Banken und Datenschutz

Susan Emmenegger (Hrsg.)

Institut für Bankrecht, Universität Bern

SBT 2019 – Schweizerische Bankrechtstagung 2019

Banken und Datenschutz

herausgegeben von Susan Emmenegger

mit Beiträgen von
Konrad Meier
Monika Pfaffinger
Martina Reber
Andrea Opel
Adrian Hug
David Rosenthal/Barbara Epprecht
Susan Emmenegger/Martina Reber
David Vasella

Helbing Lichtenhahn Verlag

Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Die Druckvorlagen wurden von der Herausgeberin reprofertig geliefert.

ISBN 978-3-7190-4269-1

www.helbing.ch

Vorwort

Daten sind längst zur Währung geworden und als Wirtschaftsfaktor wohl wichtiger denn je. Umgekehrt ist aufgrund zahlreicher Skandale in der jüngeren Vergangenheit das Bewusstsein für den Datenschutz gewachsen, was sich auch auf der Gesetzgebungsebene zeigt. Spätestens seit Inkrafttreten der europäischen Datenschutz-Grundverordnung (DSGVO) fristet das Datenschutzrecht nicht mehr das Mauerblümchen-Dasein eines rechtlichen Randgebietes, sondern ist zur wichtigen Compliance-Materie avanciert. Dies betrifft gerade auch die Banken, da sie über gewaltige Datenschätze verfügen. Dass das Datenschutzrecht bankaufsichtsrechtlich relevant ist, zeigt der Beitrag von KONRAD MEIER.

Eine Herausforderung besteht für viele Schweizer Banken darin, nicht nur das schweizerische Datenschutzrecht, sondern auch die DSGVO einzuhalten. MONIKA PFAFFINGER erläutert die extraterritoriale Wirkung dieser Verordnung und die konkreten Pflichten, die sie den Banken auferlegt. Eine dieser Pflichten ist es, bereits ab der Planung einer Datenbearbeitung gewissermassen einen «eingebauten Datenschutz» vorzusehen (Privacy by Design). Damit und mit der Frage, wie Banken diese Pflicht umsetzen können, befasst sich MARTINA REBER.

Ein an der Tagung heiss diskutiertes Thema war die Amtshilfepraxis der Eidgenössischen Steuerverwaltung. ANDREA OPEL kritisiert diese Praxis, insbesondere die Übermittlung ungeschwärzter Namen von Bankmitarbeitenden. Den Kontrapunkt bildet der Beitrag von ADRIAN HUG, der die Sicht der Steuerverwaltung darlegt.

Wer bin ich – und wenn ja wie viele? Diese Frage von Richard David Precht dürften sich auch die Banken gelegentlich stellen, wenn sie eruieren müssen, ob sie bei einer bestimmten Datenbearbeitung Verantwortliche, Auftragsbearbeiter oder gemeinsam Verantwortliche sind. Licht ins Dunkle bringt der Beitrag von DAVID ROSENTHAL und BARBARA EPPRECHT.

SUSAN EMMENEGGER und MARTINA REBER haben untersucht, inwieweit das neue Datenschutzrecht Anpassungen der AGB erfordert. Dabei verlagerten sie den Schwerpunkt zunehmend auf die Bearbeitung biometrischer Daten, die aber längst nicht immer in AGB geregelt ist. In ihrem Beitrag fokussieren sie sich nun ganz auf die biometrischen Daten im Bankkundenverkehr und prüfen ein Stimmauthentifizierungsverfahren auf seine Zulässigkeit.

Profiling. Der Begriff erinnert an Kriminalfilme, wird aber auch im Datenschutzrecht verwendet. DAVID VASELLA erklärt, wann ein Profiling

vorliegt, wann es rechtmässig ist und welche zusätzlichen Pflichten es mit sich bringt.

Ich möchte den Referierenden ganz herzlich danken für ihre anregenden und bereichernden Referate. Dank gebührt auch dem Team des Instituts für Bankrecht, welches mich in allen Belangen unterstützt hat. Herzlichen Dank für Euren tollen Einsatz! Besonders danke ich LESLIE ANN SOMMER und RAMIN PAYDAR für die Federführung bei der Organisation der Tagung, und MARTINA REBER, die zu diesem Band nicht nur als Autorin beigetragen hat, sondern auch für dessen Erstellung verantwortlich zeichnet.

Bern, im Juni 2019 *Susan Emmenegger*

Inhaltsübersicht

Bankaufsichtsrechtliche Relevanz des Datenschutzgesetzes

Konrad Meier, Zürich*

* Konrad Meier, Senior Manager, Head Data Privacy Law, Ernst & Young AG, Zürich. Ich danke herzlich Herrn RA Christian Perren, Ernst & Young AG, für die Unterstützung bei der Verfassung dieses Beitrages.

I. Einleitung

Der Datenschutz befindet sich gegenwärtig im Wandel: Mit der Anwendbarkeit der EU Datenschutz-Grundverordnung (DSGVO) seit dem 25. Mai 2018 und der bevorstehenden Totalrevision des Schweizerischen Datenschutzgesetzes müssen sich insbesondere die durch die FINMA[1] beaufsichtigten Finanzdienstleister die Frage stellen, wie der Stellenwert des Datenschutzes im Aufsichtsrecht zu beurteilen ist.

Es geht hierbei nicht nur um die Einhaltung rechtlicher und regulatorischer Vorschriften des Datenschutzes. Das Thema ist unlängst zu einem «Politikum» bei den Konsumenten geworden, weshalb die Tragweite des Datenschutzes über die reine Compliance hinausgeht. Nachfolgend soll dargestellt werden, wie der Stellenwert des Datenschutzrechts im Zusammenhang mit dem Finanzmarktaufsichtsrecht zu beurteilen ist.

II. Dimensionen des Aufsichtsrechts aus Sicht des Datenschutzes

1. Finanzmarktaufsichtsgesetz (FINMAG)

Die rechtlichen Grundlagen für die Ausübung der Finanzmarktaufsicht durch die FINMA finden sich in Art. 1 FINMAG, wobei namentlich folgende Finanzmarktgesetze im Vordergrund stehen:

- Pfandbriefgesetz
- Versicherungsvertragsgesetz
- Kollektivanlagengesetz
- Bankengesetz
- Börsengesetz
- Geldwäschereigesetz
- Versicherungsaufsichtsgesetz
- Finanzmarktinfrastrukturgesetz

Das Finanzdiensleistungsgesetz (FIDLEG) und das Finanzinstitutsgesetz (FINIG) werden obenstehende Liste nach ihrem Inkrafttreten – voraussichtlich per 1. Januar 2020 – ergänzen.

[1] Eidgenössische Finanzmarktaufsicht (FINMA).

Das Datenschutzgesetz als solches ist somit nicht Teil der Finanzmarktgesetze, welche die Grundlage für das Aufsichtsrecht bilden. Wo im Rahmen der Bankenaufsicht dennoch inhaltliche Anknüpfungspunkte zum Datenschutz bestehen, wird in den nachfolgenden Kapiteln ausgeführt.[2]

2. Verlautbarungen der FINMA

Die FINMA konkretisiert die in den Finanzmarktgesetzen enthaltenen aufsichtsrechtlichen Bestimmungen in zahlreichen Rundschreiben, Stellungnahmen und Aufsichtsmitteilungen.[3]

Aus Datenschutzsicht sind insbesondere das alte und das neue Outsourcing-Rundschreiben (FINMA-RS 08/7 bzw. FINMA-RS 2018/3), der Anhang 3 («Umgang mit elektronischen Kundendaten») zum Rundschreiben «Operationelle Risiken Banken» (FINMA-RS 2008/21) sowie das Rundschreiben «Direktübermittlung» (FINMA-RS 2017/6) von Bedeutung. Die vorgenannten Rundschreiben enthalten z.T. sehr spezifische Referenzen ins Datenschutzgesetz, womit diese für die Banken, die Bankenaufsicht und die Prüfgesellschaften relevant werden. Darüber hinaus verweist der Anhang 3 zum FINMA-RS 08/21 auch auf die einschlägigen Leitfäden[4] des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

Daneben gibt es diverse Stellungnahmen und Aufsichtsmitteilungen der FINMA, welche ebenfalls datenschutzrechtliche Sachverhalte adressieren. Erwähnt sei etwa die FINMA-Mitteilung 3 (2009) bezüglich der erforderlichen Kundeninformation über Restrisiken im Zahlungs- und Wertschriftenverkehr.[5]

---

[2] Auf das spezifisch auf den Kunden ausgerichtete Bankkundengeheimnis gemäss Art. 47 BankG wird im Rahmen dieses Beitrages nicht näher eingegangen.

[3] Siehe Dokumentationsübersicht der FINMA unter: <https://www.finma.ch/de/dokumentation>.

[4] Leitfäden des EDÖB zu den technischen und organisatorischen Massnahmen des Datenschutzes vom August 2015 (<https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html>) sowie für die Übermittlung von Personendaten ins Ausland (<https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html>).

[5] FINMA, Mitteilung Nr. 3 vom 17. Juni 2009 an alle Banken und Effektenhändler.

III. Anknüpfungspunkte zum Datenschutzrecht

Nachdem oben dargelegt wurde, dass der Datenschutz durchaus eine Rolle spielt im Finanzmarktaufsichtsrecht, sollen die wichtigsten aufsichtsrechtlichen Anknüpfungspunkte zum Datenschutzrecht nachfolgend näher erläutert werden.

1. FINMA Rundschreiben 08/7 und 2018/3 «Outsourcing»

Per 1. April 2018 hat das neue Outsourcing-Rundschreiben 2018/3 die Vorgängerversion 2008/7 abgelöst. Eine der wichtigsten Änderungen bezieht sich auf den Anwendungsbereich des Rundschreibens, welches nebst den Banken neu auch die Versicherungsunternehmen adressiert.

In Bezug auf den Datenschutz hat sich ebenfalls ein Paradigmenwechsel vollzogen: Das neue Rundschreiben enthält keinerlei Referenzen mehr auf das Datenschutzgesetz, wie dies im alten Rundschreiben z.T. prominent der Fall war. So wurde bereits in der Zweckbestimmung (Rz. 1 des alten Rundschreibens) festgehalten, dass das Rundschreiben die Voraussetzungen umschreibt, unter welchen eine Outsourcinglösung den *Erfordernissen des Datenschutzes* entspricht. Ferner enthielt das Rundschreiben weitere, spezifische Verweise auf das Datenschutzgesetz; so zum Beispiel im Grundsatz 4 (Sicherheit; Rz. 28 f. des alten Rundschreibens), wo auf Art. 7 DSG (Datensicherheit) und auf die Art. 8 und 9 VDSG (Verordnung zum DSG) verwiesen wurde. Ferner wurde auch im Zusammenhang mit der Auslagerung ins Ausland (Rz. 34 f. des alten Rundschreibens) festgehalten, dass der *Datenschutz nach schweizerischem Recht einzuhalten ist*.

Die FINMA hat die Streichung dieser datenschutzrechtlichen Verweise im Erläuterungsbericht zum neuen Rundschreiben wie folgt begründet:[6]

> «Der Umgang mit Personendaten wird in der Schweiz vom Datenschutzgesetz (DSG; SR 235.1), der Datenschutzverordnung (VDSG; SR 235.11) sowie weiteren Rechtsquellen umfassend geregelt, […]. Für Banken ist bezüglich des Bankkundengeheimnisses ferner Art. 47 BankG zu beachten. Der Umgang von Banken mit elektronischen Kundendaten wird sodann im Anhang 3 des FINMA-RS 08/21 geregelt. Um Doppelspurigkeiten und allfällige Divergenzen zu den Entwicklungen des Datenschutzrechts zu vermeiden und gleichzeitig eine klare Abgrenzung zwischen aufsichtsrechtlichen Anforderungen der Finanzmarktaufsicht und den im Privatrecht angesiedelten

[6] FINMA, Erläuterungsbericht zum Rundschreiben 2018/3 «Outsourcing – Banken und Versicherer», S. 12 ff.

> Pflichten gemäss Datenschutzgesetz zu gewährleisten, werden die bisherigen Ausführungen im FINMA-RS 08/07 mit Bezug zum Datenschutz (vgl. dessen Rz. 31–33, Rz. 36 und Rz. 37–39) gestrichen. Aus denselben Gründen wird der ehemalige Grundsatz 6 (Kundenorientierung) aufgehoben, mit dem das FINMA-RS 08/7 über die datenschutzrechtlichen Anforderungen hinaus ging, insbesondere mit Bezug auf die umfassenden Informationspflichten und das ausserordentliche Kündigungsrecht gemäss Rz. 39 des FINMA-RS 08/07.»

Weiter hält die FINMA aber deutlich fest:

> «Mit der Streichung der Ausführungen zum Datenschutz sind *keine materiellen Verschärfungen oder Erleichterungen* verbunden. Die Streichung des Grundsatzes „Kundenorientierung" stellt eine Erleichterung für Banken dar. Hier entfällt insbesondere das aufsichtsrechtlich angeordnete, ausserordentliche Kündigungsrecht sowie die Informationspflicht, soweit sich eine solche nicht aus anderen Rechtsquellen ergibt.»

Die Vermeidung von oben genannten Doppelspurigkeiten ist demnach durchaus im Kontext der Totalrevision des Datenschutzgesetzes zu sehen. Der Entwurf zum neuen Datenschutzgesetz[7] sieht mitunter signifikante zusätzliche Informationspflichten vor, welche gerade auch bei Auslagerungen eine Rolle spielen und im alten Rundschreiben explizit thematisiert wurden (vgl. Rz. 37 f. des alten Rundschreibens). Des Weiteren sieht der Entwurf eine massive Stärkung der Stellung des EDÖB vor, welcher zukünftig als echte Datenschutzaufsichtsbehörde mit den dazu notwendigen Aufsichtsinstrumenten versehen wird.[8] Vor diesem Hintergrund erscheint die Streichung der datenschutzrechtlichen Bestimmungen im neuen Rundschreiben durchaus als gerechtfertigt.

Die Änderungen wurden im Rahmen der Anhörung mehrheitlich begrüsst; so zum Beispiel die Stellungnahme der Schweizerischen Bankiervereinigung (SBVg), welche wie folgt lautete:

> «Wir können den Verzicht auf die Regelung der datenschutzrechtlichen Aspekte nachvollziehen. Dieser Verzicht hat zur Folge, dass der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) bezüglich datenschutzrechtlicher Aspekte im Rahmen des Outsourcings eine noch zentralere Rolle spielen wird. Es ist deshalb wichtig, dass sich die FINMA mit dem

---

[7] Entwurf vom 15. September 2017 zur Totalrevision des Bundesgesetzes über den Datenschutz, BBl 2017 7193.

[8] Z.B. erweiterte und eigenständige Untersuchungsbefugnisse sowie die Möglichkeit, selbständig Verfügungen zu erlassen (unter geltendem Recht können Verfügungen nur durch das Bundesverwaltungsgericht erlassen werden).

> EDÖB koordiniert, zumal dieser zukünftig allenfalls auch Verfügungen erlassen soll.»[9]

Es gab vereinzelt aber auch kritische Stimmen. So bemerkte der Verband Schweizerischer Kantonalbanken (VSKB) in seiner Stellungnahme:

> «Wir möchten darauf hinweisen, dass der Bundesrat am 21. Dezember 2016 den Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes (DSG) und die Änderung weiterer Erlasse zum Datenschutz in die Vernehmlassung gegeben hat. […] Wir sind sehr besorgt darüber, dass unüberlegte Verschärfungen des DSG bei Beibehaltung der Absicht der FINMA, sämtliche Bestimmungen mit datenschutzrechtlichem Gehalt aus dem bestehenden Rundschreiben Outsourcing zu streichen, den Handlungsspielraum der Banken unnötig einschränken könnte. Die Banken brauchen v.a. zeitnah griffige und einfach anwendbare Regelungen.»[10]

2. Anhang 3 zum FINMA Rundschreiben 08/21 „Operationelle Risiken Banken: Umgang mit elektronischen Kundendaten“

Der Anhang 3 zum FINMA-RS 08/21 adressiert das sachgerechte Management von Sicherheitsrisiken im Umgang mit elektronischen Kundendaten natürlicher Personen.[11] Im Zentrum steht somit der kundenseitige Datenschutz, weshalb sich zahlreiche Verweise auf datenschutzrechtliche Bestimmungen im Anhang 3 finden.

Im ersten Absatz (vgl. Rz. 1 des Anhang 3) wird explizit auf das Datenschutzrecht referenziert und zwar insbesondere auf die Art. 7 DSG sowie Art. 8 f. VDSG. Art. 7 DSG statuiert die Pflicht, angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu ergreifen und verweist des Weiteren auf die Konkretisierung dieser Pflicht in Art. 8 f. VDSG. Dabei steht die Vertraulichkeit, Verfügbarkeit und die Integrität der elektronisch bearbeiteten Kundendaten im Vordergrund, während die Rechtmässigkeit der Datenbearbeitung an sich nicht thematisiert wird.

Der Anhang 3 verweist ferner auf den einschlägigen Leitfaden «Technische und organisatorische Massnahmen des Datenschutzes»[12] des EDÖB, wel-

---

[9] SBVg, Stellungnahme zum FINMA-Rundschreiben 2018/3 «Outsourcing – Banken und Versicherer», S. 2.

[10] VSKB, Stellungnahme zum FINMA-Rundschreiben 2018/3 «Outsourcing – Banken und Versicherer», S. 3 f.

[11] Vgl. FINMA-RS 08/21 «Operationelle Risiken – Banken», Anhang 3, Rz. 1.

[12] Vgl. Fn. 6.

cher allerdings seit August 2015 nicht mehr aktualisiert wurde. Nicht nur deswegen sind in diesem Zusammenhang auch die gute Praxis bzw. der gegenwärtige Stand der Technik zu berücksichtigen.[13]

Eine weitere Referenz ins Datenschutzgesetz befindet sich in Rz. 20 des Anhang 3, wo der Datenspeicherort und -zugriff im Ausland thematisiert wird. Verwiesen wird hier auf Art. 6 DSG, welcher die Voraussetzungen für die grenzüberschreitende Bekanntgabe von Personendaten auflistet: Im Zentrum steht dabei die Frage, ob der Datentransfer in ein Land mit einem angemessenen Datenschutzniveau stattfindet bzw. wie bei Fehlen der Angemessenheit ein Datentransfer dennoch gerechtfertigt werden kann (z.B. durch die Einwilligung der betroffenen Personen oder durch hinreichende vertragliche Garantien zwischen Exporteur und Importeur).

3. Art. 72 f. Finanzdienstleistungsgesetz (FIDLEG)

Das FIDLEG beinhaltet keine direkte bzw. explizite Referenz zum Datenschutzrecht; allerdings kennt es ein dem Datenschutz bekanntes Rechtsinstitut, nämlich den Herausgabeanspruch von Dokumenten gemäss Art. 72 f. FIDLEG, welcher dem Auskunftsrecht nach Art. 8 DSG ähnelt.

Voraussetzung für eine effektive Durchsetzung materiellen Rechts ist die ausreichende Kenntnis über eine Geschäftsbeziehung, sowohl für die Finanzdienstleister selbst als auch für ihre Kunden. Da den Dokumenten, welche ein Finanzdienstleister im Rahmen einer Kundenbeziehung erstellt, eine zentrale Bedeutung zukommt, sieht das FIDLEG diesen allgemeinen Herausgabeanspruch jedes Kunden vor. Der Anspruch bezieht sich dabei auf die Herausgabe einer Kopie der sie oder ihn betreffenden Dokumente. Die Botschaft zum FIDLEG präzisiert, dass der Gegenstand der Herausgabepflicht das Kundendossier ist, also alle physischen und elektronischen Dokumentationen, zu deren Erstellung der Finanzdienstleister gemäss FIDLEG verpflichtet ist.[14] Rein interne Dokumente wie vorbereitende Studien, (Vertrags-)Entwürfe oder andere Dokumente, die für die Überprüfung des vertrags- und gesetzeskonformen Verhaltens des Finanzdientleisters nicht relevant sind, müssen nicht herausgegeben werden.[15]

Zur Geltendmachung des Herausgabeanspruchs ist vom Kunden ein schriftliches Gesuch an den Finanzdienstleister zu richten (Art. 73 Abs. 1

[13] Art. 8 Abs. 2 lit. d VDSG.

[14] Vgl. Botschaft FIDLEG/FINIG, BBl 2015 8995 f. Ziff. 4.

[15] Vgl. Botschaft FIDLEG/FINIG, BBl 2015 8995 f. Ziff. 4.

FIDLEG). Nach dessen Erhalt hat der Finanzdienstleister innert 30 Tagen die betreffenden Dokumente an den Kunden kostenlos herauszugeben (Art. 73 Abs. 2 FIDLEG). Sollte der Finanzdienstleister seiner Pflicht nicht nachkommen, so kann der Kunde das Gericht anrufen (Art. 73 Abs. 3 FIDLEG). Dies geschieht im summarischen Verfahren, um eine zeit- und kosteneffiziente Durchführung zu gewährleisten.[16] Des Weiteren kann eine Weigerung oder unvollständige Herausgabe des Finanzdienstleisters in einem späteren Rechtsstreit zwischen den Parteien beim Entscheid über die Zuteilung der Prozesskosten berücksichtigt werden (Art. 73 Abs. 4 FIDLEG).

Im Verhältnis zum Auskunftsrecht nach Art. 8 DSG gibt es diverse nennenswerte Unterschiede: Zunächst bezieht sich der sachliche Anwendungsbereich des datenschutzrechtlichen Auskunftsrechts nur auf Personendaten, auch wenn in der Praxis die herauszugebenden Dokumente bei beiden Ansprüchen zu einem grossen Teil dieselben sein dürften. Auf alle Fälle statuiert der Rechtsanspruch nach FIDLEG ausdrücklich, dass Kopien herauszugeben sind, während dies aus Art. 8 f. DSG nicht ohne Weiteres hervorgeht. Gemäss Art. 8 Abs. 2 DSG ist jedoch zusätzlich erforderlich, dass dem Gesuchsteller Auskunft gegeben wird über die Herkunft der Daten, Zweck der Datenbearbeitung, Rechtsgrundlagen der Bearbeitung, die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten sowie die Datenempfänger. Diesbezüglich geht das datenschutzrechtliche Auskunftsrecht weiter als der Herausgabeanspruch nach FIDLEG.

Für beide Ansprüche gilt, dass keine spezifischen Gründe erforderlich sind, um Auskunft oder Herausgabe zu verlangen; die persönliche Eigenschaft des Gesuchstellers als Kunde i.S. des FIDLEG bzw. als betroffene Person i.S. des DSG ist ausreichend. Sodann sind die beiden Rechtsansprüche kumulativ anwendbar, allenfalls zusammen mit anderen bestehenden vertraglichen, gesetzlichen und zivilprozessualen Informationsansprüchen.[17]

Der anspruchsberechtigte Personenkreis ist zumindest nach geltendem Recht bei beiden Ansprüchen derselbe: Er umfasst natürliche wie auch juristische Personen. Mit Inkrafttreten des revidierten Schweizer Datenschutzgesetzes wird sich dies jedoch ändern, da juristische Personen fortan nicht mehr betroffene Personen im Sinne des DSG sind und somit vom datenschutzrechtlichen Auskunftsrecht keinen Gebrauch mehr machen können.

[16] Vgl. Botschaft FIDLEG/FINIG, BBl 2015 8924 Ziff. 1.4.4.

[17] Vgl. DOMMER, sui-generis 2018, S. 224 f. Rz. 10.

4. FINMA Rundschreiben 2017/6 «Direktübermittlung»

Art. 42c FINMAG räumt den Finanzdienstleistern die Möglichkeit ein, unter bestimmten Voraussetzungen nicht öffentliche Informationen direkt an ausländische Behörden und Stellen zu übermitteln. Das Rundschreiben «Direktübermittlung» legt den Gesetzesartikel näher aus. Damit unterstützt es die Finanzdienstleister bei der einheitlichen Anwendung der Norm und hilft ihnen, die damit verbundenen Risiken zu minimieren.[18] Nebst der Erläuterung der Voraussetzungen für die Direktübermittlung werden die Umstände ausgeführt, unter welchen eine vorgängige Meldung der beabsichtigten Übermittlung an die FINMA zu erfolgen hat.[19]

In Bezug auf den Datenschutz hält das Rundschreiben Folgendes in Rz. 30 und 31 fest:

> «Bezüglich der Rechte von Kunden und Dritten haben die Beaufsichtigten unter anderem das Geschäfts- und Bankkundengeheimnis, die *Bestimmungen über den Datenschutz* sowie die Rechte aus dem Arbeitsverhältnis zu wahren. Die im konkreten Fall zu treffenden Vorkehrungen bestimmen sich nach dem jeweils anwendbaren Schweizer Recht. Die Erfüllung dieser rechtlichen Voraussetzungen liegt in der Verantwortung der Beaufsichtigten.»

