

Übermittlung von Personendaten von Rechtsanwältinnen und Rechtsanwälten an US-Behörden

RA Dr.iur. Alice Reichmuth Pfammatter*, erstattet am 02.06.2014

Vorbemerkung

Der vorliegende Leitfaden wurde aus Anlass des US-Programms zur Bereinigung des Steuerstreits der Schweizer Banken mit den Vereinigten Staaten erstellt.

Er richtet sich an Rechtsanwältinnen und Rechtsanwälte, die im Rahmen ihrer eigentlichen Anwaltstätigkeit mit dieser Fragestellung konfrontiert werden. Rechtsanwältinnen und Rechtsanwälte, die als Finanzintermediäre tätig sind, sowie Datenübermittlungen im Rahmen eines Rechtshilfeverfahrens werden aus den Überlegungen ausgeklammert.

Der Leitfaden enthält Hinweise auf datenschutzrechtliche Aspekte, beleuchtet nicht aber bank- oder finanzrechtliche Fragestellungen. Er ist allgemein gehalten und entbindet nicht davon, die Umstände im Einzelfall zu prüfen. Der einfacheren Lesbarkeit halber wird die Bezeichnung „Rechtsanwälte“ verwendet, ohne Rechtsanwältinnen zu diskriminieren.

* Datenschutzbeauftragte des Kantons FR; Rechtskonsultantin bei Kessler Wassmer Giacomini & Partner in Schwyz und Wollerau.

Zusammenfassung

1. US-Program for Non-Prosecution Agreements (NPA) or Non-Target Letters for Swiss Banks

- Ausgangslage → **Ziffer 1.1**
- Eigentliche „Kundendaten“ im engeren Sinn werden nicht übermittelt; „Leaver-Listen“ können allerdings Daten des Rechtsvertreters resp. Anwalts enthalten und somit als mittelbare Identifikatoren qualifiziert werden → **Ziffer 1.2**
- Bestehen Befürchtungen über eine Datenübermittlung kann allenfalls sofortiges Handeln angezeigt sein → **Ziffern 1.3 und 3.2**

2. Datenschutzrechtliche Argumente:

- Die Datenübermittlung ins Ausland ist nicht rechtmässig und verletzt Datenschutzgrundsätze → **Ziffer 2.1**
- Bei den „Leaver-Listen“ handelt es sich gemäss Definition um nicht kundenbezogene Daten; es kann sich allerdings um Personendaten handeln, sofern die Daten nicht vollumfänglich anonymisiert sind und somit den Rückschluss auf die betroffene Person mittelbar zulassen → **Ziffer 1.2**
- Bei Information durch die Bank besteht sofortiger Handlungsbedarf: Widerspruch. → **Ziffer 2.2 und 2.3, 3.2**
- Ausübung des Auskunftsrechts (Art. 8 DSG): Die Bank hat über die Gesamtheit der sie betreffenden Daten, Herkunft der Daten, Zweck der Bearbeitung Kategorien der Personendaten und Datenempfänger, Auskunft zu erteilen → **Ziffer 2.4**

3. Klageverfahren

Hält die Bank an der Datenübermittlung fest, ist der Bank gerichtlich zu untersagen, die fraglichen Personendaten an US-Behörden zu übermitteln (Art. 15 Abs. 1 DSG i.V. mit Art. 28 und 28a ZGB).

- Klage im ordentlichen Verfahren, nach vorgängiger Durchführung einer Schlichtungsverhandlung
- Es kann sich aufdrängen, sofort aktiv zu werden, ein Schlichtungsgesuch zu stellen → **Ziffer 3.1** allenfalls vorsorgliche Massnahmen verlangen → **Ziffer 3.2**

Überblick über Datenkategorien und die Zulässigkeit von deren Übermittlung:

Datenkategorien	Übermittlung
Kundendaten: Name, Konto-Nr, AHV-Nr	Explizit verboten (Bankgeheimnis)
Mittelbare Identifikatoren des Kunden	Implizit verboten Aus der Sicht des Anwalts: Die Übergabe von Daten des Anwalts erlaubt eine mittelbare Identifikation des Kunden und ist von der Bewilligung des Bundesrates nicht gedeckt.
Leaver Listen: Nicht kundenbezogene Daten, betreffen aber Transfer der Gelder (Menge, Adressaten...)	Erlaubt, soweit keine Personendaten / möglicherweise verboten wegen Art. 273 al. 2 StGB (Geschäftsgeheimnis)
Dritte werden vom Bankgeheimnis nicht geschützt: Anwälte	Bedingt zulässig, sofern keine Verletzung der Datenschutzgesetzgebung, namentlich: <ul style="list-style-type: none"> • Unerlaubte Zweckänderung der Datenerhebung • Öffentliches Interesse: es kann nicht zulässig sein, den Anwalt zu zwingen, zwischen einer Verletzung des Berufsgeheimnisses in der Schweiz und einer Strafverfolgung im Ausland zu entscheiden. Die Datenüberweisung gefährdet somit den Grundsatz

	<p>des Berufsgeheimnisses i.S. Art. 13 BGFA i.V.m. Art. 321 StGB.</p> <ul style="list-style-type: none"> • Proportionalität: Soweit ein Anwalt sein Berufsgeheimnis nicht verletzen darf, ist es unverhältnismässig, seine Daten an ausländische Behörden zu übermitteln; denn die Verfahren sind nicht geeignet, allfällige Steuerhinterzieher aufzudecken, fügen aber dem Anwalt Schaden zu.
--	---

