über einen Mindestinhalt verfügen muss. Entsprechend muss der für die Datenbearbeitung Verantwortliche eine Datenschutz-Folgeabschätzung machen, die insbesondere dann notwendig wird, wenn die gesammelten Daten umfangreich, systematisch und ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person haben kann (Art. 22 nDSG), sog. Profiling. Allerdings entfällt eine solche Datenschutz-Folgeabschätzung, wenn die Datenbearbeitung Privater aufgrund einer gesetzlichen Bestimmung verlangt wird (Art. 22 Abs. 4 nDSG).

Neu haben betroffene Personen ein Auskunftsrecht, das sie berechtigt, Auskunft zu den über sie bearbeiteten Daten zu verlangen (Art. 25 nDSG). Inhaltlich muss die Auskunft diejenigen Informationen enthalten, welche bereits in der DSE aufgeführt sind. Es handelt sich dabei um die Identität und die Kontaktdaten des für die Bearbeitung Verantwortlichen, den Bearbeitungszweck, Kategorien der bearbeiteten Personendaten, Kategorien der möglichen Empfänger von Personendaten oder die möglichen Zielstaaten, sofern die Bekanntgabe auch ins Ausland erfolgt.

Zudem kann die betroffene Person die Berichtigung oder die Löschung der über sie bearbeiteten Daten verlangen. Schon im Interesse der Datensparsamkeit sind Daten, welche für die Bearbeitung nicht mehr gebraucht werden, zu löschen und nicht «auf Vorrat» zu halten.

4. Spannungsfeld zwischen den Anforderungen des GwG und DSG

4.1. Generelles Verhältnis

Wie bereits erwähnt, hat der Gesetzgeber das grundsätzliche Spannungsfeld wie folgt gelöst: Gemäss Art. 33 GwG und dem nur formal angepassten Art. 33 nGwG bleibt das DSG auch im Bereich der Sammlung von Daten unter dem GwG anwendbar. Indessen führt der Vorbehalt in Art. 22 Abs. 4 nDSG (unter bisherigem Recht Art. 14 Abs. 4 DSG) dazu, dass im Verhältnis Finanzintermediär – Kunde vom uneingeschränkten Recht des Finanzintermediärs ausgegangen werden kann, dass er im Rahmen der Art. 3 ff. GwG die notwendigen Daten und Informationen beschaffen kann und muss. Entsprechend ist auch der Kunde generell verpflichtet, die entsprechenden Daten zur Verfügung zu stellen, was in der Vertragsdokumentation, inkl. Allgemeine Geschäftsbedingungen (AGB), noch explizit festgehalten werden kann. Allerdings entbindet das die Finanzintermediäre nicht, die Grundsätze des Datenschutzgesetzes und namentlich die Vorgaben zur Datensicherheit einzuhalten.

4.2. Prüfung und Abklärung allgemein zugänglicher Quellen und Daten

Ungeachtet der weitgehenden gesetzlichen Erlaubnis zur Datenbeschaffung zum Zweck der Bekämpfung von Geldwäscherei, Terrorismusfinanzierung und qualifizierter Steuerdelikte sind die folgenden Punkte, die im revidierten DSG verdeutlicht werden, zu beachten:

Im neuen DSG sind die Grundsätze «Privacy by Design» (Datenschutz durch Grundeinstellung), sowie «Privacy by default» (Datenschutz durch datenschutzfreundliche Grundeinstellungen) festgehalten. Damit werden sowohl Behörden wie auch private Unternehmen verpflichtet, die im Datenschutzrecht geltenden Bearbeitungsgrundsätze bereits ab der Planung ihrer Vorhaben einzubauen und umzusetzen, insbesondere durch die Implementierung geeigneter technischer und organisatorischer Massnahmen. So wird beispielsweise verlangt, dass die Applikationen so programmiert sind, dass Daten standardmässig anonymisiert und gelöscht werden, wenn der Zweck der Bearbeitung erfüllt ist. Dies sollte künftig helfen, dass nur «need to know» – Daten erhoben und bearbeitet werden, und nicht auch «nice to know». Das dient nicht zuletzt dem Schutz der Betroffenen vor Missbrauch, Datenlecks, Phishing, etc. und gilt auch, soweit Informationen aus öffentlich-zugänglichen Quellen wie Zeitungsartikel, internationalen Datenbanken, Sanktionslisten im Rahmen des Informationsaustausches erhalten bzw. beschafft wurden (Art. 6 Abs. 5 nDSG).