Analog zum Outsourcing-Rundschreiben 2018/03 belässt es die FINMA somit bei einer simplen Referenz auf das Datenschutzgesetz und verzichtet auf spezifischere Ausführungen.

Im Erläuterungsbericht zum Rundschreiben präzisiert die FINMA beispielhaft, was die Wahrung der Rechte im Bereich des Datenschutzes bedeuten könnte:

> «Die Rechte von Kunden und Dritten, welche bei einer Übermittlung im Sinne von Art. 42c Abs. 1 FINMAG zu wahren sind, ergeben sich vor allem aus dem Geschäfts- und Bankkundengeheimnis, dem Datenschutz- oder dem Arbeitsrecht. Denkbar ist beispielsweise – abhängig von den im konkreten Fall zu wahrenden Rechten – *die Zustimmung der betroffenen Kunden oder Dritten zur Übermittlung einzuholen oder die Passagen, die Rückschlüsse auf deren Identität zulassen, zu schwärzen.* Wie diese Rechte im konkreten Anwendungsfall gewahrt werden, liegt in der Verantwortung der Beaufsichtigten.»[20]

---

[18] FINMA, Erläuterungsbericht zum Rundschreiben 2017/6 «Direktübermittlung», S. 4.

[19] FINMA-RS 17/6 «Direktübermittlung», Rz. 43 ff.

[20] FINMA, Erläuterungsbericht zum Rundschreiben 2017/6 «Direktübermittlung», 7. Juli 2016, S. 10.

Im Rahmen der Anhörung wurde diese Sichtweise der FINMA wiederholt von den betroffenen Finanzdienstleistern kritisiert. Dahingehend wurde im Rahmen der Anhörung zum Entwurf des Rundschreibens von der UBS und der Schweizerischen Bankiervereinigung (SBVg) gefordert, dass die FINMA konkret umschreiben sollte, welche Möglichkeiten zur Wahrung der Rechte von Kunden und Dritten bestehen.[21] Die FINMA hat diese Forderung im Anhörungsbericht abgelehnt und festgehalten:

> «Es liegt allein in der Verantwortung der Beaufsichtigten, die Rechte von Kunden und Dritten zu wahren. [...] Die FINMA gibt keine Empfehlungen ab, wie die Rechte von Kunden und Dritten zu wahren sind.»[22]

Berücksichtigt man die zuvor erwähnte Begründung der FINMA für die Streichung der datenschutzrechtlichen Bestimmungen im neuen Outsourcing-Rundschreiben, nämlich die Vermeidung von Doppelspurigkeiten, so erscheint die Haltung der FINMA in diesem Fall durchaus als stimmig. Es bleibt also auch hier bei einem einfachen Verweis auf das Datenschutzgesetz, welches im Rahmen der Direktübermittlung von den beaufsichtigten Banken einzuhalten ist.

IV. Blick nach Europa

Die vorstehenden Ausführungen haben gezeigt, dass das schweizerische Finanzmarktaufsichtsrecht datenschutzrechtliche Fragestellungen nur am Rande bzw. mittels Verweise ins Datenschutzgesetz adressiert. Spezifische Regelungen im Bereich des Datenschutzes möchte die FINMA bewusst nicht vorgeben und grenzt sich somit zu privatrechtlichen Bestimmungen ab, aber auch zum EDÖB, welcher die Aufsicht über die Einhaltung des Datenschutzes hat.

Die Schweizer Finanzmarktaufsicht folgt damit den europäischen Finanzmarktaufsichtsbehörden, welche datenschutzrechtliche Fragestellungen ebenfalls nicht gesondert regeln.[23] Auch bei diesen gilt die Praxis, dass Doppelspurigkeiten mit Bestimmungen, die zumindest formell nicht Teil des Finanzmarktaufsichtsrechts sind, möglichst vermieden werden sollen. Mit der

---

[21] FINMA, Bericht über die Anhörung vom 7. Juli bis 1. September 2016 zum Entwurf des Rundschreibens 2017/6 «Direktübermittlung», S. 17.

[22] FINMA, Bericht über die Anhörung vom 7. Juli bis 1. September 2016 zum Entwurf des Rundschreibens 2017/6 «Direktübermittlung», S. 17.

[23] Eine Ausnahme ist Polen, wo die Finanzmarktaufsicht zu datenschutzrechtlichen Fragestellungen eigenständig Position bezieht.

angestrebten Harmonisierung des Datenschutzrechts in der EU durch die DSGVO hat sich dieser Kurs der Finanzmarktaufsichtsbehörden gefestigt. Hinzu kommt, dass den Datenschutzaufsichtsbehörden in den EU-Mitgliedstaaten eine relativ starke Stellung zukommt. Vereinzelt bestehen aber auch Absprachen zwischen den Aufsichtsbehörden: So haben in Grossbritannien das Information Commissioner's Office (ICO) und die Financial Conduct Authority (FCA) in einem Memorandum of Understanding[24] die Aufsichtstätigkeiten im Bereich des Datenschutzes voneinander abgegrenzt bzw. wo angebracht, eine gemeinsame Kooperation vereinbart.[25]

V. Die aufsichtsrechtliche Prüfung in der Praxis

Die gesetzliche Grundlage für die aufsichtsrechtliche Prüfung durch die Wirtschaftsprüfungsgesellschaften findet sich in Art. 24 Abs. 1 lit. a FINMAG. Die Prüfung orientiert sich dabei gemäss Art. 24 Abs. 2 FINMAG an einem risikobasierten Aufsichtskonzept mit dem Kundenschutz im Fokus. Weiter ausgeführt wird die Prüfung der Beaufsichtigten durch die Prüfgesellschaften im FINMA Rundschreiben 2013/3 «Prüfwesen» und in den dazugehörigen Anhängen. Massgebend ist hierbei insbesondere der Anhang 2 «Standardprüfstrategie – Banken / Effektenhändler»,[26] welcher für jeden Aufsichtsbereich die minimale Standardprüfstrategie für die Basisprüfung vorgibt.

Ausgangspunkt jeder Prüfung ist zunächst im Rahmen der Risikoanalyse[27] die Bestimmung des Bruttorisikos bzw. des inhärenten Risikos,[28] welches einem Prüfgebiet zugrunde liegt; anschliessend werden die diesbezüglich implementierten Kontrollen beim Beaufsichtigten im Sinne eines Kontrollrisikos beurteilt. Aus der Gesamtbetrachtung von Brutto- und Kontrollrisiko ergibt sich schliesslich das sogenannte Nettorisiko. Dieses ist entscheidend und bestimmt die Prüftiefe sowie die Periodizität der Prüfung.[29]

---

[24] Abrufbar auf der Webseite des Information Commissioner's Office (ICO UK) unter: <https://ico.org.uk/media/2614342/financial-conduct-authority-ico-mou.pdf>.

[25] So könnte z.B. im Falle eines Verlustes von Kundendaten bei einer Bank das ICO und die FCA in gemeinsamer Abstimmung Aufsichtstätigkeiten wahrnehmen.

[26] Abrufbar auf der Webseite der FINMA unter: <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/2ueberwachung/pruefwesen-banken/anhang-02-darstellung-pruefstrategie-banken-kat-2-bis-5-20190101.pdf?la=de>.

[27] FINMA-RS 13/3 «Prüfwesen», Rz. 9.

[28] FINMA-RS 13/3 «Prüfwesen», Rz. 22-24.

[29] FINMA-RS 13/3 «Prüfwesen», Rz. 25, 79-85.

Die FINMA sieht im Rundschreiben 2013/3 zwei Prüftiefen vor:

– «*Prüfung:* Die Prüfgesellschaft muss sich ein vertieftes Bild über den zu prüfenden Sachverhalt verschaffen. Es ist ein eindeutiges Prüfurteil über die Einhaltung der aufsichtsrechtlichen Bestimmungen abzugeben (positive assurance).»[30]
– «*Kritische Beurteilung:* Die Prüfgesellschaft verschafft sich einen angemessenen Überblick über den zu prüfenden Sachverhalt. Der Prüfer nimmt Stellung dazu, ob sich im Rahmen der vorgenommenen Prüfungshandlungen (Durchsicht von Dokumenten, Befragungen usw.) Sachverhalte ergeben haben, aus denen zu schliessen wäre, dass die aufsichtsrechtlichen Bestimmungen nicht eingehalten werden (negative assurance).»[31]

Nachfolgend soll die Prüfstrategie beispielhaft anhand des FINMA Outsourcing Rundschreibens und des Anhang 3 zum FINMA Rundschreiben «Operationelle Risiken – Banken» aufgezeigt werden.

1. Aufsichtsrechtliche Prüfung im Rahmen des Outsourcing-Rundschreibens 2018/3

Seit dem 1. April 2018 richtet sich die Prüfung grundsätzlich nach dem neuen Rundschreiben 2018/3. Zu beachten sind jedoch die Übergangsbestimmungen im revidierten Rundschreiben: Banken und Effektenhändler haben 5 Jahre Zeit, um ihre bestehenden Auslagerungen an die Anforderungen des neuen Rundschreibens anzupassen; eine unmittelbare Anpassung ist nur dann notwendig, wenn nach dem Inkrafttreten neue Outsourcingverhältnisse abgeschlossen oder bestehende geändert werden.[32] Dies bedeutet, dass innerhalb der Übergangsfrist von 5 Jahren das alte Rundschreiben 08/7 auf vorbestehende Auslagerungen Anwendung finden kann, sofern diese nach Inkrafttreten des neuen Rundschreibens noch nicht angepasst oder geändert wurden. *Somit sind gegebenenfalls auch die datenschutzrechtlichen Bestimmungen des alten Rundschreibens während der Übergangsfrist noch relevant und Gegenstand der aufsichtsrechtlichen Prüfung*.[33]

---

30 FINMA-RS 13/3 «Prüfwesen», Rz. 33.

31 FINMA-RS 13/3 «Prüfwesen», Rz. 34.

32 FINMA-RS 18/3 «Outsourcing – Banken und Versicherer», Rz. 37.

33 Anders bei einer Prüfung basierend auf dem neuen Rundschreiben 2018/3, wo datenschutzrechtliche Aspekte aufgrund der Streichung der einschlägigen Bestimmungen nicht mehr geprüft werden.

Für das Thema Outsourcing sieht Anhang 2 zum Rundschreiben 2013/3 «Prüfwesen» folgende Prüftiefe bzw. Periodizität gemäss Standardprüfstrategie vor:

> «Graduelle Abdeckung der Elemente über 6 Jahre; für neue Outsourcing-Vereinbarungen Prüfung im ersten Jahr.»

Die «graduelle Abdeckung» bedeutet, dass die Prüfgesellschaften über 6 Jahre risikobasiert Prioritäten innerhalb des Themenbereichs setzen können. In Bezug auf die Prüftiefe gibt die FINMA vor, dass für neue Outsourcing-Vereinbarungen (also nach Inkrafttreten des neuen Rundschreibens) eine *Prüfung (i.S. einer positive assurance)* durchzuführen ist.[34]

2. Aufsichtsrechtliche Prüfung im Rahmen des Anhang 3 zum Rundschreiben «Operationelle Risiken Banken: Umgang mit elektronischen Kundendaten»

Für das Prüfgebiet Umgang mit elektronischen Kundendaten sieht Anhang 2 zum Rundschreiben 2013/3 «Prüfwesen» folgende Prüftiefe bzw. Periodizität gemäss Standardprüfstrategie vor:

> «Keine Intervention falls Nettorisiko tief; Prüfung alle 6 Jahre falls Nettorisiko mittel; Intervention alle 3 Jahre falls Nettorisiko hoch (abwechselnd kritische Beurteilung - Prüfung); jährliche Prüfung falls Nettorisiko sehr hoch.»[35]

Des Weiteren besteht für das Prüfgebiet ein detailliertes Prüfprogramm, welches den Prüfgesellschaften die minimalen Prüfungshandlungen vorgibt.[36] Dieses Prüfprogramm wurde von der FINMA zusammen mit den Prüfgesellschaften ausgearbeitet. Bemerkenswerterweise gibt es für das ebenso prominente Outsourcing-Thema (noch) kein von der FINMA erarbeitetes, offizielles Prüfprogramm; diesbezüglich arbeiten die Prüfgesellschaften mit eigens erstellten Prüfprogrammen.

---

[34] FINMA-RS 2013/3 «Prüfwesen», Anhang 2, S. 2.

[35] FINMA-RS 2013/3 «Prüfwesen», Anhang 2, S. 2.

[36] Abrufbar auf der Webseite der FINMA unter: <https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/2ueberwachung/pruefwesen-banken/pruefpunkte-vertraulichkeit-kundendaten.docx?la=de>.

VI. Zusammenfassung und Ausblick

Zunächst haben die vorstehenden Ausführungen gezeigt, dass im Finanzmarktaufsichtsrecht zahlreiche Anknüpfungspunkte zum Datenschutzgesetz bestehen. Auch wenn sich diese Anknüpfungspunkte mehrheitlich auf einfache Gesetzesverweise beschränken, so haben sie doch einen materiellen Gehalt, welcher von den beaufsichtigten Unternehmen nicht unterschätzt werden darf. Und soweit die FINMA datenschutzrechtliche Regelungen zukünftig unterlässt,[37] um Doppelspurigkeiten mit dem Privatrecht zu vermeiden, so bedeutet dies materiell keine Erleichterung in Bezug auf die datenschutzrechtlichen Anforderungen.

Darüber hinaus dürfte der Datenschutz in der Schweiz im Lichte der EU DSGVO und der Totalrevision des Schweizer Datenschutzgesetzes generell an Brisanz gewinnen. Dabei spielt auch die zukünftig stärkere Stellung des EDÖB eine wichtige Rolle: Die Finanzdienstleister müssen sich darauf einstellen, dass die Datenschutzbehörde von morgen mit ihren erweiterten Kompetenzen die Aufsicht pro-aktiver und konsequenter wahrnehmen wird.

[37] Vgl. oben die Ausführungen zu FINMA-RS 2013/3 «Prüfwesen», III., 1.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 6. Mai 2019.

DOMMER NICOLAS, Der Herausgabeanspruch gemäss Art. 75 E-FIDLEG, sui-generis 2018, S. 221 ff.

HÜNERWADEL PATRICK/TRANCHET MARCEL, Basler Kommentar zum Finanzmarktaufsichtsgesetz (FINMAG) und Finanzmarktinfrastrukturgesetz (FinfraG), 1. Kapitel: Allgemeine Bestimmungen, Art. 1 und 2 FINMAG, 3. Auflage, Basel 2019.

Materialien

Botschaft zum Finanzdienstleistungsgesetz (FIDLEG) und zum Finanzinstitutsgesetz (FINIG) vom 4. November 2015, BBl 2015 8901.

Eidgenössische Finanzmarktaufsicht FINMA

- Bericht über die Anhörung vom 7. Juli bis 1. September 2016 zum Entwurf des Rundschreibens 2017/6 «Direktübermittlung», 8. Dezember 2016.
- Erläuterungsbericht zum Rundschreiben 2017/xx «Direktübermittlung», 7. Juli 2016.
- Erläuterungsbericht zum Rundschreiben 2018/3 «Outsourcing – Banken und Versicherer», 6. Dezember 2016.
- Rundschreiben 2008/7 «Outsourcing Banken», Auslagerung von Geschäftsbereichen bei Banken, 20. November 2008.
- Rundschreiben 2008/21 «Operationelle Risiken – Banken», Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken, 20. November 2008.
- Rundschreiben 2013/3 «Prüfwesen», 6. Dezember 2012.
- Rundschreiben 2017/6 «Direktübermittlung», Direkte Übermittlung von nicht öffentlichen Informationen an ausländische Behörden und Stellen durch Beaufsichtigte, 8. Dezember 2016.
- Rundschreiben 2018/3 «Outsourcing – Banken und Versicherer», Auslagerungen bei Banken und Versicherungsunternehmen, 21. September 2017.

Schweizerische Bankiervereinigung (SBVg), Stellungnahme zum FINMA-Rundschreiben 2017/xx «Outsourcing – Banken und Versicherer», 31. Januar 2017.

Verband Schweizerischer Kantonalbanken (VSKB), Stellungnahme zum FINMA-Rundschreiben 2017/xx «Outsourcing – Banken und Versicherer», 31. Januar 2017.

DSGVO: Extraterritoriale Wirkung und konkrete Pflichten für die Banken

Monika Pfaffinger, Zürich*

* Prof. Dr. iur., Head Data Protection and Privacy Practice, Lexperience AG; Professorin, Kalaidos Law School; Habilitandin, Universität Basel; für die produktiven Diskussionen danke ich meinen Kolleginnen und Kollegen.

I. Vorbemerkungen

Der räumliche Anwendungsbereich der DSGVO und hierbei namentlich die extraterritoriale Wirkung zeigt sich in der Praxis selbst ein Jahr nach Ablauf der Umsetzungsfrist als Kernherausforderung gerade auch für schweizerische Unternehmen. Der europäische Datenschutzausschuss (European Data Protection Board, EDPB) hat Ende 2018 ein *Consultation Paper* zum räumlichen Anwendungsbereich der DSGVO publiziert. Ebenda wird eine vielsagende, Unheil ankündende Wendung eingesetzt: Gesprochen wird vom «Triggern» des Scopes der DSGVO.[1] Befasst man sich mit dem Anwendungsbereich der DSGVO, den von ihr statuierten tief- und weitreichenden Pflichten sowie ebensolchen behördlichen Massnahmen, triggert das vorab einmal Stress. Strukturieren lautet folglich die Devise, um Klarheit zu gewinnen, auch und gerade, wenn weiterhin einige Fragen im Bereich der datenschutzrechtlichen Neuerungen offen sind.

Dieser Beitrag will Orientierung geben und strukturiert sich wie folgt: Zunächst werden *Grundlagen und Leitplanken* umrissen, um damit ein Koordinatensystem zum Verständnis des Anwendungsbereiches wie auch der resultierenden Pflichten zur Verfügung zu stellen. Alsdann wird der *räumliche, insb. der extraterritoriale Anwendungsbereich der DSGVO* analysiert, wobei Beispiele der Veranschaulichung dienen. In Bezug auf die Anwendungstatbestände sowie Rechtsfolgen der DSGVO ist namentlich auch die Rollendifferenzierung zwischen Verantwortlichen resp. Auftragsverarbeitenden relevant, weshalb diese unter allen Titeln (II. 4, III. und IV.) thematisiert wird.[2] Die entsprechend *resultierenden Pflichten* werden aus sachlogischen Gründen punktuell im Rahmen der Scope-Analyse integriert, teilweise in einem letzten Titel eigenständig beleuchtet.

Bei vielen Schweizer Unternehmen nicht nur der Finanzbranche, lässt sich heute ein *beträchtlicher Auf- und Nachholbedarf mit Blick auf die Implementierung und Operationalisierung* des Datenschutzes feststellen.[3] An deren Anfang steht

---

1 Vgl. EDPB, Consultation Paper Scope, S. 6, S. 8 f., S. 13 ff., S. 17 f., S. 21.

2 Grundlegend auch zur Auftragsdatenverarbeitung der Beitrag von ROSENTHAL in diesem Band.

3 Vgl. PFAFFINGER/BALKANYI-NORDMANN, Schweizer Bank Mai 2018, S. 21; EBERT/WIDMER, S. 19.

vorab eine *Basisanalyse,* ob und inwiefern man in den *Anwendungsbereich der DSGVO* fällt.[4]

II. Grundlagen und Leitplanken

1. Elemente des Anwendungsbereiches der DSGVO

Das räumliche Element ist nur ein Element des Anwendungsbereichs der DSGVO. Insgesamt müssen *vier Elemente* erfüllt sein, um ihren Scope zu triggern.[5] *Erstens* der *zeitliche* Anwendungsbereich. Die Umsetzungsfrist endete am 25. Mai 2018. *Zweitens und drittens* der *sachliche* sowie *persönliche* Anwendungsbereich, vgl. Art. 1, Art. 2 und Art. 4 DSGVO:[6] Die DSGVO bezieht sich auf die Verarbeitung von Personendaten natürlicher Personen. Als personenbezogen gelten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[7] Geschützt sind natürliche Personen, die DSGVO findet keine Anwendung auf die Verarbeitung von Personendaten juristischer Personen. Der Verarbeitungsbegriff wird weit definiert und meint nahezu jeden, namentlich automatisierten, Umgang mit personenbezogenen Angaben: Erheben, organisieren, speichern, auswerten, weiterleiten usf.[8] In persönlicher Hinsicht kann es sich auf Seiten der Verarbeitenden um natürliche wie juristische Personen handeln, die alleine oder gemeinsam oder im Auftrag, Personendaten verarbeiten. Die Rollen der Verarbeitenden spielen eine Hauptrolle gemäss DSGVO und werden entsprechend zumindest in den Grundzügen umrissen. [9]

Ist der zeitliche, sachliche wie persönliche Anwendungsbereich der DSGVO gegeben, ist *viertens der räumliche Anwendungsbereich* zu prüfen. In der Beratungspraxis stösst man insofern auf Seiten der schweizerischen Unternehmen auf grosse Unsicherheiten.[10] Der räumliche Anwendungsbereich

---

4 Hierzu auch PFAFFINGER/BALKANYI-NORDMANN, Private Q1 2019, S. 22.

5 Insofern bereits PASSADELIS/ROTH, Jusletter 4. April 2016, Rz. 6 ff.

6 Zu Art. 4 DSGVO mit den Begriffsbestimmungen sei generisch auf die einschlägige Kommentarliteratur verwiesen.

7 Art. 4 Nr. 1 DSGVO.

8 Art. 4 Nr. 2 DSGVO; hierzu HERBST, Art. 4 Nr. 2, Beck-Komm. DSGVO, N 1 ff.

9 EDPB, Consultation Paper Scope, S. 3 ff.; vertiefend sodann CNIL, Guide sous-traitant, *passim*; WP 29, Concept of controller and processor, *passim*; BLD, FAQ Auftragsverarbeitung, S. 1–3; vgl. HARTUNG, Art. 4 Nr. 7 und Nr. 8 sowie Art. 28, Beck-Komm DSGVO; vertiefend hierzu auch ROSENTHAL in diesem Band.

10 Dokumentiert ist dieser Befund auch bei EBERT/WIDMER, S. 11 f. und S. 19.

wird in Art. 3 DSGVO geregelt, wobei *zwei Hauptkriterien* zu unterscheiden sind: *Erstens* das *Niederlassungskriterium nach Abs. 1* und *zweitens das sogenannte Targetingkriterium nach Abs. 2*, das seinerseits *zwei Unterfälle* umfasst, in *lit. a den Angebotstatbestand*, in *lit. b den Monitoringtatbestand*. Mangels Relevanz für das hier beschäftigende Thema wird auf die Erörterung von Art. 3 Abs. 3 DSGVO verzichtet.

Mit Blick auf den räumlichen Anwendungsbereich sind die erwähnten Guidelines des europäischen Datenschutzausschusses vom November 2018 aufschlussreich; zwar handelt es sich erst um ein Konsultationspapier, wobei ein solches Dokument die unzähligen Auslegungsfragen weder abschliessend beantworten kann, noch soll.[11] Vielmehr wird sich eine konstante Lehre und Praxis im Laufe der kommenden Jahre erst konsolidieren müssen. Gleichwohl gibt das Dokument *indikative Richtungshinweise*, womit sich mit diesem hinsichtlich Auslegung der DSGVO Tendenzen und Linien abzeichnen.