1. Ausgangslage

1.1 US-Program for Non-Prosecution Agreements (NPA) or Non-Target Letters for Swiss Banks

Am 29. August 2013 hat das US Department of Justice ein Programm zur Bereinigung des Steuerstreits der Schweizer Banken mit den Vereinigten Staaten („Program for Non-Prosecution Agreements or Non-Target Letters for Swiss Banks“) verabschiedet. Gemäss FINMA-Mitteilung 50(2013) enthält dieses Programm „die Vorgaben und Bedingungen, gemäss welchem derzeit nicht in US-Steuerstrafverfahren verwickelte Schweizer Banken ihre Situation direkt mit den zuständigen US-amerikanischen Behörden regeln können“. Dabei steht es den Instituten frei, zur Regelung ihrer Situation ein Non-Prosecution Agreement gemäss den Bedingungen von Ziffer II des Programms (category 2), einen Non-Target Letter gemäss Bedingungen von Ziffer III (Category 3) oder IV (Category 4) zu beantragen¹.

Wie den Informationen des Schweizerischen Staatssekretariates für internationale Finanzfragen zu entnehmen ist, beinhaltet die Lösung drei Elemente: das Joint Statement zwischen den Regierungen der beiden Länder, das unilaterale amerikanische Programm, an welchem sich die Banken auf freiwilliger Basis beteiligen können sowie die Bewilligungen des Bundesrates gemäss Art. 271 StGB, welche den Banken die Kooperation ermöglicht².

¹ FINMA-Mitteilung 50/2013 vom 30. August 2013.

² <http://www.sif.admin.ch/themen/00502/00806/index.html?lang=de>

In Ziffer 5 des Joint Statements zwischen dem US-Justizdepartement und dem Eidg. Finanzdepartement vom 29. August 2013 (inoffizielle Übersetzung) wird festgehalten³:

„5. Aufgrund der Bedeutung, die beide Seiten dem hohen Schutz der Personendaten und der Privatsphäre aller Individuen gemäss ihrem Recht beimessen, gehen die Unterzeichner davon aus, dass die zur Verfügung gestellten Personendaten nur zu Strafverfolgungszwecken (die auch Regelungsmassnahmen umfassen können) in den USA oder zu anderen gemäss US-Recht gestatteten Zwecken verwendet werden.“

Bewilligungen des Bundesrates gemäss Art. 271 des Schweizerischen Strafgesetzbuches an Bankinstitute

Die Banken, welche sich am Programm beteiligen wollen, benötigen eine Bewilligung des Bundesrates gemäss Art. 271 Ziff. 1StGB, mit den zuständigen US-Behörden im Rahmen der Schweizerischen Gesetzgebung zu kooperieren⁴. Diese Bewilligung dient dem Schutz vor Strafverfolgung wegen verbotenen Handlungen für einen fremden Staat.

Gestützt auf die Musterverfügung des schweizerischen Staatssekretariates 3. Juli 2013 für internationale Finanzfragen SIF umfasst die Bewilligung sämtliche relevanten Daten, insbesondere generelle Angaben und Dokumentationen, die einen Bezug zu einer US-Person haben, Leaver-Listen sowie Personendaten von Mitarbeitenden und Dritten.

Kundendaten sind von der Bewilligung nicht erfasst. Diese dürfen nur im Rahmen eines Amtshilfeverfahrens, basierend auf dem Doppelbesteuerungsabkommen übermittelt werden, wie das SIF⁵ auf seiner Homepage publiziert⁶.

Die Bewilligungen des Bundesrates enthalten u.a. Auflagen, Mitarbeitende und Dritte vor einer Bekanntgabe ihrer Personendaten zu informieren, sie gegebenenfalls auf den Rechtsweg hinzuweisen sowie solche

³ <http://www.news.admin.ch/NSBSubscriber/message/attachments/31813.pdf>

⁴ Eine Musterverfügung mit Wegleitung ist auf der Website des Staatssekretariats für internationale Finanzfragen SIF abrufbar

<http://www.sif.admin.ch/00488/index.html?lang=de&msg-id=50049>

⁵ Fachkontakt: info@sif.admin.ch

⁶ <http://www.sif.admin.ch/themen/00502/00806/index.html?lang=de>

Personendaten erst nach rechtskräftiger Abweisung der Klage zu übermitteln⁷. Die Auflagen sind Bestandteil der Bewilligung und es entfällt bei Einhaltung der Bedingungen die Strafbarkeit nach Art. 271 Ziff. 1 StGB. Die Missachtung der Bedingungen wird zudem unter die Strafandrohung von Art. 292 StGB gestellt.