4.3. Erkundigungen bei Direktbetroffenen

Wie bereits erwähnt, gilt es auch unter dem revidierten Datenschutzgesetz bei der Beschaffung und der Bearbeitung von Personendaten die Grundsätze der Rechtmässigkeit, der Transparenz, der Verhältnismässigkeit, der Richtigkeit sowie der Zweckmässigkeit zu beachten (vgl. Art. 6 Abs. 1–4 nDSG). Um den Anforderungen der Transparenz gerecht zu werden, muss ein privater Verantwortlicher künftig grundsätzlich bei jeder beabsichtigten Beschaffung von Personendaten die direkt betroffene Person vorgängig angemessen informieren, sog. Informationspflicht. Konkret sind dabei die Identität und Kontaktdaten des Verantwortlichen, der Bearbeitungszweck und gegebenenfalls die Empfänger von Personendaten bekanntzugeben (Art. 19 nDSG). Diese Informationspflicht wird durch zahlreiche Ausnahmen gemäss Art. 20 nDSG beschränkt oder aufgehoben, so falls die betroffene Person bereits entsprechend informiert wurde oder die Bearbeitung von Daten gesetzlich vorgesehen ist. Letzteres dürfte aufgrund der weitgehenden Rechtfertigung der Beschaffung von umfangreichen Personendaten gemäss Art. 3 ff. GwG zur Anwendung gelangen. Kunden von Finanzintermediären wissen oder müssen wissen, dass über sie selbst und über weitere Personen, namentlich wirtschaftlich Berechtigte, Bevollmächtigte und ihnen nahestehenden Personen, Daten beschafft und bearbeitet werden.

Während die Kunden und Vertragspartner als Direktbetroffene letztlich eine Einwilligung in die Datenbearbeitung gegeben haben, ist dieser Punkt bei den weiteren Recherchen, die ein Finanzintermediär vornehmen muss, nicht offensichtlich. Das gilt nicht nur für Vertragspartner des Kunden, weitere Betroffene in komplexen Strukturen, z.B. Minderheitsaktionäre, sondern auch generell für den weiten Kreis der nahestehenden natürlichen und/oder juristischen Personen. Das wird besonders deutlich bei nahestehenden Personen von sog. politisch exponierten Personen (PEP) gemäss Art. 2a Abs. 1 lit. a GwG. Vertragsbeziehung mit Letzteren werden aufgrund deren Status automatisch zu einer Geschäftsbeziehung mit erhöhten Risiken, was sich auf die nahestehenden Personen ausdehnt, obwohl eine klare gesetzliche Grundlage fehlt, die nahestehende von nicht-nahestehenden Personen abgrenzt, spricht doch Art. 2a Abs. 2 GwG nur davon, dass diese Personen «aus familiären, persönlichen oder geschäftlichen Gründen *erkennbar* nahestehen» müssen. Diese Personen werden von der Datenbearbeitung erfasst, auch wenn sie selber keine Vertragsbeziehungen unterhalten und ihr Auskunftsrecht nicht ausüben können.

4.4. Auskunftsrecht bei der Ausübung der Meldepflicht und des Melderechts

Die Art. 9 ff. nGwG bringen Änderungen und Präzisierungen im Zusammenhang mit der Meldung bei Geldwäschereiverdacht oder dem Recht der MROS zur Erlangung weiterer Informationen nach Art. 11a nGwG mit sich. Zum einen muss eine Geschäftsbeziehung nicht mehr automatisch, sondern nur dann gesperrt werden, wenn die MROS den Finanzintermediär entsprechend instruiert, was immer dann der Fall ist, wenn sie das Dossier den Strafuntersuchungsbehörden weiterleitet.

Im bisherigen Recht und weiterhin ist vorgesehen, dass der Finanzintermediär den Kunden nicht informieren darf, wenn er eine Meldung erstattet. Während im bisherigen Recht unklar blieb, wie das datenschutzrechtliche Auskunftsrecht gehandhabt werden soll und kann, hält Art. 34 Abs. 3 nGwG fest, dass nach erfolgter Meldung das Auskunftsrecht gemäss Art. 25 nDSG nurmehr gegenüber der Meldestelle ausgeübt werden kann. Dies ist u.E. eine klare und transparente Lösung und entlastet Finanzintermediäre und Betroffene.

4.5. Datenweitergabe (im In- und Ausland)

Auch unter dem revidierten Datenschutzgesetz können Daten ins Ausland gegeben werden, sofern neu der Bundesrat feststellt, dass die Gesetzgebung des Drittstaates einen angemessenen Schutz gewährleistet (Art. 16 nDSG). Bisher hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) diese Liste geführt. Wie bisher können Daten auch in ein Land übertragen werden, welches nicht auf dieser Liste steht, sofern ein geeigneter Datenschutz auf andere Weise, beispielsweise durch einen völkerrechtlichen Vertrag, entsprechend vereinbarte Datenschutzklauseln oder unternehmensinterne Datenschutzvorschriften ge-

währleistet wird. Falls eine Datenbekanntgabe ins Ausland geplant ist, so müssen die entsprechenden Länder angegeben werden, unabhängig davon, ob diese Länder über einen angemessenen Datenschutz verfügen. Das gilt auch bei der Speicherung von Daten auf einem sich nicht in der Schweiz befindlichen System wie beispielsweise einer Cloud.