2. Richtungsimpulse mit Blick auf die Auslegung

Der europäische Datenschutzausschuss will mit dem Paper auf die Etablierung einer *konsistenten und gemeinsamen Interpretation* hinsichtlich des räumlichen Anwendungsbereiches der DSGVO hinwirken. Es geht mit anderen Worten um die *Harmonisierung*.[12] Zunächst lässt sich eine eher enge Anlehnung an den *Verordnungstext* erwarten.[13] Ebendies reflektierend findet auch in diesem Beitrag eine enge Orientierung am Verordnungstext statt. Zudem ist damit zu rechnen, dass die DSGVO *zwar autonom, nicht aber beziehungslos oder bezugsblind* mit Blick auf angrenzende Rechtsgebiete ausgelegt wird.[14] Weiter darf man aufgrund des Papers zum räumlichen Anwendungsbereich mit einer *weiten, nicht aber exzessiven* Interpretation rechnen.[15] Wie ein roter Faden zieht sich die Forderung durch das Dokument, im Rahmen der zu täti-

11 Auch schweizerische Expertinnen/Stellen haben auf offene Punkte im Dokument hingewiesen, so kontextspezifisch namentlich die EBF, Response guidelines scope GDPR, S. 1 ff.

12 Vgl. EDPB, Consultation Paper Scope, S. 3.

13 Beachte allerdings zum Angebotstatbestand den Hinweis auf die «manifested intention» EDPB, Consultation Paper Scope, S. 15.

14 Illustrativ EDPB, Consultation Paper Scope, S. 15.

15 Vgl. EDPB, Consultation Paper Scope, S. 5 f.

genden Assessments, *sämtliche konkreten Umstände des Einzelfalls zu evaluieren*.[16] Lediglich eine *Gesamtsicht*, die alle, *namentlich auch die faktischen Gegebenheiten* in die Analyse inkludiert, vermag Tatbestandselemente, wie diejenigen zum Anwendungsbereich, zu Rollen der Agierenden und daraus resultierende Pflichten, adäquat zu evaluieren. In diesem Punkt widerspiegelt sich ein Trend des zeitgenössischen Datenschutzrechts, eine bisher in erster Linie *formalistische Herangehensweise zu überwinden* und die *faktische Verwirklichung des Datenschutzrechts* zu stärken.

3. Koordinaten- und Navigationssysteme

Zwei Elemente sind für die Thematik dieses Beitrags von besonderer Relevanz.

Erstens die Differenzierung zwischen *direkter und indirekter Anwendbarkeit der DSGVO*.[17] Gemäss Art. 3 DSGVO kann diese direkt anwendbar sein ebenso für Non-EU-Gesellschaften, also auch für Schweizer Banken, sei es in der Rolle des Verantwortlichen (Controller) oder derjenigen des Auftragsverarbeiters (Processor). Mangels direkter Anwendbarkeit basierend auf Art. 3 DSGVO ist sodann die indirekte Anwendbarkeit aufgrund eines Vertrages denkbar, vgl. Art. 28 Abs. 3 DSGVO.

Um prüfen zu können, ob man in den Scope der DSGVO fällt, aber auch zur anschliessenden Erfüllung der konkreten Pflichten, muss man vorab seine *Verarbeitungslandschaft, die Prozesse der Personendatenverarbeitung kennen.* Insofern liesse sich ein Prüfungsschema in Anlehnung an die für das Obligationenrecht geprägte Lehrformel formulieren, die lautet: Wer verarbeitet welche Personendaten wie und wozu (sowie wie lange)? Zur Beantwortung dieser Fragen dient auch das neue Instrument des *Verarbeitungsverzeichnisses*.[18] Die besagte Inventarisierung der Personendatenverarbeitungen ist nicht nur eine eigenständige Pflicht der DSGVO, vgl. Art. 30 DSGVO und des geplanten Entwurfs zur Totalrevision des DSG, vgl. Art. 11 E-DSG.[19] Das Verarbeitungsver-

---

16 EDPB, Consultation Paper Scope, S. 3, S. 5 f., S. 8, S. 12, S. 16; ein entsprechender Hinweis findet sich auch in der einschlägigen Kommentarliteratur.

17 Vgl. EDPB, Consultation Paper Scope, S. 10.

18 Insofern auch PASSADELIS/ROTH, Jusletter 4. April 2016, Rz. 78.

19 Zur Totalrevision des DSG vgl. insb. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017-1084, S. 6941–7192.

zeichnis ist zugleich *Herz wie Gehirn der Datenschutz-Compliance in toto* und Basisinstrument, um die zahlreichen datenschutzrechtlichen Vorgaben erfüllen zu können. Es dient vorgeschaltet dem Scope-Assessment.[20]

Zweitens bezieht sich eine damit zusammenhängende Basisanalyse auf die *Rollen der Akteure im Rahmen der Personendatenverarbeitungsprozesse.*[21] Entscheidend ist die Frage, inwiefern man als alleiniger Controller, als Co-Controller oder Processor verarbeitet. Je nachdem, in welcher Rolle der Verarbeitende tätig ist und aufgrund welchen Tatbestandes die DSGVO anwendbar ist, variieren denn auch die Rechtsfolgen: Es sind Differenzierungen mit Blick auf die resultierenden Pflichten zu beachten. Folglich empfiehlt es sich nicht selten, die Data Governance mit ihren zahlreichen Aufgaben und Workstreams entlang dieser Rollendefinierung zu entwickeln.

Grundlegend ist folglich auch für Schweizer Banken die sorgfältige Basisanalyse, ob, inwiefern und in welcher Rolle man in den Anwendungsbereich der DSGVO fällt, wobei hierzu die Erstellung eines Inventars unverzichtbar ist.

Mit diesen Basisanalysen und deren Dokumentation trägt man zugleich dem sog. *Grundsatz der Accountability Rechnung*:[22] Die DSGVO verankert umfassende Dokumentations- und Rechenschaftspflichten hinsichtlich der Einhaltung ihrer Vorgaben, vgl. insb. Art. 5 Abs. 2 und Art. 24 DSGVO.[23]

In diesem Zusammenhang ist zugleich auf ihren *risikobasierten Ansatz* hinzuweisen, der sich in zahlreichen Normen und Instrumenten niederschlägt, so z.B. Art. 24 Abs. 1 DSGVO und Erwägungsgrund 77, Art. 33 f., Art. 35 DSGVO. Der Accountability-Ansatz und das Inventar leisten ihrerseits einen Beitrag dazu, den Risiko-Ansatz umzusetzen, ermöglichen sie doch, Risiken angemessen zu evaluieren, risikobasiert Massnahmen zu priorisieren, implementieren, dokumentieren und kontrollieren.

Die erwähnten Ansätze und Umsetzungsinstrumente sind gerade in einem jungen Rechtsgebiet, in dem viele Fragen offen sind, wichtig und hilfreich. Die entsprechenden Vorgaben lassen sich damit keineswegs bloss als Traktieren von Seiten des Gesetzgebers wahrnehmen. Vielmehr sollten sie als Massnahmen verstanden werden, die gleichzeitig einen Beitrag zur Effektuierung des Datenschutzrechts wie auch zum leichteren Navigieren in einer

---

20 Zur Notwendigkeit dieser Analyse EDPB, Consultation Paper Scope, S. 4.

21 EDPB, Consultation Paper Scope, S. 4 f., S. 9 ff.

22 EDÖB, EU-DSGVO und die Schweiz, S. 8.

23 Vertiefend RASCHAUER, Art. 24, NomosKomm. DSGVO, N 1 ff.

teilweise nebulösen Landschaft leisten. Der Nachweis, dass man sich mit einer datenschutzrechtlichen Herausforderung befasst hat – beispielsweise die Prüfung, ob man in den Anwendungsbereich der DSGVO fällt – und ein Argumentarium, warum man welche Massnahmen (nicht) ergriffen hat, versetzt einen nicht nur gegenüber den Behörden, sondern auch den Datensubjekten in eine ungleich bessere Position, als wenn man sich Untätigkeit, Ignoranz oder Optimieren zu Lasten des Datenschutzrechts vorwerfen lassen muss.

4. Die Einschlägigkeit der Rollen

Wie erwähnt sind hinsichtlich des Anwendungsbereichs der DSGVO wie auch der resultierenden Pflichten die *Rollen* der Verarbeitenden einschlägig. Art. 4 Nr. 7 resp. Nr. 8, Art. 26 und Art. 28 DSGVO äussern sich punktuell zu den Rollen Controller (alleiniger Verantwortlicher), Co-Controller (gemeinsame Verantwortliche) oder Auftragsverarbeiter (Processor).[24] Mit Blick auf die Rollendefinition und -fixierung ist wiederum von einem *funktionellen Ansatz* auszugehen: Die Rollendefinierung erfolgt aufgrund der *realen Verhältnisse* und unter *Berücksichtigung sämtlicher konkreter Umstände*.[25]

(Alleiniger) Verantwortlicher resp. Controller ist, wer über Zweck und Mittel der Personendatenverarbeitung entscheidet, also wesentliche Entscheidungsbefugnisse hat, warum, wofür und wieweit verarbeitet wird. Relevant ist zudem ein Weisungs- und Aufsichtsrecht, aber auch das Auftreten nach aussen. Der Controller resp. Verantwortliche ist Adressat der umfassenden Pflichten gemäss DSGVO.

Sind *mehrere Parteien* in Personendatenverarbeitungen involviert, kann es sich um eine *gemeinsame Verantwortlichkeit* oder aber um *ein Auftragsverhältnis* handeln.

Gemäss Art. 4 Nr. 7 und Art. 26 DSGVO sind *gemeinsame Verantwortliche (Co-Controller)* möglich. In der Praxis sind Co-Controller-Konstellationen gerade in Konzernen und Unternehmensverbünden häufig. Man sieht hier oft hochkomplexe Ketten und Netzwerke zwischen diversen Akteuren. Das Ausloten der Relevanzschwelle der Mitentscheidung über die Zielrichtung und Modalitäten der Verarbeitungen kann schwierig sein. Co-Controller haben in

---

[24] Vgl. WP 29, Concept of controller and processor, *passim;* die nachfolgenden Ausführungen basieren zudem auf der einschlägigen Kommentarliteratur, z.B. INGOLD, Art. 26 und Art. 28, NomosKomm. DSGVO, auf die an dieser Stelle generisch verwiesen wird.

[25] Zum Ganzen WP 29, Concept of controller, S. 1, S. 9 f., S. 11, S. 16, S. 18, S. 27 und S. 32; HARTUNG, Art. 4, Beck-Komm. DSGVO, N 6 ff. und Art. 28, Beck-Komm. DSGVO, N 26 ff.

transparenter Weise festzulegen, wer welche Verantwortlichkeiten betreffend die Erfüllung der datenschutzrechtlichen Vorgaben wahrnimmt. Entsprechende Agreements müssen ihrerseits die realen Beziehungen und Rollen gegenüber den Datensubjekten adressieren. Im Lichte der DSGVO empfiehlt sich nicht selten eine Re-Evaluation der Rollen und Agreements. Dass diese Vereinbarungen die tatsächlichen Funktionen und Beziehungen widerspiegeln, ist gerade auch deshalb relevant, weil das «kumulative Zusammenwirken» äusserst heterogene Szenarien umfasst.[26]

Sind mehrere Parteien an Personendatenverarbeitungen beteiligt, kann es sich indes auch um ein *Auftragsverhältnis* handeln.[27] Auftragsverarbeiter resp. Processors sind natürliche oder juristische Personen oder Stellen, die Personendaten im Auftrag («on behalf») des Verantwortlichen verarbeiten. Den Auftragsverarbeiter treffen nach DSGVO bei direkter Anwendbarkeit deutlich mehr direkte Pflichten im Vergleich zur EU-Datenschutzrichtlinie und dem aktuellen DSG. Er kann bei Verletzungen ihrer Pflichten direkt sanktioniert werden. *Drei spezifische Hinweise* mit Blick auf die Auftragsdatenverarbeitung: *Erstens* muss ein schriftlicher Vertrag zwischen Verantwortlichem und Auftragsverarbeiter in transparenter Weise die Verantwortlichkeiten genauer festzulegen.[28] *Zweitens* sind die spezifischen Pflichten des Auftragsverarbeiters, insbesondere diejenigen *vis-à-vis* dem Verantwortlichen, z.B. die Unterstützung im Rahmen der Betroffenenrechte, zu fixieren. Und *drittens* ist auf die direkten Pflichten der DSGVO hinzuweisen, die sowohl von den Verantwortlichen wie den Auftragsverarbeitern zu erfüllen sind, sofern sie vom Anwendungsbereich der DSGVO erfasst werden. Exemplarisch insofern ist die Pflicht, technischen und organisatorischen Massnahmen zu ergreifen, Art. 32 DSGVO.

Im Rahmen der Auftragsverarbeitung ist darüber hinaus zudem an die *indirekte Anwendbarkeit* gemäss Art. 28 Abs. 3 DSGVO zu erinnern. Hier geht es in erster Linie um die Konstellation, in der ein EU-Verantwortlicher einen Non-EU-Auftragsverarbeiter und nicht direkt unter die DSGVO fallenden

---

26 BLD, FAQ Auftragsverarbeitung, S. 1 ff.; CNIL, Guide sous-traitant, *passim*.

27 Insofern auch PASSADELIS/ROTH, Jusletter 4. April 2016, Rz. 46 ff.

28 Der Auftragsverarbeitungsvertrag bedarf der Schriftform, die elektronische Form genügt. Was Inhalt, Gegenstand und Detailgrad ebendieses Vertrages anbelangt, gilt auch insofern der risikobasierte Ansatz der DSGVO. Die Überprüfung der Verträge auf ihre DSGVO-Konformität kann in der Praxis aufwendig sein. Daher empfiehlt sich aus Effizienzgründen nicht selten, bestehende Verträge durch DSGVO-konforme Klauseln/ Verträge zu ersetzen.

Auftragsverarbeiter beizieht. Damit ist das Feld abgesteckt, um die räumliche und extraterritoriale Wirkung der DSGVO *en détail* darzustellen.

III. Die extraterritoriale Wirkung der DSGVO

1. Vorbemerkungen

Vorausgeschickt sei, dass mit Blick auf *Kundendaten* im Banken- und Finanzsektor sowie Versicherungsbereich der DSGVO aufgrund der sektoriellen Regulierung (z.B. Stichwort: Crossboarder) eine andere Bedeutung zukommt, als in Branchen ohne entsprechende Regulierungsdichte.[29]

Mit Blick auf den räumlichen Anwendungsbereich der DSGVO verleiht eine *Stufenprüfung* Orientierung, wobei man Art. 3 DSGVO konsequent mit seinen Tatbestandselementen durchprüft. Wird der Anwendungsbereich nicht aufgrund von Art. 3 Abs. 1 DSGVO getriggert, kann die DSGVO gleichwohl aufgrund von Art. 3 Abs. 2 lit. a resp. lit. b DSGVO einschlägig sein. Stets sind die einzelnen Tatbestandselemente zu prüfen, womit die Thematik des Datenschutzrechts – obschon weit davon entfernt, in das Palmares juristischer Grundausbildung aufgenommen zu werden – perfekt geeignet wäre, die juristische Arbeitsweise und Methode im Rahmen einer Erstsemestervorlesung zu illustrieren.

2. Niederlassungskriterium gemäss Art. 3 Abs. 1 DSGVO

a) Tatbestandselemente

Am Anfang figuriert das Niederlassungskriterium als Anknüpfungselement des räumlichen Anwendungsbereichs der DSGVO, in der deutschen Fassung mit den Worten: «Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der

[29] Ein Themenfeld, das für den Finanzsektor spezifische Herausforderungen bringt, liegt in der Nutzung von Cloud-Diensten. Die sich hier stellenden Fragen gehen weit über den Anwendungsbereich der DSGVO hinaus; vgl. hierzu jüngst SBVg/EBF, Cloud-Leitfaden, S. 1 ff.

Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet».[30] Zu den Tatbestandselementen der Bestimmung im Einzelnen:

Das *erste Tatbestandselement* ist die *Niederlassung* in der EU. Wiederum greift auch an dieser Stelle *kein formeller Ansatz*, nicht entscheidend ist die Registrierung.[31] Massgeblich sind vielmehr die realen und effektiven Aktivitäten durch eine Einrichtung mit einer gewissen Beständigkeit in der EU («arrangement»).[32] Die Anforderungen insofern gelten als niedrig. Unter Umständen genüge die Anwesenheit eines einzigen Mitarbeiters oder einer Agentur. Es muss sich gerade nicht um eine Tochtergesellschaft oder Zweigniederlassung handeln.[33]

Zweitens muss die *Personendatenverarbeitung im Zusammenhang mit den Aktivitäten der Niederlassung* stattfinden.[34] Damit diese Voraussetzung erfüllt ist, haben die Verarbeitungshandlungen in einem *untrennbaren Konnex* zu den effektiven und tatsächlichen geschäftlichen Aktivitäten der Niederlassung in der EU zu stehen. Das Paper spricht insofern vom «inextricable link», wobei das Konzept unbestritten Interpretationsräume offenlässt. Ob dieser Link zwischen geschäftlicher Aktivität und Personendatenverarbeitung besteht, sei weder zu restriktiv noch zu exzessiv anzunehmen. Geboten ist erneut eine *in concreto-Analyse*, die sämtliche einschlägigen Elemente in die Erwägungen integriert.[35] Die Personendatenverarbeitung muss nicht von der Niederlassung selbst durchgeführt werden.

Damit ist man beim *dritten Tatbestandselement* und der *Rechtsfolge:* Ungeachtet dessen, ob die vorangehend beschriebene Personendatenverarbeitung in der EU oder ausserhalb der EU durchgeführt wird, ist die DSGVO auf die beleuchteten Personendatenverarbeitungsprozesse anwendbar.

---

30 In der englischen Fassung Article 3, Territorial scope, 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. […].

31 EDPB, Consultation Paper Scope, S. 5.

32 ENNÖCKL, Art. 3, NomosKomm. DSGVO, N 6 f.; hierzu auch KLAR, Art. 3, Beck-Komm. DSGVO, N 40 ff.; EDPB, Consultation Paper Scope, S. 5.

33 EDPB, Consultation Paper Scope, S. 5.

34 Zum Kriterium vgl. KLAR, Art. 3, Beck-Komm. DSGVO, N 54 ff.; EDPB, Consultation Paper Scope, S. 6 ff.; vertiefend aufgeführt werden im Consultation Paper Personendatenverarbeitungen, die im Zusammenhang mit einem *revenue raising* stehen, vgl. EDPB, Consultation Paper Scope, S. 7 f.; mit Blick auf das Kriterium des inextricable link wird namentlich auch auf den Google-Spain-Entscheid hingewiesen, vgl. Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12).

35 EDPB, Consultation Paper Scope, S. 6.

b) Beispiele

Einige Beispiele und Konstellationen zur Veranschaulichung des Tatbestandes:

Erstes Beispiel: Eine Front Einheit eines Schweizer Finanzdienstleisters mit Hauptsitz in Zürich bearbeitet für Managementzwecke auch Personendaten von Mitarbeitenden der Filialen/Tochtergesellschaft in Deutschland.–

In dieser Konstellation ist der Controller in der Schweiz, eine Niederlassung in der EU ist gegeben, wobei die Personendatenverarbeitungen im Zusammenhang mit den Geschäftsaktivitäten der Niederlassung stehen. Ungeachtet dessen, wo die Personendatenverarbeitungen stattfinden, hier in der Schweiz, ist die DSGVO direkt anwendbar auf die entsprechenden Personendatenverarbeitungen durch den Schweizer Finanzdienstleister.

Zweites Beispiel: Ein französischer Finanzdienstleister mit Hauptsitz in Paris und Niederlassung/Geschäftsstelle in der Schweiz beauftragt seine Schweizer Geschäftsstelle, spezifische Marketingaktivitäten durchzuführen.–

Es handelt sich hierbei gewissermassen um die umgekehrte Konstellation im Vergleich zum vorangehenden Beispiel. Für den Fall, dass der französische Finanzdienstleister darüber bestimmt, wie die Marketingprozesse durchgeführt werden sollen, dann ist der Verantwortliche/Controller in Frankreich und der Auftragsverarbeiter/Processor in der Schweiz. Gegeben ist eine Niederlassung in der EU, die Personendatenverarbeitung findet im Zusammenhang mit Aktivitäten der EU-Niederlassung statt. Folglich ist von der direkten Anwendbarkeit der DSGVO auf diese im Non-EU-Land durchgeführten Personendatenverarbeitungen aufgrund von Art. 3 Abs. 1 DSGVO auszugehen. Die französische Gesellschaft hat die Controller-Pflichten, die Schweizer Gesellschaft die Processor-Pflichten, und zwar die gesetzlichen Mindestpflichten sowie die vertraglich näher definierten Pflichten, einzuhalten.[36]

Drittes Beispiel: Ein Deutscher Finanzdienstleister mit Hauptsitz in München beauftragt ein Drittunternehmen in der Schweiz mit dem Marketing.–

Das deutsche Unternehmen ist, sofern es wesentliche Entscheidungsbefugnisse darüber hat, warum, wie und wieweit Personenangaben verarbeitet werden, Verantwortlicher/Controller, hier in der Rolle der «Client Company». Das deutsche Unternehmen steht selbst unter DSGVO. Die Schweizer Marketing-Gesellschaft ist Processor/Auftragsverarbeiter, ein sog. «Service

[36] Die beiden Parteien haben entsprechend in einem schriftlichen Vertrag ihr Verhältnis konkret und risikobasiert zu definieren. Gleichwohl ist die DSGVO in diesem Szenario direkt anwendbar und es greifen quasi von Gesetzes wegen direkt gewisse Mindestpflichten für den Auftragsverarbeiter.

Provider». Letztere hat keine Niederlassung in der EU, womit es zu keiner direkten Anwendbarkeit der DSGVO gestützt auf Art. 3 Abs. 1 DSGVO auf die besagten Verarbeitungshandlungen durch den Schweizer Auftragsverarbeiter kommt. Der EU-Controller/Verantwortliche hat allerdings den Non-EU-Processor/Auftragsverarbeiter über einen Vertrag gemäss Art. 28 Abs. 3 DSGVO einzubinden. Die Bestimmung gilt namentlich für ebendieses Szenario als relevant, in welchem ein EU-Verantwortlicher einen Non-EU-Auftragsverarbeiter einsetzt. Eine Vereinbarung nach Art. 28 Abs. 3 DSGVO führt nur zur vertraglichen Bindung an bestimmte Pflichten der DSGVO, nicht zur direkten Anwendung der DSGVO selbst.

*Viertes Beispie*l: Ein Schweizer Finanzdienstleister ohne Niederlassung im EU-Raum beauftragt ein Drittunternehmen in Deutschland, das Background Screening für angehende Mitarbeitende und/oder Payroll Services für Mitarbeitende durchzuführen.–

Der Einsatz eines Auftragsverarbeiters als Service Provider triggert den Anwendungsbereich gemäss Art. 3 Abs. 1 DSGVO *nicht*, mit anderen Worten wird damit keine Niederlassung begründet.[37] Folglich kommt es zu keiner direkten Anwendbarkeit der DSGVO auf den Schweizer Finanzdienstleister aufgrund von Art. 3 Abs. 1 DSGVO. In der Praxis bestehen EU-Auftragsverarbeiter oft darauf, mit dem Verantwortlichen, der nicht direkt in den Scope der DSGVO fällt, einen Vertrag nach Art. 28 Abs. 3 DSGVO zu schliessen. Die Vorgaben dieser Bestimmung treffen indes in erster Linie die umgekehrte Situation, die gerade vorher beschrieben wurde. Die Rechtslage insofern gilt als wenig(er) klar.[38]

3. Targetingkriterium gemäss Art. 3 Abs. 2 DSGVO

Wird die Anwendbarkeit der DSGVO aufgrund von Art. 3 Abs. 1 DSGVO verworfen, kann diese gleichwohl einschlägig sein.[39] Zu prüfen ist, ob sich ihre extraterritoriale Wirkung aufgrund des Targetingkriteriums gemäss Art. 3 Abs. 2 DSGVO entfaltet. Das sog. Targetingkriterium hat seinerseits zwei

---

37 EDPB, Consultation Paper Scope, S. 10 f.; hierzu VASELLA, digma 2017, S. 221.

38 EDPB, Consultation Paper Scope, S. 10; als «strange» wird eine (rechtliche) Situation beschrieben, gemäss welcher ein Services Provider eine Client Company vertraglich in die Pflicht nehmen soll, wobei entsprechend auch auf den Klärungsbedarf hingewiesen wird, vgl. EBF, Response guidelines scope GDPR, S. 3.