Empfehlungen des Eidgenössischen Datenschutzbeauftragten zur Übermittlung von Personendaten an US-Behörden

Der Eidgenössische Datenschutzbeauftragte hat bereits am 15. Oktober 2012 den im Steuerstreit involvierten Banken Empfehlungen für ein datenschutzkonformes Vorgehen bei der Übermittlung von Personendaten abgegeben. In seinem Merkblatt vom 20. Juni 2013 hat er die Grundsätze, welche die Banken im Hinblick auf eine allfällige Übermittlung von Personendaten einzuhalten haben, festgehalten⁸. Namentlich hat er in Erinnerung gerufen, dass die Datenübermittlung verhältnismässig sein müsse (Art. 4 Abs. 2 DSG⁹), was auch Personen, „die entsprechende Geschäftsbeziehungen mit Bezug zu einer US-Person organisiert, betreut oder überwacht haben“ mit einschliesse. Der Eidg. Datenschutzbeauftragte verlangte die vorgängige Information der betroffenen Personen (Art. 4 Abs. 2 und 4 DSG), die Möglichkeit der Ausübung des Auskunftsrechts innert angemessener Frist (Art. 8 DSG), die Vornahme einer Interessenabwägung im Fall des Widerspruchs der betroffenen Person (Art. 13 DSG) sowie deren Information über ihre Rechte.

1.2 Welche Daten sind betroffen?

Aus der Musterverfügung¹⁰ zur Bewilligung gemäss Art. 271 Ziffer 1 StGB ist ersichtlich, dass die Bewilligung folgende Daten und Dokumentationen umfasst:

- „generelle Angaben und Dokumentationen zum Geschäftsgebaren der Gesuchstellerin sowie Informationen zu Geschäftsbeziehungen, die einen Bezug zu einer US-Person“ haben;

⁷ Ziffer 1.4 der Musterverfügung

⁸ Empfehlungen des Eidgenössischen Datenschutzbeauftragten vom 15. Oktober 2012 an die im Rahmen der Bereinigung des Steuerstreits beteiligten Banken;
<http://www.edoeb.admin.ch/datenschutz/00628/00663/index.html?lang=de>

⁹ Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG), SR 235.1.

¹⁰ <http://www.sif.admin.ch/00488/index.html?lang=de&msg-id=50049>

- keine Bankkundendaten; diese dürfen nur auf dem Rechtshilfeweg übermittelt werden;
- sog. „Leaver-Listen“, die „nicht personalisierte Daten im Zusammenhang mit der Schliessung von Konten und dem damit verbundenen Transfer“ an andere Institute enthalten;
- Personendaten von Mitarbeitenden der Bank und Dritten, „die für solche Geschäftsbeziehungen in ähnlicher Weise tätig waren“ (d.h. Geschäftsbeziehungen „organisiert, betreut oder überwacht haben“).

Die Bewilligung sieht demnach die Übermittlung von personenbezogenen Daten – neben allgemeinen Informationen – vor; sie umfasst allerdings keine Bankkundendaten.

Daten des Rechtsanwalts

Die personenbezogenen Daten, die aufgrund der bundesrätlichen Bewilligung, mit den US-Behörden zu kooperieren, übermittelt werden können, umfassen u.U. auch solche von Rechtsanwälten, wenn sie von den Bankinstituten als „Dritte“ qualifiziert werden. Es dürfte sich bei den personenbezogenen Daten primär um Namen, Identifikationsnummern, Adressen, Mail-Adressen, Telefonnummern, Korrespondenz, E-Mail Verkehr etc. des Rechtsanwalts handeln, der für US-Kunden tätig geworden ist¹¹. Solche Informationen können in den besagten Leaverlisten enthalten sein.

Daten des Klienten

Unklar ist, inwieweit in den vom Department of Justice verlangten „erheblichen Informationen“¹² auch Kunden- resp. Klientendaten enthalten sind, zumal das US-Programm in Ziff. II.D.2¹³ verschiedene Angaben für jedes Konto verlangt (wie Wert, Anzahl der daran berechtigten Personen, Name und Funktion der mit der Betreuung des Kunden betrauten Drittperson usw.). Erlauben die Angaben, den US-Kunden zu identifizieren? Eine indirekte Identifikation ist je nach Kontext nicht auszuschliessen; dies

¹¹ Hinweis: Auch Identifikatoren, wie AHV-Nummer, Firmennummer, UID, Passnummer, Kreditkartennummer, Kontonummer oder andere Kennnummern zählen zu den Personendaten gemäss Art. 3 Bst. A DSGVO, da sie erlauben, die betroffene Person zu identifizieren (vgl. auch Rosenthal, Ziff. 21 zu Art. 3 DSGVO).

¹² Gemäss Musterverfügung Ziff. 1.1.

¹³ [Vgl. Link zum US-Programm: http://www.justice.gov/opa/pr/2013/August/13-tax-975.html](http://www.justice.gov/opa/pr/2013/August/13-tax-975.html)

umso mehr als gemäss Wegleitung zur Musterverfügung des Bundesrates der Ausdruck „Bankkundendaten‘ nur persönliche Identifikationsmerkmale des Bankkunden (Name, Adresse, Sozialversicherungsnummer, Kontonummer) umfasst“. In der Literatur ist allerdings umstritten, von welchem erforderlichen Aufwand zur Bestimmbarkeit einer Person ausgegangen werden kann¹⁴; aufgrund des Interesses der beteiligten US-Behörden dürfte von der Bestimmbarkeit der Person ausgegangen werden. Für den betroffenen Anwalt stellen sich demnach erhöhte Anforderungen, zu kontrollieren, welche Daten übermittelt werden sollen, ob die Daten genügend anonymisiert sind oder ob eine Identifikation möglich ist, um das Anwaltsgeheimnis wahren zu können.