Diese Regelung wird durch das GwG weitgehend übersteuert. Der 4. Abschnitt des Gesetzes regelt die nationale und internationale Amtshilfe. So bestimmen Art. 29 und 29a nGwG einen weitreichenden Informationsaustausch der inländischen Behörden untereinander, wozu gemäss Art. 29b nGwG explizit auch die privatrechtlich organisierten Selbstregulierungsorganisationen (SRO), die die sog. «übrigen» Finanzintermediäre geldwäschereirechtlich beaufsichtigen, und Aufsichtsorganisationen (AO) für Vermögensverwalter und Trustees gezählt werden. Die MROS kann ihrerseits mit ausländischen Meldestellen, die in der sog. Egmont Gruppe zusammengeschlossen sind, seit einigen Jahren Informationen austauschen, ohne dass datenschutzrechtliche Bestimmungen zur Anwendung gelangen.

4.6. Fehlender datenrechtlicher Schutz der juristischen Person und das Aktionärsregister

Das per 1. September 2023 in Kraft tretende neue Datenschutzrecht in der Schweiz wird künftig, wie bereits in der DSGVO so geregelt, nur noch den Schutz der Persönlichkeit von natürlichen Personen, über welche Personendaten bearbeitet werden, beinhalten. Somit werden die Daten von juristischen Personen wie AG oder GmbH, von Vereinen oder Stiftungen nicht mehr vom DSG erfasst. Diese können sich aber weiterhin auf den durch Art. 28 ZGB (Zivilgesetzbuch) gewährten Persönlichkeitsschutz, den durch Art. 162 StGB geregelten Schutz des Geschäfts- oder Fabrikationsgeheimnisses, sowie auf die entsprechenden Bestimmungen der Bundesgesetze über den unlauteren Wettbewerb und über Kartelle berufen.

Ungeachtet dessen geniessen die Privatpersonen, die als «ultimate beneficial owner» hinter juristischen Personen stehen oder ganz allgemeine Aktionäre und Gesellschafter, die Privatpersonen sind, den Schutz des DSG. Soll nun, wie von der GAFI vorangetrieben, ein Register der wirtschaftlich Berechtigten geschaffen werden, so ist dem Datenschutz und dem Schutz der Grundrechte der Privaten Rechnung zu tragen. Ein solches Register wäre wohl unter dem Gesichtspunkt der Datenschutz-Folgeabschätzung als ein für die Betroffenen hohes Risiko einzustufen (Art. 22 Abs. 1 und 2 nDSG). Das gilt sowohl inhaltlich als auch technologisch und hinsichtlich der Legitimation zur Einsicht. Es ist auch nicht sicher, ob ein solches Register unter dem Aspekt des «need to know», d.h. der Zweckmässigkeit und der Verhältnismässigkeit dem Datenschutzrecht, aber auch der Geldwäschereibekämpfung gerecht wird, oder ob es nicht einfach zu einer grossen Datenkrake wird.

5. Ausblick

Im Hinblick auf die verschiedenen Spannungsfelder GwG – DSG ist die Neuerung, die das revidierte DSG vorsieht, genauer zu betrachten. Art. 11 Abs. 1 nDSG sieht im Sinne einer Selbstregulierung vor, dass Berufs-, Branchen- und Wirtschaftsverbände, die nach ihren Statuten zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt sind, eigentliche *Verhaltenskodizes* erarbeiten können, um die datenschutzrechtlichen Vorgaben einheitlich und transparent handhaben zu können. Diese Branchenverhaltenskodizes können dem EDÖB zur Prüfung vorgelegt werden. Dieser nimmt dazu Stellung und publiziert seine Stellungnahme (Art. 11 Abs. 2 nDSG). Zurzeit sind soweit ersichtlich (noch) keine Verhaltenskodizes publiziert worden.

In eine ähnliche Richtung geht aber das Projekt der MROS bzw. des Eidg. Justizdepartements, eine Art «public-private partnership» im Zusammenhang mit der Handhabung von Meldungen und generell der Zusammenarbeit mit dem Privatsektor zu schaffen. Da würde es wohl Sinn machen, wenn die Verbände im Finanzsektor durch einen Verhaltenskodex, der dem DSG gerecht wird, einheitliche Standards schaffen würden. Eine entsprechende Konsultation wurde im September 2022 in die Wege geleitet. Die Auswertung der Ergebnisse ist noch nicht erfolgt.