39 Hierzu sowie zur Beschreibung des Abs. 2 mit dem Überbegriff des Targeting Criterion, vgl. EDPB, Consultation Paper Scope, S. 12.

Untertatbestände, den Angebotstatbestand nach lit. a und den Monitoringtatbestand nach lit. b.

a) Angebotstatbestand, Art. 3 Abs. 2 lit. a DSGVO

aa) Tatbestandselemente

Der Angebotstatbestand lautet wie folgt: «Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist». [40]

Tatbestandselemente des Angebotstatbestandes gemäss Art. 3 Abs. 2 lit. a DSGVO, der auch mit dem Begriff *Marktortprinzip* eingefangen wird, ist *erstens*, dass der Verantwortliche (resp. Auftragsverarbeiter) *keine Niederlassung in der EU* i.S.v. Art. 3 Abs. 1 DSGVO aufweist.

Zweitens erfolgt eine *Verarbeitung von Personendaten im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen an Personen in der EU*, wobei es irrelevant ist, ob eine Gegenleistung erfolgt. Ebenso wenig einschlägig ist weiter die Staatsangehörigkeit der Personen, an die sich das Angebot richtet. Vielmehr muss sich das Angebot an Personen in der EU richten, das betroffene Datensubjekt befindet sich in der EU. Gemäss europäischem Datenschutzausschuss ist die *manifestierte Absicht*, Waren oder Dienstleistungen an Personen in der EU anzubieten, hinreichendes Kriterium («manifested intention to offer goods or services»). Auch hier sind sämtliche Umstände des Einzelfalles und damit das Gesamtbild relevant.[41] Der Tatbestand bedarf folglich einer Analyse der effektiven Organisation, Produkte sowie der Produkt- und Vertriebs-

---

[40] In der englischen Fassung Article 3, Territorial scope, 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union. […].

[41] Zum Kriterium des offensichtlichen Beabsichtigens und der Notwendigkeit einer Gesamtschau KLAR, Art. 3, Beck-Komm. DSGVO, N. 80 ff.; EDPB, Consultation Paper Scope, S. 14 f. m.w.H.; ENNÖCKL, Art. 3, NomosKomm. DSGVO, N 13 f.

struktur. Im Paper werden Indizien für diese klare Angebots-Absicht aufgeführt, so die Sprache der Internetseite, Angaben von Lieferkosten für Versand in EU, ein Lieferangebot in EU-Länder usf.[42]

Für Banken wird unter der Bestimmung auch das Thema der *reverse solicitation* relevant. Geht es um eine reverse solicitation, die ihren Namen zu Recht trägt, weil die Initiative zur Geschäftsanbahnung und -beziehung tatsächlich von der Klientin ausgeht, ist alsdann wohl auch davon auszugehen, dass damit die Anforderungen an das datenschutzrechtliche Targetingkriterium nicht erfüllt werden. Über den Finanzsektor hinausgehend wirft der Tatbestand Fragen mit Blick auf *Dauerschuldverhältnisse* auf.

bb) Beispiele

Zur Illustration auch dieses Tatbestandes zwei Beispiele:

Erstes Beispiel: Ein Schweizer Asset Manager mit Freistellung von der Erlaubnispflicht durch die BaFin, vertreibt in Deutschland grenzüberschreitend Fonds an private Investoren.–

Es handelt sich um einen Controller ohne Niederlassung in der EU, der ein Angebot an natürliche Personen in der EU richtet, wobei eine Personendatenverarbeitung im Zusammenhang mit diesem Angebot vorgenommen wird.

Zweites Beispiel: Eine Kantonalbank in der Schweiz ohne Niederlassung im EU-Raum, hat als Kunden in der Schweiz niedergelassene Personen, unter anderem auch deutsche Staatsangehörige. Die Bank ist nur in der Schweiz aktiv, sie richtet keinerlei Aktivitäten in den EU-Markt. Ein deutscher Staatsangehöriger eröffnet ein Sparkonto in der Filiale im Kanton Aargau.–

Es handelt sich hierbei um ein Gegenbeispiel, sind doch zwei Elemente des Angebotstatbestandes nicht erfüllt: Das Tatbestandselement der Person in der EU fehlt, es erfolgt kein Anbieten von Waren oder Dienstleistungen an eine Person in der EU, die Staatsbürgerschaft an sich ist nicht einschlägig. Die vorgenommenen Verarbeitungen werden nicht vom Anwendungsbereich der DSGVO erfasst.

b) Monitoringtatbestand, Art. 3 Abs. 2 lit. b DSGVO

aa) Tatbestandselemente

Das dritte Kriterium, gemäss dessen der DSGVO-Scope getriggert wird, ist in Art. 3 Abs. 2 lit. b DSGVO niedergelegt und lautet: «Diese Verordnung findet

[42] EDPB, Consultation Paper Scope, S. 15 f.

Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht, das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt».[43]

Der Verantwortliche resp. Auftragsverarbeiter hat wiederum, erstens, keine Niederlassung in der EU, beobachtet indes, zweitens, das Verhalten einer Person in der EU, wobei eine Personendatenverarbeitung im Zusammenhang mit dieser Verhaltensbeobachtung steht.[44] Präzisierend wird im Konsultationspapier des EU-Datenschutzausschusses darauf hingewiesen, dass es gewisser Auswertungsaktivitäten bedarf, um den Tatbestand zu erfüllen.[45]

bb) Beispiel und Ausblick

Eine Schweizer Bank betreibt eine Website, wobei sich die Angebote nicht an Personen im EU-Raum richten. Allerdings werden sämtliche Besucher der Website getrackt.–

Wenn nun diese Angaben auch ausgewertet werden, dann ist man im Scope der DSGVO. Im Zusammenhang mit diesem Beispiel ist *en passant* auf die E-Privacy-Verordnung, auch Cookies-Verordnung genannt, hinzuweisen. Sie steht noch nicht in Kraft, wird allerdings als lex specialis zur DSGVO zu beachten sein.[46]

IV. Resultierende Pflichten

1. Einbettung

Nachdem der räumliche Anwendungsbereich der DSGVO mit ihrer extraterritorialen Wirkung umrissen wurde, ist nunmehr auf die resultierenden Pflichten einzugehen. Einige Pflichten wurden bereits im Rahmen der Darstellung des Scopes der DSGVO vorgestellt, so die Pflicht zur Erstellung eines

---

43 In der englischen Fassung Article 3, Territorial scope, 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: […] (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

44 Zum Tatbestand EDPB, Consultation Paper Scope, S. 17 f.

45 Hierin lässt sich eine «Verengung» des Anwendungsbereiches der DSGVO sehen, vgl. EDPB, Consultation Paper Scope, S. 18.

46 <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32009L0136>.

Inventars, die Pflicht zur Basisanalyse betreffend Anwendungsbereich und Rollen, die allgemeinen Dokumentations- wie Rechenschaftspflichten mit Blick auf die Einhaltung der datenschutzrechtlichen Vorgaben. Zudem wurde gezeigt, dass eine Differenzierung auch mit Blick auf die Pflichten entsprechend der Rollen der Verarbeitenden stattfindet. Als Strukturmerkmal der DSGVO wurde sodann der risikobasierte Ansatz der DSGVO beschrieben, der sich gerade auch auf die Priorisierung sowie Konkretisierung der zu ergreifenden Massnahmen zwecks Implementierung der Datenschutz-Compliance bezieht.[47]

2. Spezifische Herausforderung: Die Pflicht nach Art. 27 DSGVO

Eine Pflicht stellt Schweizer Finanzinstitute vor besondere Herausforderungen, weshalb diese vorangestellt thematisiert wird. Fällt ein Unternehmen nach Art. 3 Abs. 2 DSGVO unter den Erlass, ist es prinzipiell verpflichtet, in der EU einen sog. *Datenschutzvertreter* zu bezeichnen, Art. 27 DSGVO. Unter bestimmten Voraussetzungen kann ausnahmsweise auf die Bestellung verzichtet werden.[48] Auch zum EU-Vertreter finden sich Hinweise im Consultation Paper, wobei es namentlich für eine Unvereinbarkeit mit der Position eines externen DPO argumentiert.[49] Zudem wird empfohlen, den Vertreter dort zu stationieren, wo intensive Aktivitäten stattfinden.[50]

Eine Kernherausforderung besagter Pflicht allerdings liegt in einer *potenziellen Kollision zwischen den Rechtsordnungen*.[51] Anders gewendet: Man sieht sich unter Umständen mit einem Konflikt zwischen europäischem und eidgenössischem Recht konfrontiert, wobei im vorliegenden Kontext im Rahmen der Schweizer Rechtsordnung insb. Art. 271 StGB sowie Art. 47 BankG zu nennen sind. Die Situation kann als *dilemmatisch* charakterisiert werden:

Die Verletzung von Art. 27 DSGVO kann mit Geldbußen von bis zu 10 Mio. EUR oder im Fall eines Unternehmens mit bis zu 2% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden, vgl. Art. 83 Abs. 4 lit. a DSGVO. Zwar sind mit Blick auf die Vollstreckung und Vollstreckbarkeit von Massnahmen gestützt auf die

---

47 Hierzu PFAFFINGER/BALKANYI-NORDMANN, Schweizer Bank Mai 2018, S. 21.

48 Hierzu HARTUNG, Art. 27, Beck-Komm. DSGVO, N 6 ff.; zu den Ausnahmen auch EDPB, Consultation Paper Scope, S. 21 f.

49 Vgl. EDPB, Consultation Paper Scope, S. 20 f.

50 EDPB, Consultation Paper Scope, S. 22.

51 Für die wertvollen Hinweise im Rahmen dieser Analyse danke ich ANNA K. MÜLLER FÜRST sowie DENISE JUD, Lexperience AG, für die wertvollen Hinweise.

DSGVO im Zuge ihrer extraterritorialen Wirkung entsprechend auch gegenüber schweizerischen Stellen und Unternehmen viele Fragen offen, wobei man derzeit von der fehlenden Vollstreckbarkeit von Massnahmen gegenüber Schweizer Unternehmen ausgeht. In diesem Zusammenhang ist auch auf die Stellungnahme des Bundesrates zur Interpellation Fiala (17.4088) betr. Umsetzungsfragen zur EU-Datenschutz-Grundverordnung vom 2. März 2018 hinzuweisen. Demnach seien die Aufsichtsbehörden der EU-Mitgliedstaaten zwar durchaus zuständig für die Untersuchung und Verhängung von Sanktionen nach DSGVO gegen Unternehmen in der Schweiz.[52] Ohne Kooperationsabkommen allerdings dürften diese in der Schweiz keine Untersuchungs- und Vollstreckungshandlungen vornehmen. Ein Kooperationsabkommen zwischen der Schweiz und der EU soll zwar erarbeitet werden, der Bundesrat gedenkt allerdings damit zuzuwarten, bis die parlamentarischen Arbeiten zur Revision des DSG erfolgt sind. Und dies kann unter Umständen dauern...[53] Die Rechtslage ist folglich mit Unsicherheiten behaftet, wobei die politischen Versäumnisse schweizerische Unternehmen und gerade auch Banken hierzulande in eine anspruchsvolle Risikolandschaft versetzen:

Auf der einen Seite bringt die *Nichtbestellung* das Bussen- resp. Sanktions- und Massnahmenrisiko gemäss DSGVO. Zu den europäischen Folgen eines Verzichts auf die Bezeichnung eines Vertreters hinzu kommt unter Umständen ein aufsichtsrechtliches Risiko in der Schweiz wegen Nichtbeachtung ausländischen Rechts sowie ein Reputationsrisiko in Bezug auf die Verletzung der DSGVO. Hieran anknüpfend ist dieser Tage der Vertrauensverlust von Seiten der (potenziellen) Klientel mit resultierenden wirtschaftlichen Folgen in die Erwägungen zu integrieren.[54]

---

52 Siehe <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174088>.

53 Derzeit rechnet man nicht mit einem Inkrafttreten des totalrevidierten DSG vor 2021/2022; vgl. <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170059>. Es bleibt zu hoffen, dass dem DSG die Wiederholung eines langwierigen Prozesses diesmal erspart bleibt – im Rahmen der Verabschiedung des ersten DSG erstreckte sich der Prozess über rund zwei Dezennien.

54 Insofern unlängst PFAFFINGER/BALKANYI-NORDMANN, Schweizer Bank Mai 2018, S. 21; VESTING verortete scharf noch im Jahr 2003 im *medialen Rauschen* die Hauptwirkung des damaligen Datenschutzrechts, S. 182; richtungsweisend mit Blick auf die Diskrepanz zwischen Anspruch und Wirklichkeit im Datenschutzrecht und ein sog. Vollzugsdefizit BUCHNER, Selbstbestimmung, S. 1; für die Schweiz unlängst EBERT/WIDMER, S. 19; zur Korrelation zwischen Datenschutzvorfällen, Vertrauen und wirtschaftlichem Impact: Ponemon Institute LLC/Centrify, Impact on Reputation, insb. S. 2 ff.

Umgekehrt kann die Bestellung eines EU-Vertreters zur Folge haben, dass ausländische/europäische Behörden im Falle einer Anfrage oder Untersuchung den Datenschutzvertreter nicht mehr formell via Amtshilfe über die Schweizer Behörde anzugehen haben, stattdessen der Vertreter in der EU zumindest Zustellungsempfänger für allfällige Verfügungen ist. Im Ergebnis kann dies dazu führen, dass ein Schweizer Unternehmen ohne den Schutz der Amtshilfenormen plötzlich Partei eines ausländischen Aufsichtsverfahrens wird – mit den entsprechenden, unter Umständen einschneidenden Konsequenzen.[55] Hinzu kommt, dass es dem Schweizer Unternehmen unter der Strafandrohung gemäss Art. 271 StGB und allenfalls auch Art. 47 BankG nicht gestattet ist, mit der ausländischen Behörde zu kooperieren, geht es darum, Informationen oder Dokumente aus der Schweiz an die ausländische Behörde zu liefern.

Verschiedene Lösungsansätze lassen sich für diese Herausforderungen skizzieren. Zunächst ist zu prüfen, ob man der Problematik aufgrund des Ausnahmetatbestandes entgehen kann. Lässt sich kein Ausnahmetatbestand geltend machen, ist der Verzicht auf die Bestellung eines EU-Vertreters ein zu riskanter Weg.

Eine gangbare Strategie wird darin verortet, einen EU-Vertreter in Form einer reinen Postbox zu bestellen. Vertraglich wäre dieser u.a. zu verpflichten, sich umgehend mit dem Verantwortlichen in Verbindung zu setzen, sobald eine Anfrage von Seiten der EU-Behörden eingegangen ist. Alsdann wäre das Prozedere von Seiten des Verantwortlichen in der Schweiz auch mit den hiesigen Behörden zu klären und ggf. eine Bewilligung des Bundesamts für Justiz einzuholen. Ein solche Lösung scheint in Anbetracht der Koordinationsversäumnisse von Seiten der Schweizer Bundesbehörden ein möglicher Weg und würde eine niederschwellige Klärung der Prozesse ermöglichen.

Hat man es allerdings mit einer brachialen EU-Behörde zu tun (und die gibt es wohl), dann wird man auf wenig Verständnis für den Fall einer wegen Art. 271 StGB verweigerten Kooperation stossen. Die Risiken nach schweizerischem Recht können gemildert werden, indem alle möglicherweise herauszugebenden Informationen von Anfang an beim europäischen Vertreter vorliegen, dieser also einer aufsichtsrechtlichen Editionsverfügung Folge leisten kann, ohne auf Unterlagen aus der Schweiz Rückgriff nehmen zu müssen. Der Vertreter wäre folglich regelmässig, z.B. einmal im Jahr, mit aktuellen Informationen aufzudatieren. Sobald allerdings eine Anfrage einer EU-Behörde an

[55] Die ausländische Aufsichtsbehörde könnte beispielsweise früh im Verfahren substanzielle Sicherheit verlangen, um die Vollstreckung allfälliger Bussen sicherzustellen.

den Vertreter gerichtet wurde, errichtet sich eine Blockade infolge des Risikos gemäss Art. 271 StGB.

Entsprechend empfiehlt es sich mit Blick auf die delikaten Fragen im Zusammenhang mit dem EU-Vertreter eine *Verfahrensstrategie* zu definieren und die Vorgehensweise sorgfältig und im Voraus festzulegen. Insofern spielen nicht zuletzt Erwägungen mit Blick auf die Organisationsstruktur und gegenwärtige sowie geplante Geschäftsaktivitäten der Institution eine Rolle.[56]

3. Übersicht Pflichtenhefte

Bereits im Rahmen der bisherigen Ausführungen wurde sichtbar, dass die Pflichten gemäss DSGVO weit- und tiefgreifend sowie facettenreich sind.[57] Mehrere neu geschaffene Instrumente dokumentieren eindrücklich, wie der Gesetzgeber nunmehr darauf abzielt, das Datenschutzrecht seiner bisher primär formellen Existenz zu entheben und diesem in der Realität Griffigkeit zu verleihen. Mit anderen Worten geht es darum, einem bislang attestierten Vollzugsdefizit der Datenschutzregulierung wirksam entgegenzutreten. Personendatenverarbeitende Stellen werden früher, konkreter und nachdrücklicher in die Pflicht genommen, ein eigentliches Datenschutz-Compliance-Programm resp. eine Data Governance zu entwickeln und umzusetzen.[58] Ziel und Aufgabe ist entsprechend auch, das Datenschutzrecht operationalisierbar zu machen. Zentrale Ansätze und Elemente sind die bereits erwähnten Dokumentations- und Rechenschaftspflichten sowie der risikobasierte Ansatz, der sich wie ein roter Faden durch die Bestimmungen und damit auch Pflichten der DSGVO zieht.

Die Pflichten von Verantwortlichem/Controller und Auftragsverarbeiter/Processor bei *direkter Anwendbarkeit der DSGVO* lassen sich bildlich in *Gestalt zweier konzentrischer Kreise* darstellen, die eine gemeinsame Schnittmenge haben, wobei der Kreis des Controllers gegenüber demjenigen des Processors grösser ist. Mit anderen Worten gibt es (mehr) Pflichten, die nur den Controller, einige Pflichten, die nur den Processor treffen und solche, die von beiden zu erfüllen sind.[59] Exemplarisch für Letztere sind namentlich die sog. TOM,

---

[56] Wenn man eine Niederlassung in der EU hat, allerdings nicht aufgrund von Art. 3 Abs. 1 DSGVO, sondern gemäss Art. 3 Abs. 2 DSGVO einen EU-Vertreter zu bestellen hat, besteht ein potenzielles Vollstreckungsrisiko gegenüber der EU-Niederlassung.

[57] Zur Vertiefung sei insofern auf die Kommentarliteratur hingewiesen.

[58] Eine gute Orientierungshilfe für die Praxis liefern KRANIG/SACHS/GIERSCHMANN, Datenschutz-Compliance Handlungshilfe, *passim*.

[59] Vgl. auch PASSADELIS/ROTH, Jusletter 4. April 2016, Rz. 7 und Rz. 46 ff.

die technischen und organisatorischen Massnahmen und damit Art. 32 DSGVO. Grosse Bedeutung kommt darüber hinaus dem schriftlichen Vertrag zwischen den Parteien zu.

Im Sinne einer Übersicht die wichtigsten Pflichten, die nur oder auch für den *Auftragsverarbeiter/Processor* einschlägig sind:

- Art. 27 DSGVO: Auftragsverarbeiter aus Drittland, EU-Vertreter;
- Art. 29 DSGVO: Weisungsgebundenheit;
- Art. 30 Abs. 2 DSGVO: Führen eines Verfahrensverzeichnisses;
- Art. 31 DSGVO: Zusammenarbeit mit den Behörden;
- Art. 32 DSGVO: Sicherheitsmassnahmen;
- Art. 33 Abs. 2 DSGVO: Meldepflicht bei Datenschutzverstössen;
- Art. 35 Abs. 8 DSGVO;
- Art. 36 Abs. 2 DSGVO i.V.m. EWG 95;
- Art. 37 ff. DSGVO: Benennung eines Datenschutzbeauftragten;
- Art. 46 DSGVO.

Der *Verantwortliche/Controller* ist Adressat weitreichender, umfassender und facettenreicher Pflichten gemäss DSGVO, die nachfolgend nicht abschliessend aufgeführt werden. Besonders hingewiesen sei nur auf die folgenden Vorgaben:

- Art. 5 f. DSGVO: Einhaltung der Verarbeitungsgrundsätze;
- Art. 12 ff. DSGVO: Gewährleistung der Betroffenenrechte;
- Art. 24 DSGVO: Massnahmen der Datenschutz-Compliance;
- Art. 30 DSGVO: Erstellung des Verarbeitungsverzeichnisses;
- Art. 33 f. DSGVO: Meldepflichten bei Datensicherheitsvorfällen;
- Art. 35 DSGVO: Datenschutz-Folgenabschätzung.

4. Fazit

Die Aufgabe, eine mit den Vorgaben der DSGVO in Einklang stehende Datenschutz-Compliance zu etablieren, ist gross und komplex.[60] Dies gilt *a fortiori* für manch ein schweizerisches Unternehmen, zumal hierzulande von einem Vollzugsdefizit selbst mit Blick auf das geltende, markant mildere Regime des DSG für den privaten Bereich auszugehen ist. Zudem sehen sie sich

[60] Vgl. PASSADELIS/ROTH, Jusletter 4. April 2016, Rz. 77 f.; in diese Richtung bezeichnend der Titel des Beitrages von ROSENTHAL/VASELLA, digma 2018, S. 166–171.

unter Umständen mit der Einschlägigkeit diverser Erlasse konfrontiert, neben der DSGVO können das DSG sowie Spezialgesetzgebungen zu berücksichtigen sein.[61] Einige Schweizer Unternehmen stehen damit vor der Ausgangslage, für gewisse Felder die DSGVO zu implementieren, für andere das DSG, mit Blick auf welches im Rahmen der geplanten Totalrevision vieles unklar ist, sowie bereichsspezifische Vorgaben umzusetzen. Die Aufgabe, Unternehmen datenschutzkonform aufzustellen (wozu weit mehr als die verschärften Behördenmassnahmen Anlass geben) bedingt folglich zeitliche, finanzielle und fachliche Ressourcen. Es gilt organisatorische Zuständigkeiten zu fixieren, für die verschiedenen Anforderungsfelder Massnahmenpakete zu definieren, diese risikobasiert zu priorisieren, organisatorisch zuzuweisen, umzusetzen, in der Folge zu überprüfen, nachzubessern und entsprechend der Entwicklungen zu aktualisieren, wobei all dies zu dokumentieren ist. Damit der datenschutzrechtliche Bedeutungswandel im Gesamten vollzogen wird, bedarf es des klaren Bekenntnisses auf der Stufe der Unternehmensleitung, aber auch Verantwortlichkeiten bei den Linien sowie die stufen- und bereichsadäquate Awareness bei sämtlichen Mitarbeitenden.

Dass man der Datenschutzregulierung und ihrer Einhaltung im 21. Jahrhundert Nachdruck verleiht, erstaunt für eine Gesellschaft, die sich selbst als Informations- und Kommunikationsgesellschaft und Personendaten als wertvolles Gut/Gold qualifiziert, keineswegs. Die Vorgaben, mit Personendaten integer, rechtmässig, verantwortungsvoll und vertrauenswürdig umzugehen, ist nicht nur eine Pflicht. Eröffnet werden damit zugleich wertvolle Chancen, wobei man damit ebenso grundlegenden Werten und Zielen unserer Gesellschaft Rechnung trägt.

[61] PFAFFINGER/BALKANYI-NORDMANN, Private Q1 2019, S. 23.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 1. Mai 2019.

BUCHNER BENEDIKT, Informationelle Selbstbestimmung im Privatrecht, Habil. Tübingen 2006 (zit. Selbstbestimmung).

EBERT NICO/WIDMER MICHAEL, Datenschutz in Schweizer Unternehmen 2018, in: ZHAW School of Management and Law (Hrsg.), Eine Studie des Instituts für Wirtschaftsinformatik und des Zentrums für Sozialrecht, S. 1–24.

ENNÖCKL DANIEL, Art. 3, in: Sydow Gernot (Hrsg.), NomosKommentar, Handkommentar Europäische Datenschutzgrundverordnung, Baden Baden 2017 (zit. NomosKomm. DSGVO).