1.3 Liegt Dringlichkeit zum Handeln im Einzelfall vor?

Der Bundesrat sieht in seiner Bewilligung vor, dass die schweizerische Gesetzgebung wie auch die Vorschriften des Datenschutzes einzuhalten sind. Nach dem Gesagten ist die Einhaltung der Bedingungen – worunter auch die Einhaltung der datenschutzrechtlichen Ansprüche der betroffenen Personen gehört – an die Strafandrohung von Art. 292 StGB geknüpft.

Doch kann sich – gerade bei der Geltendmachung des datenschutzrechtlichen Auskunfts- und Weigerungsrechts – die Frage der Dringlichkeit stellen; mithin, ob die betroffene Person, die Übermittlung von Daten an die US-Behörden rechtzeitig verhindern kann. Es ist anzunehmen, dass die Banken, die sich zur Teilnahme am US-Programm verpflichtet haben, unter zeitlichem Druck stehen.

Es stellen sich für den betroffenen Anwalt folgende Fragen, die er in Abwägung aller Faktoren im Einzelfall zu beantworten hat:

- Gewährleisten die Auskunftsrechts- und Einsichtsrechte der betroffenen Personen – wie sie Datenschutzgesetzgebung vorsieht – die wirksame Verhinderung der Datenübermittlung?
- Hat die betroffene Person die Möglichkeit, direkt den gerichtlichen Weg zu beschreiten? Wenn ja, unter welchen Voraussetzungen?
- Liegt es im Rahmen der Möglichkeit, die Fragen mit dem Klienten zu erörtern, um einen gangbaren Weg zu finden?

¹⁴ Rosenthal, N 24 f. zu Art. 3 DSG.

1.4 Fallkonstellationen der vorliegenden Betrachtung

Es sind verschiedene Konstellationen denkbar, aufgrund welcher Rechtsanwälte aus Bankunterlagen ersichtlich sind und mit der beabsichtigten Datenübermittlung konfrontiert werden. Im Blickfeld stehen vorliegend:

- (1) Rechtsanwälte, die im Rahmen ihrer angestammten Anwaltstätigkeit als Vertreter von US-Kunden tätig geworden sind (z.B. als Willensvollstrecker), und deren Namen im Zusammenhang mit einem Konto eines US-Bürgers in Erscheinung tritt.
- (2) Rechtsanwälte, die Bankinstitute im Rahmen ihrer Anwaltstätigkeit vertreten haben. Deren Namen könnte allenfalls aus generellen Informationen und Daten zum Geschäftsgebaren hervorgehen.
- (3) Rechtsanwälte, deren Namen nicht in Zusammenhang mit einem Vertretungsverhältnis erscheinen.

Nicht erfasst werden Rechtsanwälte, die Bewilligungsträger für Finanzgeschäfte sind bzw. in einem Anstellungsverhältnis mit einem Bewilligungsträger der FINMA stehen.

Ohne besondere Erwähnung finden die nachfolgenden Überlegungen auf die Kategorien (1) – (3) Anwendung.

2. Datenschutzrechtliches Argumentarium

Beabsichtigte Datenübermittlungen, die im vorliegenden Kontext den Rechtsanwalt als „Dritte“ im Sinne des US-Programms betreffen, haben Personendaten im Sinn von Art. 3 Bst. a DSGVO zum Gegenstand.

Datenschutzrechtlich werden Daten bearbeitet mit dem besonderen Zweck, sie ins Ausland zu übermitteln¹⁵.

2.1 Ist die Datenübermittlung ins Ausland rechtmässig?

Eine Datenübermittlung ins Ausland darf gestützt auf Art. 6 DSG die Persönlichkeit der betroffenen Person nicht verletzen; sie muss rechtmässig sein (Art. 4 Abs. 1 DSG) und auf einem Rechtfertigungsgrund beruhen. Das alleinige öffentliche Interesse im Sinn von Art. 6 Abs. 2 Bst. b DSG genügt den Anforderungen nicht¹⁶.

Durch die Datenübermittlung an US-Behörden werden die Persönlichkeitsrechte sowohl des Klienten wie des betroffenen Rechtsanwalts widerrechtlich verletzt; Rechtfertigungsgründe im Sinne von Art. 13 DSG, welche die Interessen der betroffenen Personen überwiegen, erscheinen uns nicht gegeben.

Als Gründe für eine **unrechtmässige Datenbearbeitung** lassen sich anführen:

Auf Seiten des Klienten:

- Unter der Marginalie „Wirtschaftlicher Nachrichtendienst“ schützt Art. 273 Abs. 2 StGB u.a. gesetzliche Geheimnisse vor deren Preisgabe an ausländische Organisationen oder Behörden¹⁷. Der Bundesrat stellt zwar Bankinstituten eine Bewilligung aus, mit den US-Behörden zu kooperieren. Diese Bewilligung wird gestützt auf Art. 271 StGB erteilt und schliesst einzig eine Strafbarkeit nach dieser Bestimmung aus. Der Bundesrat hält in seiner Musterverfügung vom 3. Juli 2013 ausdrücklich fest, dass „die Bewilligung aber nicht von der Einhaltung der übrigen Bestimmungen des schweizerischen Rechts, insbesondere von der Beachtung bestehender Geschäfts- und Bankkundengeheimnisse, der Bestimmungen über den Datenschutz und der Verpflichtungen als Arbeitgeberin“ entbindet. Die Bewilligung des Bundesrates gestützt auf Art. 271 StGB ermächtigt demnach die Bank nicht, das Bankkundengeheimnis preiszugeben, auch nicht durch mittelbare Identifikatoren (z.B. durch Übermittlung von Personendaten des Anwalts). Eine Datenübermittlung unter Missachtung des Bankgeheimnisses verletzt Schweizer Recht. Daran

¹⁵ Als besonders heikle Art der Datenbearbeitung, da die Personendaten den ursprünglichen Bearbeitungskreis verlassen.