HARTUNG JÜRGEN, Art. 4 Nr. 7 und Nr. 8, in: Kühling Jürgen/Benedikt Buchner (Hrsg.), Beck Kommentar DSGVO, Datenschutzgrundverordnung, München 2017 (zit. Beck-Komm. DSGVO).

- Art. 27 DSGVO, in: Kühling Jürgen/Benedikt Buchner (Hrsg.), Beck Kommentar DSGVO, Datenschutzgrundverordnung, München 2017 (zit. Beck-Komm. DSGVO).
- Art. 28 DSGVO, in: Kühling Jürgen/Benedikt Buchner (Hrsg.), Beck Kommentar DSGVO, Datenschutzgrundverordnung, München 2017 (zit. Beck-Komm. DSGVO).

HERBST TOBIAS, Art. 4 Nr. 2, in: Kühling Jürgen/Benedikt Buchner (Hrsg.), Beck Kommentar DSGVO, Datenschutzgrundverordnung, München 2017 (zit. Beck-Komm. DSGVO).

INGOLD ALBERT, Art. 26 und Art. 28, in: Sydow Gernot (Hrsg.), NomosKommentar, Handkommentar Europäische Datenschutzgrundverordnung, Baden Baden 2017 (zit. NomosKomm. DSGVO).

KLAR MANUEL, Art. 3, in: Kühling Jürgen/Benedikt Buchner (Hrsg.), Beck Kommentar DSGVO, Datenschutzgrundverordnung, München 2017 (zit. Beck-Komm. DSGVO).

KRANIG THOMAS/SACHS ANDREAS/GIERSCHMANN MARKUS, Datenschutz-Compliance nach der DS-GVO, Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden, Köln 2017 (zit. Datenschutz-Compliance Handlungshilfe).

PASSADELIS NICOLAS/ROTH SIMON, Weisser Rauch über Brüssel. Was Schweizer Unternehmen über die europäische Datenschutz-Grundverordnung wissen müssen, Jusletter 4. April 2016.

PFAFFINGER MONIKA/BALKANYI-NORDMANN NADINE, Neues Datenschutzrecht. Europa macht Ernst mit Datenschutz, Schweizer Bank Mai 2018, S. 21–22.

- Mit dem Datenschutz gilt es nun ernst, Private Q1 2019, S. 22–23.

RASCHAUER NICOLAS, Art. 24, in: Sydow Gernot (Hrsg.), NomosKommentar, Handkommentar Europäische Datenschutzgrundverordnung, Baden Baden 2017 (zit. NomosKomm. DSGVO).

ROSENTHAL DAVID/VASELLA DAVID, Erste Erfahrungen mit der DSGVO, digma 2018, S. 166–171.

VASELLA DAVID, Zum Anwendungsbereich der DSGVO, digma 2017, S. 220–222.

VESTING THOMAS, Das Internet und die Notwendigkeit der Transformation des Datenschutzes, in: Karl-Heinz Ladeur (Hrsg.), Innovationsoffene Regulierung des Internet, Baden-Baden 2003, S. 155–190.

Materialien

Bayerisches Landesamt für Datenschutzaufsicht (BLD), FAQ zur DS-GVO, Auftragsverarbeitung, Abgrenzung, Stand 20. Juli 2018, abrufbar unter: <https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf> (zit. BLD, FAQ Auftragsverarbeitung), S. 1–3.

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017-1084, S. 6941–7192.

Commission Nationale de l'Informatique et des Libertés (CNIL), Règlement européen sur la protection des données personnelles, Guide du sous-traitant, Stand September 2017, abrufbar unter: <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants> (zit. CNIL, Guide sous-traitant).

Eidgenössischer Öffentlichkeits- und Datenschutzbeauftragter (EDÖB), Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, Stand November 2018, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/ dokumentation/rechtliche-grundlagen/Datenschutz%20-%20International/DSGVO. html> (zit. EDÖB, EU-DSGVO und die Schweiz), S. 1–11.

European Banking Federation (EBF), EBF Response to the EDPB draft guidelines on the territorial scope to the GDPR, 18 January 2019, abrufbar unter: <https://www.swissbanking.org/de/themen/informationen-fuer-privatkunden/privatsphaere-datenschutz/ebf_035299-ebf-response-to-the-edpb-draft-guide lines-on-the-territoria-_.pdf> (zit. EBF, Response guidelines scope GDPR), S. 1–5.

European Commission, Article 29 Data Protection Working Party (WP 29), Opinion 1/2010 on the concepts of "controller" and "processor", Adopted on 16 February 2010, abrufbar unter : <https://ec.europa.eu/justice/article-29/documentation/opini on-recommendation/files/2010/wp169_en.pdf> (zit. WP 29, Concept of controller and processor), S. 1–35.

European Data Protection Board (EDPB), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for the consultation, Adopted on 16 November 2018, abrufbar unter: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb _guidelines_3_2018_territorial_scope_en.pdf> (zit. EDPB, Consultation Paper Scope), S. 1–23.

Ponemon Institute LLC/Centrify, The impact of data breaches on reputation & Share Value, Sponsored by Centrify, Independently conducted by Ponemon Institute LLC Publication Date, A Study of U.S. Marketers, IT Practitioners and Consumers, May 2017, abrufbar unter: <https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf> (zit. Impact on Reputation), S. 1–28.

Schweizerische Bankiervereinigung (SBVg/EBF), Cloud-Leitfaden, Gutachten zum Bankkundengeheimnis vom 26. März 2019, abrufbar unter: <https://www.swissbanking.org/de/medien/statements-und-medienmitteilungen/sicheres-cloud-banking-sbvg-leitfaden-schlaegt-bruecke-in-die-zukunft (zit. SBVg/EBF, Cloud Leitfaden), S. 1–44.

Privacy by Design & Privacy by Default – Relevanz für die Banken

Martina Reber, Bern*

* Rechtsanwältin, MLaw, wissenschaftliche Assistentin und Doktorandin am Institut für Bankrecht, Universität Bern.

> *We can build, or architect, or* code *cyberspace to protect values that we believe are fundamental. Or we can build, architect, or code cyberspace to allow those values to disappear.*
>
> LAWRENCE LESSIG, Code, version 2.0, S. 6.

I. Einleitung

Die Kaffeemaschine, die sich automatisch aufheizt, wenn der Wecker klingelt. Der Kühlschrank, der Vorschläge für Menus unterbreitet, die man aus seinem aktuellen Inhalt kochen kann – und der auch noch darauf hinweist, dass der Joghurt abgelaufen ist. Das Auto, das selber einen Service-Termin vereinbart. Die Smartwatch der Grossmutter, die die Angehörigen alarmiert, wenn ihre Trägerin gestürzt ist.

Unsere Alltagsgegenstände sind zunehmend mit Computern versehen. Zwar besteht zurzeit (noch?) in vielen Bereichen eine Wahlmöglichkeit zwischen herkömmlichen Geräten und sogenannten *Smart Devices.* Je nach Lebensstil sind Computer aber bereits jetzt so allgegenwärtig, dass wir sie kaum mehr wahrnehmen (*Ubiquitous Computing*).[1]

Nicht nur unsere Alltagsgegenstände, sondern auch unser Alltag verlagert sich nach und nach ins Internet: Wir kaufen online ein, wickeln unsere Zahlungen online ab, lernen online Menschen kennen, kommunizieren online, beziehen Informationen online.

Diese Verlagerung führt dazu, dass unser Leben immer mehr vom Quelltext der verwendetem Hard- und Software beeinflusst wird. LAWRENCE LESSIG verkürzte die These, dass der Quelltext im virtuellen Raum die gleiche Rolle einnehme wie das Recht im realen Raum, auf drei prägnante Worte: *Code is law*.[2] Ein zynischer Geist könnte spotten, dass die Juristinnen und Juristen nach den drei schweren Kränkungen der Menschheit, der kopernikanischen, der darwinschen und der Freud'schen Kränkung,[3] noch eine vierte, Lessig'sche Kränkung zu erdulden hätten: Dass das Recht nach und nach vom Quellcode verdrängt werde.

Obschon die Lage wohl nicht ganz so drastisch ist, gelangte man doch zunehmend zur Erkenntnis, dass ein wirksamer Datenschutz nicht alleine durch

---

1 Diese Entwicklung wurde bereits 1991 vorausgesehen, siehe dazu WEISER, S. 94 ff. Zu den datenschutzrechtlichen Fragestellungen im Zusammenhang mit Ubiquitous Computing siehe z.B. HÖDL, Rz. 2.

2 LESSIG, S. 5.

3 Zu den drei Kränkungen FREUD, S. 3 ff.

eine reaktive Betrachtung im Nachhinein realisiert werden kann, sondern proaktiv in die datenbearbeitenden Systeme eingebaut werden muss.[4] Entsprechend verpflichtet die DSGVO den Verantwortlichen, technische und organisatorische Massnahmen zur Umsetzung ihrer Anforderungen vorzusehen – und zwar bereits ab der Planung einer Datenverarbeitung (Art. 25 DSGVO). Für diese Regelung hat sich die Bezeichnung *Privacy by Design* durchgesetzt. Ein besonderer Anwendungsfall dieses Konzepts ist *Privacy by Default*, d.h. die Pflicht, Voreinstellungen datenschutzfreundlich auszugestalten. Auch im Revisionsentwurf des Bundesrates für ein neues Datenschutzgesetz (E-DSG)[5] ist eine entsprechende Regelung vorgesehen.

Nach einer Erläuterung der Begriffe und Hintergründe von Privacy by Design und Privacy by Default untersucht dieser Beitrag, wann die beiden Konzepte für Schweizer Banken gelten. Es folgt eine detailliertere Betrachtung der Konzepte mit bankbezogenen Umsetzungsbeispielen. Schliesslich zeigt der Beitrag auf, wie Privacy by Design und Privacy by Default durchgesetzt werden.

II. Begriffe

1. Privacy by Design

Der Begriff Privacy by Design, wörtlich übersetzt etwa «Privatsphäre durch Gestaltung», wird uneinheitlich verwendet.

Teilweise wird damit auf Art. 25 DSGVO (oder den analogen Art. 6 E-DSG) verwiesen, der den Verantwortlichen verpflichtet, die Anforderungen der DSGVO mittels technischer und organisatorischer Massnahmen umzusetzen. Diese Bezeichnung ist eigentlich nicht ganz präzise, da Art. 25 DSGVO nicht primär den Schutz der Privatsphäre i.S.v. Art. 7 der Charta der Grundrechte der Europäischen Union (GRCh)[6] bezweckt, sondern den Schutz personenbezogener Daten i.S.v. Art. 8 GRCh (vgl. Art. 1 Abs. 2 DSGVO). Aus diesem Grund spricht der englische Normtext von *Data Protection by Design*. Dennoch hat sich der Begriff Privacy by Design weitgehend durchgesetzt.[7]

---

4 NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 2.

5 Entwurf zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017, S. 7193-7276).

6 Charta der Grundrechte der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 391-407.

7 Zum Ganzen siehe z.B. BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 2; KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 19; MANTZ, in: Sydow (Hrsg.), Art. 25 N. 1.

Der Grund dafür ist historisch bedingt und führt uns zum zweiten möglichen Begriffsinhalt von Privacy by Design: Art. 25 DSGVO beruht auf einem historisch gewachsenen Konzept, welches in den 1990er Jahren zu sieben Grundsätzen verdichtet und als Privacy by Design bezeichnet wurde. Dieses Konzept ist zwar nicht ganz deckungsgleich mit Art. 25 DSGVO,[8] basiert aber auf der gleichen Logik: Datenschutzanliegen sollen bei sämtlichen Datenbearbeitungen von Beginn weg und während des gesamten Lebenszyklus berücksichtigt werden. Datenschutzverstösse sollen am besten bereits zum Vornherein verhindert werden, indem entsprechende Massnahmen gleich in IT-Systeme und Geschäftsabläufe implementiert werden.[9]

Dieser Beitrag interessiert sich primär für Privacy by Design i.S.v. Art. 25 DSGVO und Art. 6 E-DSG. Zum besseren Verständnis wird aber auch kurz auf den (ideen-)geschichtlichen Hintergrund Bezug genommen.

2. Privacy by Default

Privacy by Default, übersetzt etwa «Privatsphäre als Standard», hat ebenfalls zwei Bedeutungen: Einerseits ist Privacy by Default oder wörtlich «Privacy as the Default Setting» einer der sieben Grundsätze des bereits angesprochenen Konzepts Privacy by Design. Dieser Grundsatz besagt, dass IT-Systeme und Geschäftsabläufe so konzipiert werden müssen, dass der Schutz personenbezogener Daten keiner aktiven Handlung des Individuums bedarf, sondern standardmässig implementiert sein soll.[10]

Andererseits ist mit Privacy by Design häufig Art. 25 Abs. 2 DSGVO gemeint, wonach der Verantwortliche die Voreinstellungen so auszugestalten hat, dass nur die jeweils notwendigen personenbezogenen Daten verarbeitet werden. Vereinfacht gesagt: Wenn die betroffene Person einen Dienst, wie beispielsweise eine App, zum ersten Mal gebraucht, müssen die datensparsamsten Konfigurationen eingestellt sein, und sämtliche Einstellungen, die zu umfassenderen oder intensiveren Datenbearbeitungen führen, müssen von

---

8 BYGRAVE, S. 106.

9 Vgl. zum Gesamtkonzept von Privacy by Design CAVOUKIAN, passim. Zum Zweck von Art. 25 DSGVO siehe z.B. MANTZ, in: Sydow (Hrsg.), Art. 25, N. 1 ff.; zum Zweck von Art. 25 DSGVO siehe BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 1; HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 16 ff.; HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 11; MANTZ, in: Sydow (Hrsg.), Art. 25 N. 1 ff., 18 ff.; MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 8 ff.

10 Vgl. dazu CAVOUKIAN, passim.

der betroffenen Person aktiv vorgenommen werden. In der Marginalie wird dieses Prinzip als *Data Protection by Default* bezeichnet.

III. Hintergrund

Die Idee, dass Datenschutzanliegen gleich durch die Technik selber verwirklicht werden sollen, ist älter als die Datenschutzgesetzgebung.[11] Schon 1969 propagierte der US-amerikanische Rechtsprofessor ARTHUR R. MILLER entsprechende technische Massnahmen[12] und forderte, dass diese bereits von Beginn weg in die Hard- und Software zu implementieren seien:

> «Whatever technical safeguards are deemed appropriate for particular computer systems, they undoubtedly will be most efficient and economical if they are incorporated into the original design of the hardware and software than if they are added subsequently».[13]

Auch auf der Gesetzgebungsebene scheinen solche Forderungen bereits früh Beachtung gefunden zu haben: So soll der deutsche Gesetzgeber laut JÖRG POHLE bereits mit § 6 Abs. 1 BDSG 1978[14] die Einführung einer Pflicht, sämtliche Vorschriften des BDSG 1978 mittels technischer und organisatorischer Massnahmen umzusetzen, bezweckt haben.[15] Diese Absicht sei aber noch vor Inkrafttreten der Norm durch Zusammenwirken von Datenschutzbehörden und Wirtschaft vereitelt worden: Vorläufige Verwaltungsvorschriften zu § 6 hätten den Anwendungsbereich entgegen dem expliziten Wortlaut[16] auf eine blosse Datensicherheitsvorschrift beschränkt.[17]

---

11 Das weltweit erste formelle Datenschutzgesetz war das Datenschutzgesetz des Landes Hessen vom 7. Oktober 1970, in: Gesetz- und Verordnungsblatt für das Land Hessen, Teil I, 1970 Nr. 41, S. 625-642.

12 MILLER, S. 1207 ff.

13 MILLER, S. 1211.

14 Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG) vom 27. Januar 1977, in: Bundesgesetzblatt Teil I, 1977 Nr. 7, S. 201 ff.

15 POLE, S. 42.

16 § 6 Abs. 1 BDSG 1978 lautete: «Wer im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Personen oder Stellen personenbezogene Daten verarbeitet, hat die **technischen organisatorischen Maßnahmen** zu treffen, die erforderlich sind, um die Ausführung der **Vorschriften dieses Gesetzes**, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht» (Hervorhebungen hinzugefügt).

17 POLE, S. 42.

Freilich stellen bereits solche Datensicherheitsvorschriften, wie sie auch das geltende schweizerische Datenschutzgesetz[18] mit Art. 7 kennt,[19] einen Schritt in die Richtung eines eingebauten Datenschutzes dar. Denn immerhin sehen sie vor, dass ein besonders zentrales Datenschutzanliegen, welches eng mit der Verwirklichung weiterer Datenschutzanliegen zusammenhängt,[20] mittels technischer und organisatorischer Massnahmen verwirklicht werden muss. Eine solche Norm fand sich mit Art. 17 auch in der Richtlinie 46/95/EG.[21] Der ErwG 46 dieser Richtlinie ging allerdings weiter und kam umfangmässig Art. 25 DSGVO nahe, denn er nannte die Sicherheit lediglich beispielhaft.[22]

Nicht nur Lehre und Gesetzgeber, sondern auch gewisse Datenschutzbehörden trieben die Entwicklung hin zu Privacy by Design voran. 1995 veröffentlichten die Datenschutzbehörde der kanadischen Provinz Ontario und die niederländische Datenschutzbehörde eine Studie zu *Privacy Enhancing Technologies (PET).*[23] Der Begriff Privacy by Design wurde erst in den späten 1990er Jahren geprägt. Seine Urheberin ist ANN CAVOUKIAN, die von 1997 bis 2014 Datenschutzbeauftragte der kanadischen Provinz Ontario war und an der obgenannten PET-Studie mitwirkte. Sie entwickelte die sieben Grundprinzipien von Privacy by Design,[24] die anschliessend international Anerkennung fanden.[25]

---

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

19 Art. 7 Abs. 1 DSG lautet: «Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.»

20 So auch BSK-DSG-STAMM/PFISTER, Art. 7 N 2; MANTZ, in: Sydow (Hrsg.), Art. 25 DSGVO N. 6.

21 Art. 17 der Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (aufgehoben).

22 ErwG 46 der RL 46/95/EG enthielt folgenden Auszug: «Für den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten müssen geeignete **technische und organisatorische Maßnahmen** getroffen werden, und zwar sowohl zum **Zeitpunkt der Planung** des Verarbeitungssystems als auch zum **Zeitpunkt der eigentlichen Verarbeitung**, um **insbesondere deren Sicherheit** zu gewährleisten und somit jede unrechtmäßige Verarbeitung zu verhindern» (Hervorhebungen hinzugefügt).

23 INFORMATION AND PRIVACY COMMISSIONER, ONTARIO, CANADA/REGISTRATIEKAMER, THE NETHERLANDS, Privacy-Enhancing Technologies: The Path to Anonymity, August 1995. Siehe hierzu grundlegend BORKING, *passim*.

24 CAVOUKIAN, Privacy by Design, The 7 Foundational Principles.

25 So z.B. von der 32ND INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS, Jerusalem, Israel, 27-29 October, 2010, Resolution on Privacy by Design;

Mit Inkrafttreten der DSGVO wurde Privacy by Design gar zur sanktionsbewehrten Pflicht.

IV. Geltung für Schweizer Banken

Dieser Abschnitt soll darüber Aufschluss geben, unter welchen Voraussetzungen Privacy by Design und Privacy by Default für Schweizer Banken gelten.

1. Nach DSGVO

Privacy by Design und Privacy by Default sind in Art. 25 DSGVO vorgesehen und gelten daher insoweit für Schweizer Banken, als diese in den Anwendungsbereich der DSGVO fallen.[26]

Sachlich ist die DSGVO anwendbar, wenn personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden oder wenn sie zwar nicht automatisiert verarbeitet werden, allerdings in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DSGVO). Der sachliche Anwendungsbereich dürfte bei den meisten Datenverarbeitungen durch Banken gegeben sein.

Räumlich ist die DSGVO namentlich anwendbar, wenn eine Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung der Bank in der EU erfolgt – unabhängig davon, ob die Datenverarbeitung in der EU stattfindet (vgl. Art. 3 DSGVO).[27]

Weiter kann die DSGVO auch dann anwendbar sein, wenn die Bank über keine Niederlassung in der EU verfügt. Dies einerseits dann, wenn die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen, die sich in der EU befinden, Waren oder Dienstleistungen anzubieten – unabhängig davon, ob entgeltlich oder unentgeltlich (vgl. Art. 3 Abs. 2 Bst. a DSGVO). Andererseits ist die DSGVO anwendbar, wenn die Datenverarbeitung im Zusammenhang damit steht, das Verhalten betroffener Personen, die sich in der EU befinden, zu beobachten, soweit ihr Verhalten in der EU erfolgt (vgl. Art. 3 Abs. 2 Bst. b DSGVO).[28]

---

von der ARTIKEL-29-GRUPPE, WP 223, Opinion 8/2014. Weiterführend zur Entstehungsgeschichte von Privacy by Design international und in der Schweiz TALL, S. 39 ff.

[26] Ausführlich dazu PFAFFINGER, Extraterritoriale Wirkung, zur Publikation vorgesehen.

[27] Für weitere Ausführungen zum Niederlassungserfordernis siehe EDPB, Guidelines 3/2018, S. 4 ff.

[28] Für weitere Ausführungen zum Marktortpinzip siehe EDPB, Guidelines 3/2018, S. 12 ff.

2. Nach E-DSG

Der Revisionsentwurf des Bundesrates sieht eine Pflicht des Verantwortlichen vor, «die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 5.» Dies hat er ab der Planung zu tun (Art. 6 Abs. 1 E-DSG). Privacy by Design ist somit im Revisionsentwurf vorgesehen. Auch Privacy by Default, d.h. eine Pflicht zu datenschutzfreundlichen Voreinstellungen, ist im Revisionsentwurf enthalten (Art. 6 Abs. 3 E-DSG).

Je nach Ausgang der parlamentarischen Beratungen muss daher damit gerechnet werden, dass Privacy by Design und Privacy by Default künftig für Schweizer Banken gelten.

3. Nach DSG

a) Privacy by Design

Privacy by Design ist fragmentarisch bereits im geltenden Recht enthalten. Einzelnen Datenschutzanliegen muss nämlich bereits jetzt mittels technischer und organisatorischer Massnahmen Rechnung getragen werden.

So sind Personendaten gemäss Art. 7 Abs. 1 DSG durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen. Dass diese Massnahmen vor der eigentlichen Datenbearbeitung getroffen werden müssen, damit die Datensicherheit ab Beginn der Bearbeitung gewährleistet ist, gebietet die Logik.[29] Die Datensicherheit steht zu verschiedenen weiteren Datenbearbeitungsgrundsätzen in Beziehung oder bildet gar deren Voraussetzung.[30] Dies zeigt sich in den konkretisierenden Art. 8 ff. VDSG: Beispielsweise dient nach Art. 10 Abs. 1 VDSG die Protokollierungspflicht namentlich dem Zweckbindungsgrundsatz.[31] Weiter sind Datensammlungen gemäss Art. 9 Abs. 2 VDSG «so zu gestalten, dass die betroffenen Personen ihr Auskunftsrecht und ihr Recht auf Berichtigung wahrnehmen können». Hilfestellung zur Umsetzung bieten der Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes des EDÖB und, für Banken, der Anhang 3 des FINMA-Rundschreibens 2008/21.

---

29 Vgl. ROSENTHAL, Rz. 40.

30 BSK-DSG-STAMM/PFISTER, Art. 7 N 2.

31 Vgl. Art. 10 Abs. 1 Satz 2 VDSG: «Eine Protokollierung hat insbesondere dann zu erfolgen, wenn sonst nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen **Zwecke** bearbeitet wurden, für die sie **erhoben oder bekannt gegeben** wurden» (Hervorhebungen hinzugefügt).

Privacy by Design ist für Schweizer Banken somit nicht vollständig neu. Neu ist lediglich, dass sämtliche Datenschutzanforderungen und nicht nur einzelne mittels technischer und organisatorischer Massnahmen umgesetzt werden müssen.

b) Privacy by Default

Eine ausdrückliche Pflicht zu datenschutzfreundlichen Voreinstellungen ist im DSG nicht enthalten. Allerdings ergibt sie sich aus dem Verhältnismässigkeitsprinzip in Art. 4 Abs. 2 DSG. Danach muss jede Datenbearbeitung geeignet, erforderlich und zumutbar sein.[32] Erforderlich ist diejenige Massnahme, welche die Interessen der betroffenen Person am wenigsten beeinträchtigt, mithin den geringstmöglichen Eingriff darstellt.[33] Dies gebietet, dass auch die Voreinstellungen so ausgestaltet werden müssen, dass nur die für den konkreten Bearbeitungszweck erforderlichen Daten bearbeitet werden. [34]

V. Privacy by Design nach Art. 25 Abs. 1 DSGVO

Nachfolgend sollen die Anforderungen von Privacy by Design, wie sie in Art. 25 DSGVO vorgesehen sind, näher erläutert werden.

1. Wortlaut

Der mit Corrigendum vom 19. April 2018 nochmals angepasste Wortlaut von Art. 25 Abs. 1 DSGVO lautet folgendermassen:[35]

> «Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung —, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den

32 Z.B. BSK-DSG-MAURER-LAMBROU/STEINER, Art. 4 N. 9, m.w.H.

33 Z.B. BSK-DSG-MAURER-LAMBROU/STEINER, Art. 4 N. 9, m.w.H.

34 So auch VASELLA, in: Staffelbach/Keller (Hrsg.), N. 7.156.

35 Corrigendum abrufbar unter: <http://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf>.

Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen».

2. Zweck

Der Zweck von Privacy by Design ist, Datenschutz zu einem möglichst frühen Zeitpunkt zu verwirklichen.[36] Dazu soll der Datenschutz bereits bei der Konzeption und Entwicklung der datenverarbeitenden Systeme berücksichtigt und idealerweise in diese «eingebaut» werden.[37] Davon erhofft sich der Gesetzgeber eine proaktive Verhinderung von Datenschutzverstössen.[38]

3. Adressat

Adressat von Art. 25 DSGVO ist nur der Verantwortliche.[39] Auftragsverarbeiter werden mittelbar erfasst (vgl. Art. 28 DSGVO). Nicht adressiert werden die Hersteller. Diese sollen gemäss ErwG 78 lediglich zur Berücksichtigung des Datenschutzes «ermutigt werden». Dies stellt eine erhebliche Relativierung von Privacy by Design dar, da die Verantwortlichen regelmässig fertige Hard- und Software einsetzen und dabei mit denjenigen Produkten vorliebnehmen müssen, die ihnen die Hersteller anbieten.[40]

4. Zielrichtung

Als Ziel nennt Art. 25 Abs. 1 DSGVO zunächst die Umsetzung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DSGVO, d.h. Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Weiter sollen notwendige Garantien geschaffen werden, um die Rechte der betroffenen Personen gemäss Art. 12 ff. DSGVO (Information, Auskunft, Berichtigung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch) zu gewährleisten und den Anforderungen der DSGVO zu genügen.

---

36 BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 1.

37 BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 1.

38 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 2.

39 Als solcher gilt gemäss Art. 4 Ziff. 7 DSGVO «die natürliche oder juristische Person, behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet […]».

40 Vgl. MANTZ, in: Sydow (Hrsg.), Art. 25 N. 17, m.w.H.

Kurz: Die Norm bezweckt die Einhaltung sämtlicher Anforderungen der DSGVO.[41]

Mit «Garantien» (englisch: «safeguards») ist nicht gemeint, dass der Verantwortliche jegliche Verletzung der DSGVO zum Vornherein verhindern müsste.[42] Es wird lediglich erwartet, dass er über ein technisches und organisatorisches Gesamtkonzept hinsichtlich Datenschutz verfügt.[43] Dies geht auch aus ErwG 78 hervor, wonach der Verantwortliche «interne Strategien festlegen und Maßnahmen ergreifen» soll.

5. Bedeutung und Systematik

Da Art. 25 Abs. 1 DSGVO auf sämtliche Anforderungen der DSGVO verweist, stellt er wohl deren umfassendste Norm dar.[44] Seine Bedeutung wird dadurch unterstrichen, dass seine Verletzung mit Busse bedroht ist (vgl. Art. 83 Abs. 4 Bst. a DSGVO), er darüber hinaus auch bei der Verhängung einer Busse wegen eines *anderen* DSGVO-Verstosses zu berücksichtigen ist (vgl. Art. 83 Abs. 2 Bst. c).

Systematisch ist Art. 25 DSGVO im Kapitel IV bei den allgemeinen Pflichten des Verantwortlichen angesiedelt und konkretisiert Art. 24 DSGVO, der den Verantwortlichen verpflichtet, nach einem risikobasierten Ansatz geeignete technische und organisatorische Massnahmen vorzusehen.[45] Überschneidungen weist Art. 25 DSGVO zu Art. 32 DSGVO auf, der eine Pflicht vorsieht, technische und organisatorische Massnahmen zur Datensicherheit zu treffen.[46] Teilweise wird vertreten, die beiden Normen würden unterschiedliche Schutzzwecke aufweisen: Art. 32 DSGVO bezwecke die Datensicherheit und Art. 25 DSGVO die Datenminimierung.[47] Diese Ansicht übersieht, dass Art. 25 DSGVO weit mehr als bloss die Datenminimierung bezweckt, nämlich die wirksame Umsetzung sämtlicher Anforderungen der DSGVO einschliesslich

41 Z.B. MANTZ, in: Sydow (Hrsg.), Art. 25 N. 19; MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 34; HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 17.

42 NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 20.

43 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 29; ausführlich NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 20.

44 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 DSVGO N. 15.

45 BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 8; HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 10; KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 17; EDPS, Opinion 5/2018, Rz. 249.

46 HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 10; KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 17; HÖTZENDORFER, S. 145.

47 HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 10.

der Datensicherheit.[48] Art. 32 DSGVO weist daher einen engeren Schutzzweck auf als Art. 25 DSGVO und stellt eine Konkretisierung desselben bezüglich der Datensicherheit dar.[49] Hinsichtlich des Adressatenkreises ist Art. 32 DSGVO hingegen weiter als Art. 25 DSGVO und gilt nicht nur für den Verantwortlichen unmittelbar, sondern auch für den Auftragsverarbeiter.

6. Zeithorizont

Das genuin Neue von Art. 25 DSGVO im Vergleich zu Art. 24 DSGVO ist, dass die Pflicht, technische und organisatorische Massnahmen zu treffen, zeitlich ausdrücklich vorverlagert wird: Sie gilt bereits ab der «Festlegung der Mittel», also dem verbindlichen Entscheid über die Mittel der Verarbeitung, der beispielsweise in Abmachungen mit Dritten oder internen Entscheidungen liegen kann.[50] Streng genommen ist zu diesem Zeitpunkt die DSGVO noch gar nicht anwendbar, denn diese gilt erst ab der eigentlichen Datenverarbeitung (vgl. Art. 2 DSGVO). Die einschlägige Lehre erachtet es daher als unwahrscheinlich, dass eine Missachtung von Art. 25 DSGVO zu einer Sanktionierung führt, solange noch keine Datenverarbeitung i.S. der DSGVO stattgefunden hat.[51]

Selbstverständlich gilt die Pflicht auch während der eigentlichen Verarbeitung. Dazu zählt auch die Löschung (vgl. Art. 4 Ziff. 2 DSGVO). Beabsichtigt wird, dass der Datenschutz während des gesamten Lebenszyklus der Verarbeitung gewährleistet wird.[52]

7. Technische und organisatorische Massnahmen

Der wohl grösste Kritikpunkt an Art. 25 Abs. 1 DSGVO ist, dass er zu abstrakt formuliert ist und kaum konkrete Anhaltspunkte enthält, welche technischen und organisatorischen Massnahmen zu ergreifen sind.[53] Hilfestellung bieten

---

48 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 18 f.; NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 8; KNYRIM, S. 145; HÖTZENDORFER, S. 146.

49 So auch HÖTZENDORFER, S. 145.

50 NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 13; KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 30.

51 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 35, m.w.H.; MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 43b; HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 23.

52 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 33, mit Verweis auf die Materialien; NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 14; MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 43c.

53 Z.B. HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 15; TAMÒ-LARRIEUX, S. 235.

einerseits Materialien von Behörden wie die Berichte der European Union Agency for Network and Information Security (ENISA),[54] der Leitfaden der norwegischen Aufsichtsbehörde,[55] die Vorläufige Stellungnahme des Europäischen Datenschutzbeauftragten[56] oder das Standard-Datenschutzmodell der 95. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, und andererseits wissenschaftliche Publikationen.[57]

Bei der Wahl seiner Vorgehensweise[58] sowie der konkreten Massnahmen hat der Verantwortliche ein erhebliches Auswahl- und Gestaltungsermessen.[59] Er selbst ist am besten in der Lage, die mit der Datenverarbeitung einhergehenden Folgen und die Wirksamkeit von Massnahmen einzuschätzen.[60] Aufgrund der weitreichenden Rechenschaftspflichten des Verantwortlichen ist es allerdings ratsam, wenn er seine Entscheidungen sauber dokumentiert.[61]

In diesem Kapitel werden einige Beispiele für technische und organisatorische Massnahmen gezeigt, die zur Umsetzung ausgewählter Anforderungen der DSGVO beitragen können. Sie sind selbstverständlich nicht abschliessend. Auf eine Betrachtung von Massnahmen zur Gewährleistung der Datensicherheit wird verzichtet, da den Banken hierzu bereits ausreichende Quellen zur Verfügung stehen.[62]

a) Allgemeine organisatorische Massnahmen

Während sich die technischen Massnahmen zur Umsetzung der einzelnen Datenschutzanliegen häufig stark unterscheiden, lassen sich mit den organisatorischen Massnahmen vielfach gleich mehrere Datenschutzanliegen verwirklichen. Sie weisen mithin häufig einen allgemeineren Charakter auf.

---

54 Insbesondere ENISA Privacy by Design; DIES., Big Data; DIES., Mobile Apps; DIES., PETs; DIES., Privacy by Default.

55 DATATILSYNET, Guide.

56 EDPS, Opinion 5/2018.

57 Erwähnt sei hier die Dissertation von TAMÒ-LARRIEUX, die in einerseits allgemeine Hinweise und andererseits ein konkretes Umsetzungsbeispiel enthält.

58 Zu den verschiedenen Methodiken des Privacy Engineering z.B. EDPS, Opinion 5/2018, Rz. 60 ff.

59 Z.B. NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 21.

60 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 48.

61 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 48.

62 Beispielsweise der Anhang 3 des FINMA-Rundschreibens 2008/21.

Eine mögliche organisatorische Massnahme sind interne Richtlinien, die Verhaltensregeln, Verantwortlichkeiten, Prozesse und interne Informationsflüsse klar festlegen.[63] Konkret kann die Bank in solchen Richtlinien beispielsweise regeln, wie sie ihre Informationspflichten nach Art. 13 f. DSGVO zu erfüllen gedenkt (z.B. durch den Kundenberater im Rahmen der Kontoeröffnung), wie die Zuständigkeiten und die Prozesse für die Wahrnehmung der Betroffenenrechte aussehen, mit welchen Rollen- und Berechtigungskonzepten sie den Grundsätzen der Vertraulichkeit, der Zweckbindung und der Datenminimierung Rechnung trägt (need-to-know-Basis), dass bei der Verarbeitung besonderer Kategorien personenbezogener Daten ein Vier-Augen-Prinzip gilt oder wer bei einem *data breach* zu benachrichtigen ist.

Damit diese internen Richtlinien von den Mitarbeitenden auch umgesetzt werden, können Schulungen durchgeführt und interne Massnahmen zur Durchsetzung (z.B. Stichproben, Ahndung von Verstössen) getroffen werden.[64] Von nicht zu unterschätzender Bedeutung ist die Kommunikation: Laut der ENISA setzen Entwickler Datenschutz häufig mit Datensicherheit gleich.[65] Es daher wichtig, dass die Juristinnen und die Techniker eine gemeinsame Sprache finden.

In der Literatur wird weiter vorgeschlagen, dass für komplexe Projekte interdisziplinäre Projektteams gebildet werden, dass in Einzelfällen zur Vornahme komplexer Abwägungsvorgänge (ggf. unabhängige) Ethikkomitees eingesetzt werden oder dass freiwillige Datenschutzfolgeabschätzungen unterhalb der Relevanzschwelle durchgeführt werden.[66]

b) Rechtmässigkeit

Im Anwendungsbereich der DSGVO ist jeweils zu beachten, dass anstelle des Erlaubnisprinzips mit Verbotsvorbehalt, wie es nach schweizerischem Recht gilt, das Verbotsprinzip mit Erlaubnisvorbehalt gilt. Danach ist eine Datenverarbeitung nur rechtmässig, wenn ein Erlaubnistatbestand gegeben ist (Art. 6 Abs. 1 DSGVO). Für besondere Kategorien personenbezogener Daten gilt ein eingeschränktes Erlaubnisregime (vgl. Art. 9 DSGVO), die Verarbeitung

---

63 NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 17; MANTZ, in: Sydow (Hrsg.), Art. 25 N. 60.

64 NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 17; MANTZ, in: Sydow (Hrsg.), Art. 25 N. 60.

65 ENISA, Mobile Apps, S. 45.

66 NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 17; KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 38.

personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten ist noch stärker eingeschränkt (vgl. Art. 10 DSGVO).

Der Rechtmässigkeit der Datenverarbeitung kann in erster Linie organisatorisch Rechnung getragen werden, beispielsweise, indem die Prozesse dergestalt definiert werden, dass vor jeder Datenverarbeitung die Rechtsgrundlage ermittelt und dokumentiert werden muss.[67]

Besonders anspruchsvoll in der Umsetzung sind die Anforderungen der DSGVO an die Einwilligung. Hervorzuheben ist hier das Erfordernis, dass es der betroffenen Person ermöglicht werden muss, in verschiedene Verarbeitungsvorgänge gesondert einzuwilligen (ErwG 43). Weiter kann die betroffene Person eine Einwilligung jederzeit widerrufen (Art. 7 Abs. 3 DSGVO). Zur Umsetzung dieser Anforderungen kann ein automatisiertes Einwilligungsmanagement eingesetzt werden.[68] In Apps kann dem Widerrufsrecht beispielsweise dadurch Rechnung getragen werden, dass den Nutzern ermöglicht wird, einzelne Funktionen wieder zu deaktivieren.

> Beispiel: Eine Bank bietet eine Mobile-Banking-App an, bei der das Login mittels Fingerabdruck erfolgen kann. Die Kundin kann die Fingerabdruck-Identifikation jederzeit wieder ausschalten.

c) Treu und Glauben

Aus dem Grundsatz von Treu und Glauben wird abgeleitet, dass die Systeme so gestaltet werden müssen, dass den betroffenen Personen bei der Wahrnehmung ihrer Rechte keine Hürden in den Weg gelegt werden dürfen.[69]

> Ein Negativbeispiel sind hier sog. *dark patterns*, d.h. Gestaltungen der Benutzeroberfläche, die den Nutzer gezielt dahingehend beeinflussen sollen, Konfigurationen vorzunehmen, die möglichst umfassende Datenverarbeitungen erlauben.[70] Dies geschieht beispielsweise dadurch, dass datenschutzfreundliche Optionen versteckt werden, dass deren Einstellung massiv länger dauert als die Wahl von Optionen, die umfangreichere Datenverarbeitungen erlauben, oder durch vermeintliche «Warnhinweise», die bei der Auswahl datenschutzfreundlicher Optionen angezeigt werden.[71]

---

67 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 62.

68 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 62.

69 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 63.

70 Siehe hierzu z.B. FORBRUKERRÅDET, S. 3 ff.

71 FORBRUKERRÅDET, S. 3 ff.

Weiter hat es der Verantwortliche zu tolerieren, wenn die betroffenen Personen Selbstdatenschutz-Tools (z.B. Browser mit Do-Not-Track-Einstellung, Werbeblocker) verwendet.[72]

d) Transparenz

Der Grundsatz der Transparenz (Art. 5 Abs. 1 Bst. a DSGVO) ist von fundamentaler Bedeutung für den Datenschutz: Nur wenn die betroffene Person die wesentlichen Umstände einer Datenverarbeitung kennt, kann sie ihre übrigen Rechte geltend machen.[73] Entsprechend wird der Transparenzgrundsatz durch verschiedene Normen konkretisiert, insbesondere durch die Informationspflichten des Verantwortlichen bei der Erhebung personenbezogener Daten in Art. 13 f. DSGVO. Bei der Umsetzung dieser Informationspflichten kann sich die Bank durch die Technik unterstützen lassen.

Beispiele:

Hat eine Bank festgelegt, dass der Kundenberater die Kundin im Rahmen einer Kontoeröffnung entsprechend zu informieren hat, kann das CRM-System so programmiert werden, dass es ihn jeweils auf diese Pflicht aufmerksam macht.

Für Online-Kontoeröffnungen können die Datenschutzhinweise gut sichtbar in die Website eingebunden werden.[74]

Bietet die Bank eine Mobile-Banking-App an, können die Datenschutzhinweise im App-Store platziert werden.

Zu beachten ist, dass die Information gemäss Art. 12 Abs. 1 DSGVO «in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache» zu erfolgen hat.

Um diesem Erfordernis nachzukommen und gleichzeitig die notwendige Detailliertheit gewährleisten zu können, bieten sich Multi-Layer-Strukturen an, d.h. Strukturen mit mehreren Ebenen. In der äussersten Ebene werden die wichtigsten Punkte zusammengefasst, und die inneren Ebenen enthalten weitergehende Informationen.[75]

Denkbar ist auch, dass der Kundin – beispielsweise in ihrem E-Banking-Bereich oder in der Mobile-Banking-App – ein Privacy Dashboard zur Verfügung gestellt wird, d.h. eine grafische Benutzeroberfläche, die ihr detailliert

---

72 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 63.

73 PÖTTERS, in: Gola, Art. 5 N. 11.

74 Vgl. BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 13.

75 Vgl. z.B. ENISA, Privacy by Design, S. 45; DIES., Mobile Apps, S. 12.

anzeigt, welche personenbezogenen Daten gesammelt werden, wie sie verwendet werden und wem sie zugänglich gemacht werden.[76]

Zur (ex-post-)[77]Transparenz tragen auch die saubere Dokumentation der Verarbeitungstätigkeiten sowie der erteilten Einwilligungen und Widerrufe und die Protokollierung («Logging») von Zugriffen und Änderungen bei.[78]

Weiter wird z.B. vorgeschlagen, die Datenschutzhinweise in maschinenlesbarem Format anzubieten, damit sie durch nutzereigene Tools ausgewertet werden können, oder standardisierte Bildsymbole i.S.v. Art. 12 Abs. 7 DSGVO zu verwenden.[79]

e) Zweckbindung

Der Grundsatz der Zweckbindung verlangt, dass personenbezogene Daten «für festgelegte, eindeutige und legitime Zwecke erhoben werden» und «nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden» (Art. 5 Abs. 1 Bst. b DSGVO).

Diesem Erfordernis kann namentlich dadurch Rechnung getragen werden, dass der Kreis der zugriffsberechtigten Personen auf diejenigen beschränkt wird, die diesen zur Erfüllung ihrer Aufgaben benötigen.[80] Wurden auf organisatorischer Ebene entsprechende Rollen- und Berechtigungskonzepte vorgesehen, kann diesen auf der technischen Ebene mittels entsprechenden Zugriffs- und Bearbeitungsberechtigungen Rechnung getragen werden.[81]

Ein wichtiges Stichwort, welches u.a. im Zusammenhang mit dem Zweckbindungsgrundsatz häufig genannt wird, lautet *Unlinkability* und bedeutet, dass personenbezogene Daten nicht mit weiteren personenbezogenen Daten, die allerdings zu einem anderen Zweck erhoben wurden, verknüpft und zu Persönlichkeitsprofilen verdichtet werden können.[82] Diesem Erfordernis kann dadurch Rechnung getragen werden, dass die Daten gleich bei ihrer Er-

---

76 Vgl. ENISA, Privacy by Design, S. 45.
77 Vgl. ENISA, Privacy by Design, S. 7.
78 Standard-Datenschutzmodell, S. 24; ENISA, Privacy by Design, S. 7.
79 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 64.
80 Z.B. MANTZ, in: Sydow (Hrsg.), Art. 25 N. 58.
81 ENISA, Privacy by Design, S. 7.
82 Vgl. ENISA, Privacy by Design, S. 7; vgl. auch Standard-Datenschutzmodell, S. 20.

hebung anhand ihres Zwecks getrennt und anschliessend separat weiterverarbeitet werden.[83] Dies kann beispielsweise durch die Verwendung verschiedener voneinander getrennter Datenbanken geschehen.[84] Alternativ können die Daten mit *Tags*, d.h. elektronischen Etiketts, versehen werden, die ihren jeweiligen Bearbeitungszweck kennzeichnen.[85] Unlinkability kann weiter durch die Schliessung von Schnittstellen und das Unterlassen von Backdoors[86] unterstützt werden.[87] Ferner tragen Verschlüsselung und frühestmögliche Anonymisierung zur Unlinkability bei.[88]

f) Datenminimierung und Speicherbegrenzung

Dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 Bst. c DSGVO) kann auf Stufe der Datenerhebung dadurch Rechnung getragen werden, dass weniger Attribute der betroffenen Personen erfasst werden.[89]

Auch eine Aggregation der vorhandenen Daten kann zur Datenminimierung beitragen.[90]

> Beispiel: Die Bank erfasst nur die durchschnittliche Verweildauer auf ihrer Website anstelle des vollständigen Datensatzes.

Eine weitere mögliche Massnahme zur Datenminimierung stellt die Begrenzung des Personenbezuges von Daten dar – beispielsweise durch Anonymisierung oder die erwähnten Massnahmen zur Herstellung von Unlinkability.[91]

Am Ende des Verarbeitungszyklus fordern sowohl der Grundsatz der Datenminimierung als auch der Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 Bst. e DSGVO), dass die Daten wieder gelöscht werden. Auf organisatori-

---

83 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 58; BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 13; ENISA, Privacy by Design, S. 20.

84 TAMÒ-LARRIEUX, S. 247.

85 MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 30; MANTZ, in: Sydow (Hrsg.), Art. 25 N. 58; KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 39, HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 16; BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), N. 13; HANSEN, in: Simitis et al. (Hrsg.), N. 65.

86 Backdoors sind alternative Zugangsmöglichkeiten zu einer Hard- oder Software, die es erlauben, Zugriffsschutz und Sicherheitsmechanismen zu umgehen.

87 Standard-Datenschutzmodell, S. 23 f.

88 ENISA, Privacy by Design, S. 7.

89 Standard-Datenschutzmodell, S. 22.

90 NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 16.

91 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 66.

scher Ebene muss die Bank dazu zunächst für alle Daten oder Datenkategorien eine Speicherfrist festlegen. Diese ergibt sich «aus dem Minimum dessen […], was für den Zweck der Verarbeitung erforderlich ist.»[92] Überdies muss die Bank entscheiden, was nach Ablauf dieser Fristen mit den Daten zu geschehen hat (z.B. Löschung, Anonymisierung, Prüfung einer Verlängerung der Speicherdauer gestützt auf Art. 5 Abs. 1 Bst. e DSGVO). [93]

g) Betroffenenrechte

Für die Umsetzung der Betroffenenrechte ist zentral, dass die Bank Zuständigkeiten und Prozesse definiert: Wer nimmt ein Auskunftsersuchen entgegen, prüft es, beantwortet es? Wie kann sichergestellt werden, dass die Auskunft fristgerecht erfolgt? Welche technischen Anforderungen muss das System aufweisen, damit effizient eruiert werden kann, welche Daten über eine Person verarbeitet werden und die ersuchten Daten der betroffenen Person zur Verfügung gestellt werden können? Wer soll – angesichts des Grundsatzes der Datenminimierung – über die Berechtigung verfügen, alle über die betroffene Person gespeicherten Daten zwecks Erteilung eines Auskunftsersuchens zusammenzuführen?

Auf der technischen Ebene können die bereits angesprochenen Privacy Dashboards von Nutzen sein.[94] Diese dienen nämlich nicht nur der Transparenz, sondern bilden eine Schnittstelle zwischen dem Verantwortlichen und der betroffenen Person und erlauben dieser, ihre Rechte nach der DSGVO (z.B. Berichtigungsrecht, Widerrufsrecht, etc.) auszuüben.[95] Ein solches Dashboard trägt überdies der in ErwG 78 erwähnten Forderung Rechnung, wonach der betroffenen Person ermöglicht werden soll, die Verarbeitung ihrer personenbezogenen Daten zu überwachen.