¹⁶ Werden Personendaten ins Ausland übermittelt, unterstehen sie nicht mehr Schweizer Recht.

¹⁷ Vgl. Rosenthal, N 2 f. zu Art. 273 StGB.

ändert auch nichts, dass Bankkundendaten nicht „direkt“ übermittelt werden sollen. Wenn die zu liefernden Leaver-Listen die Klienten zu bestimmen ermöglichen, ist die Datenübermittlung rechtswidrig.

- Mit der Datenzusammenstellung und der anschliessend beabsichtigten Datenübermittlung an US-Behörden werden die im Rahmen der Vertragsabwicklung zwischen Bank und Klient bzw. Rechtsanwalt gesammelten und erhobenen Daten einem neuen Zweck zugeführt. Dies widerspricht dem Grundsatz, wonach Personendaten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 2 DSGVO). Das Bankinstitut hat die Personendaten im Rahmen seines spezifischen Tätigkeitsbereichs, in welchem es über branchenspezifisches Fachwissen und Know-how verfügt, erhoben. Der betroffene Rechtsanwalt selbst ist nicht im Bankensektor tätig, vielmehr hat er im Rahmen des Vertragsverhältnisses auf die Fachkunde und die korrekte Abwicklung des Vertrags vertraut. Zu diesen Zwecken wurden die Personendaten des Klienten sowie allenfalls von dessen Vertreter erhoben und bearbeitet im Sinne der DSGVO. Die Bearbeitung der Daten im Rahmen des US-Programms, sei es durch Übermittlung an einen „Independent Examiner“ zur Bearbeitung, sei es durch Übermittlung an US-Behörden erfolgt zu völlig anderen Zwecken, als zu jenen, zu welchen sie für die Abwicklung der konkreten geschäftlichen Beziehung erhoben worden sind. Die Bearbeitung der Daten, wie sie nun gehandhabt werden soll, war nicht voraussehbar.
- Im Einzelfall ist zu prüfen, ob die Datenzusammenstellung und – übermittlung gegen Treu und Glauben sowie den Grundsatz der Verhältnismässigkeit verstösst (zum Beispiel aufgrund des bisherigen Geschäftsgebarens (Korrespondenz, von Zusicherungen etc.) zu prüfen; vgl. Art. 4 Abs. 2 DSGVO).

Argumentation in Bezug auf die persönliche Situation des Rechtsanwalts:

Die Situation des Anwalts erscheint prekär: In den Leaver-Listen, die das Bankinstitut den US-Behörden zu übermitteln hat, befinden sich zwar „nicht-personalisierte Daten“ gemäss Musterverfügung des Bundesrates. Aber selbst „nicht-personalisierte Daten“ können bei ungenügender Anonymisierung die Person bestimmbar machen. Dies kann namentlich dann der Fall sein, wenn diese Listen Namen von sog. „Dritten“ enthalten. Solche Drittpersonen (u.a. Rechtsanwälte) standen mit der Bank im

Zusammenhang mit der einzelnen Kundenbeziehung in Kontakt; die Daten von solchen Drittpersonen können sich auf den Leaver-Listen befinden. Der Anwalt befindet sich diesfalls in einer Zwangssituation: Einerseits ist er an das Berufsgeheimnis gebunden, andererseits setzt er sich der Strafverfolgung aus, sei es, dass er möglicherweise von amerikanischen Behörden infolge fehlender Kooperation sanktioniert wird, sei es, dass er sich einer Strafverfolgung wegen Verletzung des Berufsgeheimnisses nach Art. 321 StGB aussetzt. In den Bewilligungen des Bundesrates sind keine Auflagen zum Schutze von „Drittpersonen“ vorgesehen, wie dies für Mitarbeitende der Fall ist.

Als Argumente lassen sich anführen:

- Die Übergabe von Daten des Anwalts kann eine mittelbare Identifikation des Kunden erlauben, d.h. über die Daten des Anwalt lassen sich Mandatsverhältnis resp. die persönliche Vertretung eruieren. Diese Datenübergabe ist von der Bewilligung des Bundesrates nicht gedeckt (Bankgeheimnis).
- Art. 273 StGB schützt u.a. gesetzliche Geheimnisse. Die beabsichtigte Übermittlung von Leaver-Listen, die Daten von Rechtsanwältinnen enthalten, können gegebenenfalls dessen Geschäftsgeheimnisse verletzen¹⁸. Art. 273 StGB begründet nicht einen originären Geheimnisschutz, sondern erlangt lediglich dann Bedeutung, wenn ein Geheimhaltungsgrund bereits anderweitig begründet worden ist¹⁹. Mit einer Datenübermittlung ins Ausland macht das Bankinstitut Geheimnisse einer fremden Organisation zugänglich. Damit kann sich das Bankinstitut im Sinne von Art. 273 Abs. 2 StGB strafbar machen. Dies bedingt allerdings, dass der Anwalt substantiiert einen Schaden nachweisen kann, der direkte Folge der Geheimnisverletzung ist (Entscheid des Bundesstrafgerichts vom 25. April 2013, BB.2012.133).