8. Abwägungskriterien

Wie erwähnt, kommt der Bank bei der Wahl der konkreten technischen und organisatorischen Massnahmen ein grosser Ermessensspielraum zu. Die

---

92 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 68.

93 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 68.

94 KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 41; HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 17.

95 Ausführlich z.B. RASCHKE/KÜPPER/DROZD/KIRRANE, S. 222. Ein Beispiel für ein solches (fiktives) Dashboard ist ersichtlich unter: <http://raschke.cc/GDPR-privacy-dashboard/>.

DSGVO gibt ihr allerdings gewisse Kriterien vor, die sie dabei zu berücksichtigen hat.

a) Stand der Technik

Zu berücksichtigen ist einerseits der «Stand der Technik». Dieser wird in der DSGVO nicht definiert. Vielfach wird zu seiner Konkretisierung das deutsche Recht herangezogen, wo der Begriff zwischen dem «Stand der Wissenschaft und Forschung» und den «allgemein anerkannten Regeln der Technik» verortet wird: Anders als beim «Stand der Wissenschaft und Forschung» müssten beim Stand der Technik die Verfahren effektiv realisierbar sein; anders als die «Allgemein anerkannten Regeln der Technik» verlange der Stand der Technik nicht nur, dass sich die Techniken in der Praxis bewährt hätten, sondern dass sie einem «fortgeschrittenen Stand der technischen Entwicklung entsprechen» würden.[96] Dabei darf nicht vergessen werden, dass es sich bei der DSGVO um europäisches Recht handelt. Zu Recht wird daher eine eigenständige Interpretation des Begriffs unter Berücksichtigung sämtlicher europäischer Rechtsordnungen gefordert.[97]

Zu beachten ist, dass der Stand der Technik dynamisch ist, weshalb sich der Verantwortliche laufend vergewissern muss, ob die getroffenen Massnahmen noch dem Stand der Technik entsprechen.[98] Hilfestellung zur Bestimmung des Stands der Technik bieten beispielsweise die ENISA-Berichte.[99]

b) Implementierungskosten

Ein weiteres Kriterium sind die Implementierungskosten. Deren genauer Umfang ist umstritten. Insbesondere bei der Frage, ob Betriebs- und Folgekosten erfasst sind, scheiden sich die Geister.[100] Auch die Frage, ob die indivi-

---

96 Z.B. MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 39 ff.; TeleTrust, Handreichung zum Stand der Technik, S. 11.

97 KNOPP, S. 665; HANSEN, in: Simitis et al. (Hrsg.), Art. 32 N. 22.

98 KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 46.

99 Z.B. ENISA, PETS; DIES., Privacy by Design.

100 Für eine weite Auslegung plädieren z.B. NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 24; HANSEN, in: Simitis et al. (Hrsg.), Art. 32 N. 26; HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 22. Enger ausgelegt wird der Begriff z.B. durch KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 47; MANTZ, in: Sydow (Hrsg.), Art. 25 N. 45, MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 41; BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 15.

duelle finanzielle Leistungsfähigkeit des Verantwortlichen jeweils berücksichtigt werden darf oder nicht, wird unterschiedlich beantwortet.[101] Jedenfalls muss auch die im Einzelfall gewählte kostengünstigste von mehreren Massnahmen wirksam sein.[102] Das «Ob» der Umsetzung wird durch die Implementierungskosten m.a.W. nicht beeinflusst, sondern nur das «Wie».[103]

c) Risiken

Schliesslich sind die Risiken für die Rechte und Freiheiten der betroffenen Person sowie die Eintrittswahrscheinlichkeit und Schwere dieser Risiken zu berücksichtigen. Anders als bei der Datenschutz-Folgeabschätzung nach Art. 35 DSGVO sind bei der Risikoabschätzung nach Art. 25 DSGVO nicht nur hohe, sondern alle Arten von Risiken relevant.[104] Die hohen Anforderungen an eine Datenschutz-Folge-Abschätzung sind aber nur bei hohen Risiken zu berücksichtigen.[105]

Als Risiken nennt ErwG 75 namentlich physische, materielle oder immaterielle Schäden wie z.B. Diskriminierung, Identitätsdiebstahl oder –betrug, finanzielle Verluste, Rufschädigung, den Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten und die unbefugte Aufhebung der Pseudonymisierung. Anlässlich der Risikoabschätzung hat der Verantwortliche auch die in Art. 25 DSGVO genannten weiteren Kriterien der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung zu berücksichtigen (vgl. ErwG 75, 76). So stellen gemäss ErwG 75 beispielsweise die Verarbeitung besonderer Kategorien personenbezogener Daten, die Verarbeitung grosser Datenmengen sowie die Bewertung persönlicher Aspekte (wie z.B. Arbeitsleistung, wirtschaftliche Lage, Aufenthaltsort, Vorlieben und Interessen) Risiken dar.

---

101 Befürwortend z.B. KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 47; ablehnend MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 42. Offen gelassen von MANTZ, in: Sydow (Hrsg.), Art. 25 N. 46.

102 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 46; HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 22.

103 MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 42.

104 HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 20.

105 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 21.

Obwohl der Europäische Datenschutzausschuss bisher noch keine entsprechenden Leitlinien, Empfehlungen und bewährten Verfahren bereitgestellt hat (vgl. Art. 70 Abs. 1 Bst. h DSGVO),[106] existieren verschiedene Modelle und Tools, die den Verantwortlichen bei der Risikoanalyse unterstützen. Zu nennen sind etwa das Standard-Datenschutzmodell, das von der ENISA ausdrücklich erwähnte[107] LINDDUN-Modell[108] und das Gratis-PIA-Tool der französischen Commission Nationale de l'Informatique et des Libertés (CNIL).[109]

VI. Privacy by Default nach Art. 25 Abs. 2 DSGVO

In diesem Abschnitt soll die Privacy by Default, d.h. die Pflicht zu datenschutzfreundlichen Voreinstellungen, näher betrachtet werden.

1. Wortlaut

Der Wortlaut von Art. 25 Abs. 2 DSGVO lautet folgendermassen:

> «Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden».

2. Zweck

Studien zeigen, dass die meisten Nutzerinnen und Nutzer von Internetdiensten jeweils die Voreinstellungen übernehmen.[110] Dies wird von verschiedenen

---

106 Die Art. 29-Gruppe hat allerdings ein entsprechendes Working Paper (WP 248) vorgelegt.

107 ENISA, Privacy by Design, S. 13.

108 Einzelheiten unter: <https://linddun.org/>.

109 Download unter: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>.

110 Siehe z.B. betreffend soziale Netzwerke KUCZERAWY/COUDERT, S. 233-234; AUSLOOS/LIEVENS/KINT/DUMORTIER, S. 15 f.

Anbietern ausgenutzt, indem sie die Voreinstellungen so ausgestalten, dass möglichst viele Daten gesammelt und verarbeitet werden.[111]

> Beispiel: Bei der Google-Suche wird standardmässig personalisierte Werbung gezeigt.

Mit Art. 25 Abs. 2 DSGVO bezweckt der Gesetzgeber, dass die Verarbeitung auf das notwendige Mindestmass beschränkt wird, sofern die betroffene Person die Voreinstellungen nicht ändert – dass ihr also ihre Untätigkeit oder Unwissenheit nicht zum Nachteil gereicht.[112]

3. Anwendungsbereich

In persönlicher Hinsicht erfasst auch Art. 25 Abs. 2 DSGVO nur den Verantwortlichen unmittelbar – obwohl es häufig die Hersteller sind, die über die Voreinstellungen ihrer Produkte entscheiden.[113] In sachlicher Hinsicht sind datenverarbeitende Systeme betroffen, die Voreinstellungen enthalten. Voreinstellungen sind initiale Konfigurationen, die geändert werden können. Umstritten scheint zurzeit noch, ob Art. 25 Abs. 2 DSGVO nur anwendbar ist, wenn diese Änderungsmöglichkeiten nutzerseitig bestehen[114] oder ob auch Voreinstellungen erfasst sind, die allein der Verantwortliche ändern kann und die für die betroffene Person nicht sichtbar sind.[115] Ob der Verantwortliche Voreinstellungen vorsehen will oder ausschliesslich fest eingebaute Funktionalitäten ohne Konfigurationsmöglichkeit, liegt in seinem Ermessen.[116] Letztlich hängt der sachliche Anwendungsbereich von Privacy by Default also von einem Gestaltungsentscheid des Verantwortlichen ab.[117]

Konkret können unter Art. 25 Abs. 2 DSGVO neben sozialen Netzwerken z.B. Webseiten, Apps, Betriebssysteme und die Steuerungssoftware von Wearables oder Drohnen fallen.[118] Banken dürften vor allem im Bereich ihrer Online-Banking-Portale und ihrer Mobile-Banking-Apps betroffen sein.

---

111 Siehe hierzu z.B. FORBRUKERRÅDET, S. 3 ff.
112 Vgl. MANTZ, in: Sydow (Hrsg.), Art. 25 N. 63.
113 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 65, m.w.H.
114 So z.B. MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 46c.
115 So HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 41 ff.
116 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 24; ENISA; Privacy by Default, S. 15.
117 HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 24.
118 KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 58.

4. Verhältnis zu Art. 25 Abs. 1 DSGVO

Art. 25 Abs. 2 DSGVO und Art. 25 Abs. 1 DSGVO stehen in einem Verhältnis der Spezialität: Privacy by Default stellt einen besonderen Anwendungsfall von Privacy by Design dar.[119]

5. Erforderlichkeit

Die erforderlichen Verarbeitungen beziehen sich immer auf den konkreten Verarbeitungszweck (Art. 25 Abs. 2 DSGVO). Und diesen bestimmt der Verantwortliche weitgehend frei – der Zweck muss lediglich legitim sein (Art. 5 Abs. 1 Bst. b DSGVO).[120] Legitim ist ein Verarbeitungszweck, wenn er im Einklang mit der Rechtsordnung steht.[121] Sofern es der Verarbeitungszweck erfordert, sind daher auch Voreinstellungen denkbar, die eine besonders umfassende bzw. intensive Datenverarbeitung vorsehen.[122] Zu beachten ist aber, dass Verarbeitungszweck und -modalitäten hinreichend transparent sein müssen.[123]

Die Erforderlichkeit bestimmt sich einerseits hinsichtlich der Menge der erhobenen Daten.

> Beispiel: Eine App, die das Ziel hat, der Nutzerin den nächstgelegenen Geldautomaten oder die nächstgelegene Bankfiliale anzuzeigen, benötigt zwar den Zugriff auf den Standort des Kunden, nicht aber den Zugriff auf sein Adressbuch.

Weiter bestimmt sich die Erforderlichkeit nach dem Umfang der Verarbeitung (englisch: «extent of processing»). Damit ist die Verarbeitungstiefe und –intensität gemeint – beispielsweise, ob die erhobenen Daten einmal oder mehrmals analysiert werden, ob sie an Dritte weitergegeben werden oder ob sie zu einem Persönlichkeitsprofil verdichtet werden.[124]

---

119 KEBER/KEPPELER, in: Schwartmann et al. (Hrsg.), Art. 25 N. 58 Fn 137; NOLTE/WERKMEISTER, in: Gola (Hrsg.), Art. 25 N. 9.

120 MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 45b; BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 18.

121 HEBERLEIN, in: Ehmann/Selmayr (Hrsg.), Art. 5 N. 15.

122 BAUMGARTNER, in: Ehmann/Selmayr, Art. 25 N. 18.

123 Vgl. BAUMGARTNER, in: Ehmann/Selmayr, Art. 25 N. 18.

124 MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 50; HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 27; HANSEN, in: Simitis et al. (Hrsg.), Art. 25 N. 49; ENISA, Privacy by Default, S. 17.

Auch die Speicherfrist muss erforderlich sein. Der Verantwortliche muss die minimale Speicherfrist im Hinblick auf den konkreten Zweck festlegen. Dies kann auch bedeuten, dass gar keine Speicherung stattfindet.[125]

> Beispielsweise erfordert der Zweck einer App, dem Kunden den nächstgelegenen Geldautomaten anzuzeigen, wohl keine über die konkrete Anfrage im Einzelfall hinausgehende Speicherung seiner Standortdaten.

Schliesslich bestimmt sich die Erforderlichkeit auch nach der Zugänglichkeit personenbezogener Daten. Hier ist insbesondere zu beachten, dass personenbezogene Daten nicht ohne Eingreifen der betroffenen Person einer unbestimmten Zahl natürlicher Personen zugänglich gemacht werden dürfen.

VII. Durchsetzung von Privacy by Design und Privacy by Default

In diesem Kapitel soll gezeigt werden, wie Privacy by Design und Privacy by Default nach DSGVO, DSG und E-DSG – soweit sie nach diesen Erlassen gelten – durchgesetzt werden.

1. DSGVO

a) Rechenschaftspflichten

Die DSGVO enthält an zahlreichen Stellen Rechenschaftspflichten. Am prominentesten sind wohl Art. 5 Abs. 2 DSGVO betreffend die Einhaltung der Datenschutzgrundsätze und Art. 24 Abs. 1 DSGVO betreffend die Einhaltung der Anforderungen der DSGVO. Art. 25 Abs. 3 DSGVO und ErwG 78 sehen vor, dass auch die Einhaltung von Privacy by Design und Privacy by Default nachzuweisen sind.[126]

Diese Rechenschaftspflichten stellen ein wesentliches Durchsetzungselement von Privacy by Design und Privacy by Default dar – zwingen sie doch den Verantwortlichen, sich vorgängig Gedanken über seine Datenverarbeitungen zu machen und diese zu dokumentieren. Sie tragen daher dem proaktiven Charakter von Privacy by Design Rechnung.[127]

---

125 ENISA; Privacy by Default, S. 17.

126 Zum Verhältnis der einzelnen Rechenschaftspflichten zueinander siehe VEIL, passim.

127 Ähnlich MANTZ, in: Sydow (Hrsg.), Art. 25 N. 70.

b) Befugnisse der Aufsichtsbehörden

Ein weiteres wichtiges Durchsetzungselement für Privacy by Design und Privacy by Default sind die weitreichenden Untersuchungs- und Abhilfebefugnisse der Aufsichtsbehörden (vgl. Art. 58 DSGVO). Diese können eine Verarbeitung insbesondere verbieten (vgl. Art. 58 Abs. 2 Bst. f) oder zumindest die Anweisung erteilen, Verarbeitungsvorgänge in Einklang mit der DSGVO zu bringen (vgl. Art. 58 Abs. 2 Bst. d). Die Nichtbefolgung einer Anweisung der Aufsichtsbehörde ist mit Busse bedroht (vgl. Art. 83 Abs. 5 Bst. e; Art. 83 Abs. 6 DSGVO).

c) Schadenersatz

Gemäss Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstosses gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz. Schwer vorstellbar ist, dass die blosse Verletzung von Privacy by Design oder Privacy by Default bereits zu einem Schaden führen könnte.[128] Allerdings könnte eine Verletzung von Art. 25 DSGVO im Rahmen eines Schadenersatzprozesses wegen einer anderen DSGVO-Verletzung zum Misslingen des Exkulpationsbeweises nach Art. 82 Abs. 3 DSGVO führen.[129]

d) Sanktionen

Art. 83 Abs. 4 Bst. a DSGVO bedroht die Verletzung von Art. 25 DSGVO mit Geldbusse bis zu EUR 10 Mio. oder, im Falle eines Unternehmens, bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres, je nachdem, welcher der Beträge höher ist. Bei einem Verstoss gegen Art. 25 DSGVO dürften allerdings regelmässig weitere Bestimmungen wie insbesondere die Datenverarbeitungsgrundsätze nach Art. 5 Abs. 1 DSGVO verletzt sein werden,[130] was mit dem doppelten Strafrahmen bedroht ist (vgl. Art. 83 Abs. 5 Bst. a DSGVO). Überdies sind die technischen und organisatorischen Massnahmen, die der Verantwortliche in Umsetzung von Art. 25 DSGVO getroffen hat, allgemein bei der Verhängung und Bemessung von

---

128 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 77; HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 31.

129 MANTZ, in: Sydow (Hrsg.), Art. 25 N. 77; HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 31.

130 BAUMGARTNER, in: Ehmann/Selmayr (Hrsg.), Art. 25 N. 24.

Geldbussen aufgrund von Verletzungen der DSGVO zu berücksichtigen (Art. 83 Abs. 2 Bst. d DSGVO).

Aufgrund der zahlreichen unbestimmten Rechtsbegriffe und Abwägungskriterien dürfte eine Verletzung von Art. 25 DSGVO schwierig nachzuweisen sein.[131] Allfällige Auseinandersetzungen dürften sich daher um vorgängig ergangene konkretisierende Anordnungen der Aufsichtsbehörden drehen.[132]

2. DSG

a) Keine Rechenschaftspflicht

Im Unterschied zur DSGVO ist im DSG keine Rechenschaftspflicht vorgesehen.

b) Persönlichkeitsschutz

Gemäss Art. 12 Abs. 1 DSG darf, wer Personendaten bearbeitet, die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzen. Liegt eine Persönlichkeitsverletzung vor, ohne dass dafür ein Rechtfertigungsgrund besteht, ist sie widerrechtlich (vgl. Art. 13 Abs. 1 DSG). Der betroffenen Person stehen in einem solchen Fall gemäss Art. 15 DSG die Rechtsansprüche nach Art. 28, 28a und 28l ZGB zu.

aa) Verletzung von Privacy by Design

Privacy by Design wurde im DSG nicht vollständig, sondern nur im Rahmen von Art. 7 DSG verwirklicht (siehe oben). Dessen Verletzung stellt gemäss Art. 12 Abs. 2 Bst. a DSG eine Persönlichkeitsverletzung dar. Eine solche liegt bereits vor, wenn Daten bearbeitet werden, ohne dass entsprechende technische und organisatorische Massnahmen getroffen wurden. Ein konkretes Ereignis wie z.B. ein Datenverlust ist nicht vorausgesetzt.[133]

Soweit Privacy by Design im DSG verwirklicht wurde, stellt seine Verletzung folglich eine Persönlichkeitsverletzung dar.

131 HARTUNG, in: Kühling/Buchner (Hrsg.), Art. 25 N. 31.
132 MARTINI, in: Paal/Pauly (Hrsg.), Art. 25 N. 5.
133 BSK-DSG-RAMPINI, Art. 12 N. 9.

bb) Verletzung von Privacy by Default

Wie erwähnt, lässt sich das Gebot, datenschutzfreundliche Voreinstellungen vorzusehen, aus dem Verhältnismässigkeitsprinzip ableiten. Die Verletzung des Verhältnismässigkeitsprinzips stellt eine Persönlichkeitsverletzung dar (Art. 12 Abs. 2 Bst. a i.V.m. 4 Abs. 2 DSG). Sobald also – beispielsweise aufgrund unangemessener Voreinstellungen – unverhältnismässige Datenbearbeitungen stattfinden, liegt eine Persönlichkeitsverletzung vor.

c) Befugnisse des EDÖB

Im Privatbereich klärt der EDÖB gemäss Art. 29 Abs. 1 DSG von sich aus Meldung Dritter hin den Sachverhalt ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzten (Systemfehler), wenn Datensammlungen registriert werden müssen oder wenn eine Informationspflicht nach Art. 6 Abs. 3 DSG besteht. Er kann aufgrund seiner Abklärungen Empfehlungen aussprechen (Art. 29 Abs. 3 DSG) und an das Bundesverwaltungsgericht gelangen, sofern eine solche Empfehlung nicht befolgt oder abgelehnt wird (Art. 29 Abs. 4 DSG).

d) Keine Sanktionen

Sanktionen sind im DSG nur bei der Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten (Art. 34 DSG) sowie der beruflichen Schweigepflicht (Art. 35 DSG) vorgesehen.

3. E-DSG

a) Keine Rechenschaftspflicht

Die Rechenschaftspflicht, wie sie die DSGVO kennt, wurde nicht in das E-DSG übernommen. Auch ins Verzeichnis der Bearbeitungstätigkeiten müssen nur die Massnahmen zur Gewährleistung der Datensicherheit nach Art. 7 E-DSG aufgenommen werden, nicht aber diejenigen zur Umsetzung von Privacy by Design und Privacy by Default gemäss Art. 6 E-DSG (vgl. Art. 11 Abs. 2 Bst. f). Dies stellt zwar eine Erleichterung für den Verantwortlichen dar, birgt aber die Gefahr, dass Privacy by Design und Privacy by Default bei der Planung datenbearbeitender Systeme vergessen werden.

b) Persönlichkeitsschutz

Im E-DSG existiert keine gesetzliche Fiktion, wonach die Verletzung von Art. 6 E-DSG, der Rechtsgrundlage von Privacy by Design und Privacy by Default, eine Persönlichkeitsverletzung darstellen würde. Eine solche wird nur für den Teilgehalt der Datensicherheit, der in Art. 7 E-DSG geregelt ist, fingiert (vgl. Art. 26 Abs. 2 Bst. a E-DSG).

Denkbar wäre allerdings, dass eine Persönlichkeitsverletzung damit begründet würde, dass der Rechtmässigkeitsgrundsatz verletzt sei, weil eine datenschutzrechtliche Norm verletzt werde. Umstritten ist jedoch, ob sich diese Norm auch im DSG selber befinden darf oder nicht.[134]

Die Diskussion dürfte von geringer Relevanz sein: Ist Privacy by Design verletzt, dürften in den überwiegenden Fällen auch Datenbearbeitungsgrundsätze verletzt sein, was eine Persönlichkeitsverletzung darstellen würde (vgl. Art. 26 Abs. 2 Bst. a E-DSG). Bei einer Verletzung von Privacy by Default wäre, wie erwähnt, gleichzeitig der Verhältnismässigkeitsgrundsatz verletzt.

c) Befugnisse des EDÖB und Sanktionen

Die Befugnisse des EDÖB werden im E-DSG erweitert: Neu kann er auch verfügen. Insbesondere kann er ein Bundesorgan oder eine private Person anweisen, die Vorkehren nach Art. 6 E-DSG bezüglich Privacy by Design und Privacy by Default sowie nach 7 E-DSG betreffend Datensicherheit zu treffen. Die Missachtung von Verfügungen des EDÖB werden mit Busse bis zu CHF 250'000 bestraft (Art. 57 E-DSG). Nach E-DSG kann also die Verletzung von Privacy by Design und Privacy by Default dann eine Sanktion nach sich ziehen, wenn der EDÖB das Treffen entsprechender Massnahmen angeordnet hat und einer solchen Anordnung nicht Folge geleistet wurde. Ebenfalls mit Busse bis CHF 250'000 wird die Nichteinhaltung der Mindestanforderungen an die Datensicherheit bedroht (Art. 55 Bst. c E-DSG).

VIII. Fazit

Privacy by Design ist kein vollständig neues Konzept, sondern ist bereits im geltenden DSG teilweise verwirklicht. Für Schweizer Banken ist hier neben

---

[134] Befürwortend SHK-BAERISWYL, Art. 4 N. 5; EPINEY, in: Belser/Epiney/Waldmann, S. 520; BSK-DSG-MAURER-LAMBROU/STEINER, Art. 4 N. 6; ablehnend HK-ROSENTHAL, Art. 4 N. 7; MEIER, N. 640.

dem DSG und der VDSG insbesondere der Anhang 3 des FINMA-Rundschreibens 08/21 relevant. Privacy by Default lässt sich bereits im geltenden Recht aus dem Verhältnismässigkeitsgrundsatz ableiten.

Neu ist nach der DSGVO und dem E-DSG, dass *sämtlichen* darin enthaltenen Anforderungen mittels technischer und organisatorischer Massnahmen Rechnung getragen werden muss. Schweizer Banken haben hier zu beachten, dass die DSGVO nicht nur für Verantwortliche mit Sitz in der EU gilt, sondern einen extraterritorialen Anwendungsbereich aufweist. Eine Abklärung, ob das eigene Institut von diesem erfasst ist, ist daher zentral. Diejenigen Schweizer Banken, die nicht in den Anwendungsbereich der DSGVO fallen, werden Privacy by Design und Privacy by Default wahrscheinlich künftig umsetzen müssen, da beide Institute im E-DSG enthalten sind.