Datenschutzrechtliche Argumente:

- Die Datenübermittlung erfolgt unrechtmässig und widerspricht den allgemeinen Datenbearbeitungsgrundsätzen, insbesondere von Art. 4 DSGVO: Werden Daten gegen den Willen des betroffenen Anwalts übermittelt, verletzt diese Datenbearbeitung allgemeine Datenschutzgrundsätze. Darüber hinaus findet eine zweckfremde Datenbearbeitung statt (vgl. Art. 4 Abs. 2 DSGVO; vgl. oben).

¹⁸ Rosenthal, N 41 zu Art. 273 StGB.

¹⁹ Rosenthal, N 41 zu Art. 273 StGB.

- Die Datenübermittlung liegt nicht im öffentlichen Interesse: In der Interessenabwägung, die im Rahmen einer streitigen Datenübermittlung unerlässlich ist, muss den öffentlichen Interessen an der Einhaltung des anwaltlichen Berufsgeheimnisses Vorrang eingeräumt werden. Es kann nicht angehen, den Anwalt zu zwingen, zwischen einer Berufspflichtverletzung und einer Strafverfolgung im Ausland zu entscheiden. Die Datenüberweisung gefährdet somit den Grundsatz des Berufsgeheimnisses i.S. Art. 13 BGFA i.V.m. Art. 321 StGB. Mit zu berücksichtigen ist, dass der Anwalt bei einer allfälligen Verurteilung wegen Berufsgeheimnisverletzung die persönlichen Voraussetzungen für die Ausübung des Anwaltsberufs (Registereintrag) nicht mehr erfüllen kann.
- Die Datenübermittlung widerspricht dem Verhältnismässigkeitsprinzip insoweit, als die Kommunikation des Namens des Anwalts nicht geeignet ist, den Zweck der eigentlichen Massnahme zu erreichen, nämlich allfällige Steuerhinterzieher zu verfolgen. Es ist davon auszugehen, dass Rechtsanwälte ihre Berufspflichten nicht verletzen werden, so dass die Massnahme ihr Ziel verfehlt.

Darüber hinaus ist die Konsequenz für den Anwalt, seine Berufspflichten nicht einzuhalten, umso mehr unverhältnismässig, als die Folgen in den USA für den Betroffenen nur schwer absehbar sind: Gemäss Ziffer 5 des Joint Statement ist davon auszugehen, „dass die zur Verfügung gestellten Personendaten nur zu Strafverfolgungszwecken (die auch Regelungsmassnahmen umfassen können) in den USA oder zu anderen gemäss US-Recht gestatteten Zwecken verwendet werden“. Mit einer solchen Ungewissheit ist die Datenübertragung unhaltbar.

2.2 Information durch die Bank

Die bundesrätliche Musterverfügung sieht als Auflage vor, die von einer Datenübermittlung betroffenen Personen rechtzeitig zu informieren. Aus datenschutzrechtlicher Sicht sollte diese Information umfassend sein, damit sich die betroffene Person ein Bild über Umfang und Tragweite der Datenübermittlung machen kann. Jedenfalls **sollte** diese Information eine

Reaktion der betroffenen Person auslösen, dies in ihrem Interesse. In Betracht fallen:

- der sofortige Widerspruch gegen die beabsichtigte Datenübermittlung (2.3),
- die Geltendmachung des Auskunftsrechts, um genaue Angaben über Umfang und Art der Daten sowie den Zeitraum, aus dem die Daten stammen, zu erhalten (2.4) oder
- die sofortige Klageeinreichung (3.)

2.3 Widerspruch gegen beabsichtigte Datenübermittlung

Es wird empfohlen, gegenüber dem Bankinstitut **sofort Widerspruch** gegen die Übermittlung der Daten zu erheben. Die beabsichtigte Datenübermittlung verstösst nach dem Gesagten gegen datenschutzrechtliche Grundsätze sowie Schweizer Recht; sie verletzt damit die Persönlichkeitsrechte der betroffenen Personen. Gründe, welche die Persönlichkeitsverletzung rechtfertigen würden, liegen nicht vor: Weder liegt eine Einwilligung vor, noch ist die Verletzung durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt (vgl. Art. 13 DSG). Spricht sich die betroffene Person gegen die Datenübermittlung aus, müsste nach Massgabe des Gesetzes die Bank eine Interessenabwägung gemäss Art. 13 DSG vornehmen. Ob sie dies in allen Fällen tut, sei dahingestellt. Jedenfalls wird die betroffene Person gerichtlich vorgehen müssen, wenn die Bank an der Datenübermittlung festhält.

2.4 Auskunftsrecht

Lassen es die zeitlichen Vorgaben, das bisherige Geschäftsgebaren oder Zusicherungen der Bank zu, davon auszugehen, dass eine allfällige Datenübermittlung nicht vor Klärung der Situation und vor Ausschöpfung der rechtlichen Möglichkeiten erfolgen wird, kann die betroffene Person vom Auskunftsrecht nach Art. 8-10 DSG²⁰ Gebrauch machen.

Worauf ist bei der Ausübung des Auskunftsrechts zu achten?

²⁰ Sowie Art. 1 und 2 der Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (VDSG).

- Die betroffene Person kann vom Bankinstitut Auskunft zu sämtlichen Dokumenten verlangen, die Daten über sie enthalten, verlangen (Art. 8 DSGVO); darunter fallen auch Angaben über die Herkunft der Daten, den Zweck und gegebenenfalls die Rechtsgrundlagen des Bearbeitens, die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger.
- Das Auskunftsrecht steht ihr grundsätzlich voraussetzungslos zu.
- Die Modalitäten der Einsichtnahme sind im Einvernehmen mit dem Inhaber der Datensammlung bzw. dem Bankinstitut zu regeln (vgl. Art. 1 Abs. 3 VDSG). Es wird empfohlen, in die Dokumente, welche Personendaten der betroffenen Person enthalten und an Dritte/US-Behörden übermittelt werden sollen, an Ort und Stelle Einsicht zu nehmen, und Kopien oder Ausdrücke davon zu verlangen.
- Häufig werden Standardschreiben verwendet, die lediglich mögliche Kategorien von Dokumenten auflisten, und es bleiben darin Datenempfänger unklar bzw. sie werden nur pauschal umschrieben („US Department of Justice“ or other authorities). Weiter muss für die betroffene Person auch ersichtlich sein, wie die Bank die Personendaten der betroffenen Person bekannt zu geben gedenkt (Codierungen, Einschwärzungen usw.); die betroffene Person muss allfällige Pseudonymisierungen erkennen können. Es ist daher zu fordern, dass die betroffene Person sowohl in die nicht eingeschwärzten wie auch in die eingeschwärzten Dokumente, wie sie zur beabsichtigten Übermittlung vorbereitet sind, Einsicht nehmen kann und ihr davon Kopien oder Ausdrücke ausgehändigt werden²¹. Nur durch einen solchen Vergleich lassen sich Umfang und Tragweite der Übermittlung erkennen. Es ist davon auszugehen, dass solche Personendaten und Informationen zu einem bestimmten Konto – auch wenn dieses nicht mittels Kundennamen und Kontonummer bezeichnet ist – letztendlich der Identifikation des Kontoinhabers im Hinblick auf ein Rechtshilfeverfahren dient.

Bei der Ausübung des Auskunftsrechts stellen sich u.a. folgende Fragen:

- Erfolgt die Information seitens des Bankinstituts über die beabsichtigte Datenübermittlung rechtzeitig, sodass eine angemessene Reaktion möglich ist?

²¹ Die Erstellung von Kopien haben die Zürcher Gerichte einem pensionierten Banker zugestanden (Bezirksgericht Zürich vom 14. Oktober 2013, CG120124-L/U; Obergericht Zürich vom 28. Februar 2014).

- Welche Daten sind über die betroffene Person in ihrer Gesamtheit vorhanden? (Grundsätzlich hat eine Person ein Auskunftsrecht über die Gesamtheit der sie betreffenden Daten.)
- Welches ist der Umfang der beabsichtigten Übermittlung von Personendaten (betrifft die Übermittlung mehrere Personen, mehrere Dokumente, verschiedene Listen usw.)?
- Welche Dokumente sollen im Einzelnen übermittelt werden?
- Aus welchen Zeiträumen stammen die Personendaten und die Dokumente, welche übermittelt werden sollen?
- Werden die Personendaten eingeschwärzt inkl. Kontodaten und Personenidentifikator?
- Handelt es sich um anonymisierte Personendaten, die keinen Rückschluss auf die betroffene Person ermöglichen²²?
- Oder handelt es sich um pseudonymisierte Personendaten, die anhand eines bestimmten Schlüssels oder eines Personenidentifikators Rückschlüsse auf die betroffene Person zulassen?
- Welches sind die Datenempfänger? Kategorien von möglichen Datenempfängern? Werden die Personendaten an einen „Independent Examiner“ übermittelt? Wenn ja, findet diesfalls bereits eine Bekanntgabe von Personendaten ins Ausland statt?
- Wurden zusätzliche Daten bei Dritten beschafft? Welches ist die Herkunft dieser Daten?
- Zu welchem Zweck werden die Personendaten bekanntgegeben?
- Werden Codierungen verwendet, die für die betroffene Person nicht verständlich sind?
- Sind die Personendaten, die übermittelt werden sollen, richtig?

Sind keine Daten vorhanden muss dies auch entsprechend mitgeteilt werden²³.

²² Zur Unterscheidung von Anonymisierung und Pseudonymisierung, vgl. Rosenthal, N 36 zu Art. 3 dSG.

²³ Vgl. zum Auskunftsrecht Rosenthal/Jöhri, Handkommentar zum Datenschutzgesetz, N 13 ff. zu Art. 8 DSG.

Stellt die betroffene Person fest, dass Daten unrichtig sind, soll sie auf jeden Fall deren Berichtigung verlangen (Art. 5 Abs. 2 DSGVO). Dieser Anspruch auf Berichtigung kann jederzeit, mündlich oder schriftlich geltend gemacht werden.

Wird das Auskunftsrecht verweigert oder eingeschränkt, lohnt es sich wohl nicht, das Auskunftsrecht gerichtlich durchzusetzen²⁴. In der vorliegenden Konstellation ist vielmehr gleich Klage betreffend Verbot der Datenbekanntgabe einzureichen.

3. Zivilrechtliche Klage

Beharrt das Bankinstitut auf der Datenübermittlung, verbleibt der betroffenen Person gestützt auf Art. 15 Abs. 1 DSGVO einzig den Klageweg zu beschreiten.

Die Musterverfügung des Bundesrates weist in Ziffer 1.4.c. auf den Klageweg hin und sieht als Auflage ausdrücklich vor, dass eine allfällige Datenübermittlung erst nach rechtskräftiger Abweisung der Klage erfolgen darf.

3.1 Klage

Es ist bei einer widerrechtlichen Verletzung der Persönlichkeit nach Massgabe von Art. 28 und 28a ZGB zu klagen. Die betroffene Person kann insbesondere verlangen, dass dem Bankinstitut verboten wird, die Daten an US-Behörden zu übermitteln.

Gerichtsstand: Am Ort einer der Parteien (Art. 20 Bst. a und d ZPO)

Verfahren: Ordentliches Verfahren nach Art. 219 ff. ZPO, welches mit einem Schlichtungsgesuch nach Art. 202 ff. ZPO einzuleiten ist.

²⁴ Das Auskunftsrecht ist im vereinfachten Verfahren nach eidg. ZPO durchzusetzen (vgl. Art. 15 Abs. 4 DSGVO i.V.m. Art. 243 Abs. 2 Bst. d ZPO).

Rechtsbegehren: Die Rechtsbegehren sind aufgrund der Umstände des Einzelfalles zu formulieren. Primär geht es im vorliegenden Kontext darum, die drohende Verletzung der Persönlichkeitsrechte durch Übermittlung von Personendaten an ausländische bzw. US-Behörden zu verbieten²⁵. Nach Möglichkeit ist das Rechtsbegehren detailliert zu fassen.

Empfohlen wird, Vollstreckungsmassnahmen nach Art. 343 Abs. 1 ZPO zu verlangen, insbesondere die Anordnung der Strafdrohung nach Art. 292 StGB.

Legitimation: Aktivlegitimiert ist die betroffene Person im Sinne von Art. 3 Bst. b DSGVO.

Passivlegitimiert ist das Bankinstitut; das Verhalten ihrer Organe ist der juristischen Person anzurechnen. Die Passivlegitimation definiert sich nach Massgabe der Persönlichkeitsverletzung.

Rechtsschutzinteresse: Eine drohende Rechtsverletzung zu verbieten, setzt ein entsprechendes Rechtsschutzinteresse voraus. Dieses liegt vor, wenn die widerrechtliche Handlung unmittelbar droht, d.h. wenn das Verhalten des Beklagten die Handlung befürchten lässt (BGE 124 III 74).

3.2 Vorsorgliche und superprovisorische Massnahmen

Es drängt sich nach dem Gesagten allenfalls auf, den Antrag zu stellen, dem Bankinstitut superprovisorisch bzw. vorsorglich zu verbieten, Dokumente mit Personendaten der betroffenen Person den US-Behörden zu übermitteln. Dieses Begehren kann auch vor der Rechtshängigkeit der Klage gestellt werden (vgl. Art. 263 ZPO). Dieses Vorgehen drängt sich insbesondere dann auf, wenn aufgrund der zeitlichen Dringlichkeit oder besonderer Umstände sich Zweifel aufdrängen, ob tatsächlich mit der Datenübermittlung zugewartet wird.

Zwar enthält die Musterverfügung des Bundesrates ebenfalls für den Fall der Missachtung der Auflagen die Strafdrohung von Art. 292 StGB. Der Vorteil eines Gesuchs um superprovisorische resp. vorsorgliche Massnahmen besteht – Gutheissung des Begehrens vorausgesetzt – darin,

²⁵ Allenfalls kann sich auch aufdrängen zu verlangen, dass unrechtmässig beschaffte Daten zu vernichten sind (vgl. BSK-Rampini, N 8 zu Art. 15 DSGVO).

dass die Strafdrohung auf den konkreten Fall bezogen ausgesprochen werden kann.

Die Herausforderung für den Anwalt besteht allenfalls darin, ohne detaillierte Angaben - mangels Ausübung des Auskunftsrechts - das Gesuch hinreichend zu begründen - unter Darlegung einer Hauptsachen- und Nachteilsprognose.

Zum Schluss:

Die Situation des Anwalts ist delikat. Es drängt sich auf, dass er sehr früh von den Möglichkeiten zur Verhinderung einer Datenübermittlung Gebrauch macht.

Quellen:

Hinweise auf Websites:

Staatssekretariat für internationale Finanzfragen SIF zum US-Steuerstreit

<http://www.sif.admin.ch/themen/00502/00806/index.html?lang=de>

Joint-Statement zwischen dem US-Justizdepartement und dem Eidgenössischen Finanzdepartement

<http://www.news.admin.ch/NSBSubscriber/message/attachments/31813.pdf>

Link zum US-Programm

<http://www.justice.gov/opa/pr/2013/August/13-tax-975.html>

Vorlagen:

Auskunftsersuchen:

<http://www.edoeb.admin.ch/datenschutz/00628/00638/00640/index.html?lang=de>

Literatur:

David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz,
Zürich 2008

Gerichtsurteile

Obergericht Zürich

http://www.gerichte-zh.ch/fileadmin/user_upload/entscheide/oeffentlich/LB130059.pdf

Bezirksgericht Zürich:

http://www.gerichte-zh.ch/fileadmin/user_upload/entscheide/oeffentlich/CG120124-L.pdf