Bezüglich der konkreten Umsetzung der technischen und organisatorischen Massnahmen enthalten sowohl die DSGVO als auch das E-DSG nur wenige Hinweise. Anhaltspunkte bieten Publikationen von Wissenschaftlerinnen und Behörden. Dabei existiert wohl keine one-size-fits-all-Lösung. Vielmehr hängt die Frage, welche Massnahmen eine Bank zu treffen hat, von den konkreten Umständen des Einzelfalls ab.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 30. April 2019.

AUSLOOS JEF/KINDT ELS/LIEVENS EVA/VALCKE PEGGY/DUMORTIER JOS, Guidelines for Privacy-Friendly Default Settings, ICRI Research Paper No. 12/2013, abrufbar unter: <https://ssrn.com/abstract=2220454 or http://dx.doi.org/10.2139/ssrn.2220454>.

BAERISWYL BRUNO/PÄRLI KURT, Datenschutzgesetz (DSG), SHK – Stämpflis Handkommentar, Bern 2015 (zit. SHK-BEARBEITER, Art. […] N. […].

BAUMGARTNER ULRICH, Kommentierung zu Art. 25 DSGVO, in: Eugen Ehmann/Martin Selmayr (Hrsg.), Besch'sche Kurz-Kommentare, DS-GVO, Datenschutz-Grundverordnung, Kommentar, 2. Auflage, München 2018.

BELSER EVA MARIA/EPINEY ASTRID/WALDMANN BERNHARD, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011.

BORKING JOHN, Einsatz datenschutzfreundlicher Technologien in der Praxis, DuD, Datenschutz und Datensicherheit 22 (1998), S. 636-640.

BYGRAVE LEE A., Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, in: Oslo Law Review, Volume 4, No. 2-2017, S. 105-120.

EHMANN EUGEN/SELMAYR MARTIN (Hrsg.), Besch'sche Kurz-Kommentare, DS-GVO, Datenschutz-Grundverordnung, Kommentar, 2. Auflage, München 2018.

FREUD SIGMUND, Eine Schwierigkeit der Psychoanalyse, in: IMAGO, Zeitschrift für Anwendung der Psychoanalyse auf die Geisteswissenschaften, Bd. V, 1917, S. 1-7.

GOLA PETER (Hrsg.), Datenschutz-Grundverordnung, VO (EU) 2016/679, 2. Auflage, München 2018.

KEBER TOBIAS O./KEPPELER LUTZ MARTIN, Kommentierung zu Art. 25 DSGVO, in: Rolf Schwartmann/Andreas Jaspers/Gregor Thüsing/Dieter Kugelmann (Hrsg.), DS-GVO/BDSG, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Heidelberg 2018.

KÜHLING JÜRGEN/BUCHNER BENEDIKT (Hrsg.), Datenschutz-Grundverordnung/BDSG, 2. Auflage, München 2018.

KUCZERAWY ALEKSANDRA/COUDERT FANNY, Privacy Settings in Social Networking Sites: Is It Fair?, in: Simone Fischer-Hübner/Penny Duquenoy/Marit Hansen/Ronald Leenes/Ge Zhang (Hrsg.), Privacy and Identity Management for Life, Heidelberg/Dordrecht/London/New York 2011, S. 231-241.

HANSEN MARIT, Kommentierung zu Art. 25 DSGVO, in: Spiros Simitis/Gerrit Hornung/Indra Spiecker genannt Döhmann (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019.

HARTUNG JÜRGEN, Kommentierung zu Art. 25 DSGVO, in: Jürgen Kühling/Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, 2. Auflage, München 2018.

HEBERLEIN HORST, Kommentierung zu Art. 5 DSGVO, in: Eugen Ehmann/Martin Selmayr (Hrsg.), Besch'sche Kurz-Kommentare, DS-GVO, Datenschutz-Grundverordnung, Kommentar, 2. Auflage, München 2018.

HÖDL ELISABETH, Privacy by Design, in: Jusletter IT vom 6. Juni 2012.

HÖTZENDORFER WALTER, Privacy by Design and by Default, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, in: Rainer Knyrim (Hrsg.), Datenschutz-Grundverordnung, Praxishandbuch, Wien 2016, S. 137-151.

KNOPP MICHAEL, Stand der Technik, Ein alter Hut oder eine neue Größe?, DuD, Datenschutz und Datensicherheit, 11/2017, 663-666.

LESSIG LAWRENCE, Code, version 2.0., New York 2006.

MANTZ RETO, Kommentierung zu Art. 25 DSGVO, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. Auflage, Baden-Baden 2018.

MARTINI MARIO, Kommentierung zu Art. 25 DSGVO, in: Boris P. Paal/Daniel A. Pauly (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Auflage, München 2018.

MAURER-LAMBROU, URS/BLECHTA, GABOR P. (Hrsg.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsvesetz, 3. Auflage, Basel 2014 (zit. BSK-DSG-BEARBEITER, Art. […] N. […]).

MEIER PHILIPPE, Protection des données, fondements, principes généraux et droit privé, Bern 2011.

MILLER ARHUR R., Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, in: Michigan Law Review, Vol. 67, No. 6 (Apr., 1969), S. 1089-1246.

NOLTE NORBERT/WERKMEISTER CHRISTOPH, Kommentierung zu Art. 25 DSGVO, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung, VO (EU) 2016/679, 2. Auflage, München 2018.

PAAL BORIS P./PAULY DANIEL A. (Hrsg.), Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2. Auflage, München 2018.

PFAFFINGER MONIKA, DSGVO: Extraterritoriale Wirkung und konkrete Pflichten für die Banken, zur Publikation vorgesehen.

POHLE JÖRG, Das Scheitern von Datenschutz by Design: Eine kurze Geschichte des Versagens, in: FIfF-Kommunikation 2/2015, S. 41-44.

PÖTTERS STEPHAN, Kommentierung zu Art. 5 DSGVO, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung, VO (EU) 2016/679, 2. Auflage, München 2018.

RASCHKE PHILIP/KÜPPER AXEL/DROZD OLHA/KIRRANE SABRINA, Designing a GDPR-Compliant and Usable Privacy Dashboard, in: Marit Hansen/Eleni Kosta/Igor Nai-Fovino/Simone Fischer-Hübner (Hrsg.), Privacy and Identity Management, The Smart Revolution, Ispra 2018, S. 221-236.

ROSENTHAL DAVID, Der Entwurf für ein neues Datenschutzgesetz, Was uns erwartet und was noch zu korrigieren ist, in: Jusletter 27. November 2017.

ROSENTHAL DAVID/JÖHRI YVONNE, Handkommentar zum Datenschutzgesetz sowie

weiteren, ausgewählten Bestimmungen, Zürich/Basel/Genf 2008 (zit. HK-BEARBEITER, Art. […] N. […]).

SCHWARTMANN ROLF/JASPERS ANDREAS/THÜSING GREGOR/KUGELMANN DIETER (Hrsg.), DS-GVO/BDSG, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Heidelberg 2018.

SIMITIS SPIROS/HORNUNG GERRIT/SPIECKER GENANNT DÖHMANN INDRA (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019.

STAFFELBACH OLIVER/KELLER CLAUDIA (Hrsg.), Social Media und Recht für Unternehmen, Zürich/Basel/Genf 2015.

SYDOW GERNOT (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. Auflage, Baden-Baden 2018.

TALL ISMAËL, Le renforcement de la loi fédérale sur la protection des données: le cas de la protection de la vie privée dès la conception (privacy by design), Lausanne 2015.

TAMÒ-LARRIEUX AURELIA, Designing for Privacy and Its Legal Framework, Data Protection by Design and Default for the Internet of Things, Zürich 2018.

VEIL WINFRIED, Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, ZD 2018, S. 9-16.

WEISER MARK, The Computer for the 21st Century, Scientific American, September 1991, S. 94-104.

Materialien

32ND INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS JERUSALEM, Israel, 27-29 October, 2010, Resolution on Privacy by Design, abrufbar unter: <https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf>.

95. KONFERENZ DER UNABHÄNGIGEN DATENSCHUTZBEHÖRDEN DES BUNDES UND DER LÄNDER, Das Standard-Datenschutzmodell, Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.1.1 –Erprobungsfassung, Düsseldorf 2018, abrufbar unter: <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf>.

ARTIKEL-29-GRUPPE, WP 223, Opinion 8/2014 the on Recent Developments on the Internet of Things vom 16. September 2014.

WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, abrufbar unter: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>.

CAVOUKIAN ANN, Privacy by Design, The 7 Foundational Principles, abrufbar unter: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

DATATILSYNET, Guide, Software development with Data Protection by Design and by Default, abrufbar unter: <https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/>.

EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes, August 2015.

Entwurf des Bundesgesetzes über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 7193-7276.

EUROPEAN DATA PROTECTION BOARD (EDPB), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation, Adopted on 16 November 2018.

EUROPEAN DATA PROTECTION SUPERVISOR, Opinion 5/2018, Preliminary Opinion on privacy by design, 31. Mai 2018, abrufbar unter: <https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en>.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA); Privacy and Data Protection by Design – from policy to engineering, December 2014, abrufbar unter: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> (zit. ENISA, Privacy by Design);

Privacy by design in big data, An overview of privacy enhancing technologies in the era of big data analytics, December 2015, abrufbar unter: <https://www.enisa.europa.eu/publications/big-data-protection> (zit. ENISA; Big Data);

Privacy and data protection in mobile applications, A study on the app development ecosystem and the technical implementation of GDPR, November 2017, abrufbar unter: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications> (zit. ENISA, Mobile Apps);

A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment, December 2017, abrufbar unter: <https://www.enisa.europa.eu/publications/pets-maturity-tool> (zit. ENISA, PETs);

Recommendations on shaping technology according to GDPR provisions, Exploring the notion of data protection by Default, December 2018, abrufbar unter: <https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2> (zit. ENISA, Privacy by Default).

FINMA, Rundschreiben 2008/21, Operationelle Risiken – Banken, Eigenmittelanforderungen und qualitative Anforderungen für operationelle Risiken bei Banken.

FORBRUKERRÅDET, Deceived by Design, How tech companies use dark patterns to discourage us from exercising our rights to privacy, 2018, abrufbar unter: <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>.

GSMA, Privacy Design Guidelines for Mobile Application Development, abrufbar unter: <https://www.gsma.com/publicpolicy/resources/privacy-design-guidelines-mobile-application-development>.

Information and Privacy Commissioner, Ontario Canaca/Registratiekamer, The Netherlands, Privacy-Enhancing Technologies: The Path to Anonymity, August 1995, abrufbar unter: <http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf>.

TELETRUST, BUNDESVERBAND IT-SICHERHEIT E.V., IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik" technischer und organisatorischer Maßnahmen, 2019, abrufbar unter: <https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-04_TeleTrusT_Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DEU.pdf>.

Lieferung von Bankmitarbeiterdaten an ausländische Steuerbehörden – wenn Amtshilfe ausartet

Andrea Opel, Luzern*

* Prof. Dr. iur., Ordinaria für Steuerrecht an der Universität Luzern, Konsulentin bei Bär & Karrer, Zürich. Der Beitrag basiert auf einem anlässlich der Schweizer Bankrechtstagung vom 8. März 2019 gehaltenen Referat.

I. Einleitung: Zwei Fragen

Der vorliegende Beitrag befasst sich mit der rechtlichen Stellung von Bankmitarbeitern im Verfahren der internationalen Steueramtshilfe. Im Fokus stehen zwei Fragen:

1. Sind Namen von Bankangestellten, die in amtshilfeweise zu übermittelnden Unterlagen erscheinen, von der Eidgenössischen Steuerverwaltung (ESTV) zu schwärzen?
2. Müssen vom Informationsaustausch betroffene Bankmitarbeiter seitens der ESTV von Amtes wegen informiert werden, wenn ihre Namen in den Unterlagen ersichtlich sind?

Vorwegzunehmen ist, dass die ESTV beide Fragen grundsätzlich verneint – und dies auch praktisch so handhabt. Nachfolgend gilt es, die Haltung der ESTV anhand der einschlägigen Rechtsgrundlagen und der höchstrichterlichen Rechtsprechung kritisch zu hinterfragen.

II. Amtshilfe nach OECD-Standard

1. Rechtsgrundlagen der Amtshilfe auf Ersuchen

Untersucht wird vorliegend nur die ersuchensabhängige Amtshilfe, also weder der spontane noch der automatische Informationsaustausch. Die Rechtsgrundlagen für Amtshilfe auf Ersuchen finden sich üblicherweise in den bilateral abgeschlossenen Doppelbesteuerungsabkommen (DBA).[1] Diese werden

[1] Mit einzelnen Staaten sind sog. Steuerinformationsabkommen (SIA) abgeschlossen worden. Im Unterschied zu den DBA haben diese einzig den Informationsaustausch zum Gegenstand. Auf die SIA wird nachfolgend nicht weiter eingegangen.

seitens der Schweiz nach Vorbild des OECD-Musterabkommens (OECD-MA)[2] aufgesetzt, das die Amtshilfe in Art. 26 regelt. Zudem ist am 1. Januar 2017 das multilaterale Übereinkommen über die gegenseitige Amtshilfe in Steuersachen (ÜAS)[3] in Kraft getreten, welches in Art. 5 ebenfalls eine Anspruchsgrundlage für Amtshilfe auf Ersuchen bereit hält. Sodann wurde mit den EU-Staaten ein spezielles AIA-Abkommen[4] abgeschlossen, gestützt auf dessen Art. 5 auch Ersuchensauskünfte verlangt werden können. Die verschiedenen Anspruchsgrundlagen für Amtshilfe auf Ersuchen können sich überschneiden, wobei diesfalls grundsätzlich das sog. Günstigkeitsprinzip gilt: Der ersuchende Staat kann dasjenige Abkommen anrufen, das ihm am vorteilhaftesten erscheint.[5] Im Verhältnis zu EU-Staaten stehen somit regelmässig drei Anspruchsgrundlagen zur Auswahl: das DBA, das ÜAS und das AIA-Abkommen mit der EU. Klarzustellen ist, dass die formellen und materiellen Voraussetzungen des Informationsaustauschs rechtsgrundlagenübergreifend grundsätzlich übereinstimmen, d.h. dem OECD-Amtshilfestandard entsprechen.[6]

---

2 OECD-Musterabkommen ab 1963 (letzte Aufdatierung 2017) zur Vermeidung der Doppelbesteuerung von Einkommen und Vermögen (= OECD Model Tax Convention on Income and on Capital, zu finden unter: <http://www.oecd.org/ctp/treaties/model-tax-convention-on-income-and-on-capital-condensed-version-20745419.htm>). Das OECD-MA wird von einem Musterkommentar (OECD-MK) begleitet.

3 Übereinkommen über die gegenseitige Amtshilfe in Steuersachen vom 25. Januar 1988 (SR 0.652.1). Vgl. zum Geltungsbereich die Internetseite des Eidgenössischen Departements für auswärtige Angelegenheiten (<www.eda.admin.ch/vertraege>).

4 Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Union über den automatischen Informationsaustausch über Finanzkonten zur Förderung der Steuerehrlichkeit bei internationalen Sachverhalten vom 26. Oktober 2004 (AIA-Abkommen mit der EU; SR 0.641.926.81). Dabei handelt es sich um das per 1. Januar 2017 revidierte vormalige Zinsbesteuerungsabkommen.

5 BEHNISCH, in: Aktuelle Fragen, S. 145; OPEL, ASA 86 (2017/2018), S. 260 f. Vgl. auch Botschaft ÜAS, BBl 2015 5596. Unterschiede bestehen insbesondere in Bezug auf den sachlichen (und u.U. zeitlichen) Anwendungsbereich: Während die Anwendung des ÜAS aus schweizerischer Warte auf den direktsteuerlichen Bereich beschränkt ist (vgl. Vorbehalt der Schweiz gestützt auf Art. 30 Abs. 1 lit. a ÜAS), fallen in den Geltungsbereich des AIA-Abkommens mit der EU Steuern jeder Art und Bezeichnung. Eine Beschränkung auf den Bereich der direkten Steuern erfolgt damit gerade nicht (vgl. Botschaft AIA-Abkommen-EU, BBl 2015 9209).

6 Vgl. nur die gemeinsame Erklärung der Vertragsparteien zu Art. 5 AIA-Abkommen mit der EU, wonach der OECD-MK zu Art. 26 zur Auslegung heranzuziehen ist.

Die Ausführungsbestimmungen für die ersuchensabhängige Amtshilfe sind landesintern im Steueramtshilfegesetz (StAhiG)[7] und in der Steueramtshilfeverordnung (StAhiV)[8] geregelt.

2. Der OECD-Amtshilfestandard[9]

Art. 26 OECD-MA lautet wie folgt:

> [1] Die zuständigen Behörden der Vertragsstaaten tauschen die Informationen aus, die zur Durchführung dieses Abkommens oder zur Verwaltung oder Anwendung des innerstaatlichen Rechts betreffend Steuern jeder Art und Bezeichnung, die für Rechnung der Vertragsstaaten oder ihrer Gebietskörperschaften erhoben werden, voraussichtlich erheblich sind, soweit die diesem Recht entsprechende Besteuerung nicht dem Abkommen widerspricht. Der Informationsaustausch ist durch Artikel 1 und 2 nicht eingeschränkt.
>
> [2] Alle Informationen, die ein Vertragsstaat nach Absatz 1 erhalten hat, sind ebenso geheim zu halten wie die auf Grund des innerstaatlichen Rechts dieses Staates beschafften Informationen und dürfen nur den Personen und Behörden (einschließlich der Gerichte und der Verwaltungsbehörden) zugänglich gemacht werden, die mit der Veranlagung oder Erhebung, der Vollstreckung oder Strafverfolgung oder mit der Entscheidung von Rechtsmitteln hinsichtlich der in Absatz 1 genannten Steuern oder mit der Aufsicht über diese Personen oder Behörden befasst sind. Diese Personen oder Behörden dürfen die Informationen nur für diese Zwecke verwenden. Sie dürfen die Informationen in einem öffentlichen Gerichtsverfahren oder in einer Gerichtsentscheidung offen legen. Ungeachtet des Vorstehenden können Informationen, die ein Vertragsstaat erhalten hat, für andere Zwecke genutzt werden, wenn diese Informationen für diese anderen Zwecke nach dem Recht beider Staaten genutzt werden können und die zuständige Behörde des informierenden Staates mit dieser Verwendung einverstanden ist.
>
> [3] Die Absätze 1 und 2 sind nicht so auszulegen, als verpflichteten sie einen Vertragsstaat,
>
> a) Verwaltungsmaßnahmen durchzuführen, die von den Gesetzen und der Verwaltungspraxis dieses oder des anderen Vertragsstaats abweichen;

---

7 Bundesgesetz über die internationale Amtshilfe in Steuersachen vom 28. September 2012 (Steueramtshilfegesetz, StAhiG; SR 651.1).

8 Verordnung über die internationale Amtshilfe in Steuersachen vom 23. November 2016 (Steueramtshilfeverordnung, StAhiV; SR 651.11).

9 Vgl. hierzu ausführlich OPEL, Neuausrichtung der schweizerischen Abkommenspolitik in Steuersachen: Amtshilfe nach dem OECD-Standard – Eine rechtliche Würdigung, Habil. Basel, Bern 2015.

b) Informationen zu erteilen, die nach den Gesetzen oder im üblichen Verwaltungsverfahren dieses oder des anderen Vertragsstaats nicht beschafft werden können;

c) Informationen zu erteilen, die ein Handels-, Industrie, Gewerbe- oder Berufsgeheimnis oder ein Geschäftsverfahren preisgeben würden oder deren Erteilung dem Ordre public widerspräche.

4 Wenn ein Vertragsstaat in Übereinstimmung mit diesem Artikel um Erteilung von Informationen ersucht, wendet der andere Vertragsstaat zur Beschaffung der Informationen seine innerstaatlichen Ermittlungsbefugnisse an, auch wenn er die Informationen nicht für seine eigenen Steuerzwecke benötigt. Die Verpflichtung unterliegt den Beschränkungen des Absatzes 3; diese sind aber nicht so auszulegen, als erlaubten sie einem Vertragsstaat, die Erteilung der Informationen abzulehnen, nur weil er kein eigenes Interesse an ihnen hat.

5 Absatz 3 ist nicht so auszulegen, als erlaube er einem Vertragsstaat, die Erteilung von Informationen abzulehnen, nur weil sie sich im Besitz einer Bank, einer anderen Finanzinstitution, eines Beauftragten, Bevollmächtigten oder Treuhänders befinden oder weil sie sich auf Beteiligungen an einer Person beziehen.[10]

Amtshilfeweise können nach dem OECD-Amtshilfestandard somit grundsätzlich sämtliche voraussichtlich erheblichen Informationen, die zur Durchführung des Abkommens oder zur Anwendung des innerstaatlichen Rechts erforderlich sind, eingefordert werden, ohne dass es einer Anlasstat bedürfte.[11] Art. 26 Abs. 1 OECD-MA bedingt Art. 1 OECD-MA und damit das Ansässigkeitserfordernis weg. Weiter hält Art. 26 Abs. 2 OECD-MA fest, dass die erlangten Informationen ausschliesslich Personen und Behörden zugänglich gemacht werden dürfen, «die mit der Veranlagung oder Erhebung, der Vollstreckung oder Strafverfolgung» etc. befasst sind. Der ersuchende Staat ist dazu gehalten, die amtshilfeweise übermittelten Informationen vertraulich zu behandeln und nur den in Art. 26 Abs. 2 OECD-MA vorgesehenen Steuerzwecken zuzuführen; angesprochen ist damit namentlich das sog. Spezialitätsprinzip.[12] Wie sich Art. 26 Abs. 2 OECD-MA entnehmen lässt, umfasst die

10 Wiedergegeben gemäss der vom Bundesministerium der Finanzen in Zusammenarbeit mit dem österreichischen Bundesfinanzministerium und der Eidgenössischen Steuerverwaltung erarbeiteten Übersetzung.

11 Eine solche setzt demgegenüber die immer noch nicht revidierte Amtshilfeklausel des Art. 26 DBA-USA 1996 voraus («Betrugsdelikte oder dergleichen»).

12 Vgl. zu den Vertraulichkeitspflichten des Empfängerstaates ausführlich OPEL, S. 449 ff., insb. S. 453 ff.

Amtshilfe – materiell betrachtet – auch die Steuerstrafrechtshilfe: Die Verwendung der Informationen zur Ahndung von *Steuer*delikten wird ausdrücklich zugelassen.[13] Die Steueramtshilfe ist insoweit «janusgesichtig».[14] Schliesslich ordnet Art. 26 Abs. 5 OECD-MA bekanntermassen an, dass sich das Bank(kunden)geheimnis einem Amtshilfeersuchen nicht entgegenhalten lässt.

III. Frage 1: Sind die Namen von Bankmitarbeitern zu schwärzen?

1. Gesetzliche Grundlage

Art. 4 Abs. 3 StAhiG lautet wie folgt:

> Die Übermittlung von Informationen zu Personen, die nicht betroffene Personen sind, ist unzulässig, wenn diese Informationen für die Beurteilung der Steuersituation der betroffenen Person nicht voraussichtlich relevant sind oder wenn berechtigte Interessen von Personen, die nicht betroffene Personen sind, das Interesse der ersuchenden Seite an der Übermittlung der Informationen überwiegen.

Nach dem Wortlaut des Gesetzes sind Informationen über Bankmitarbeiter somit nur zu übermitteln, wenn sie für die Abklärung der *Steuersituation* der betroffenen Person relevant sind und keine überwiegenden Interessen entgegenstehen.[15]

2. Leitentscheid des Bundesgerichts (BGE 144 II 29[16])

Anlässlich eines US-amerikanischen Amtshilfeersuchens sprach sich das Bundesgericht dafür aus, dass die Namen von Bankmitarbeitern und Rechtsvertretern im Rahmen des Informationsaustauschs grundsätzlich abzudecken sind. Zu übermitteln seien in Anwendung von Art. 26 DBA-USA 1996 und Art. 4 Abs. 3 StAhiG[17] nur voraussichtlich erhebliche Daten. Informationen

---

13 Vgl. auch OECD-MK zu Art. 26 Ziff. 5, wonach sich der Geltungsbereich auf «alle Steuerangelegenheiten» erstreckt, sowie Ziff. 12 bezüglich der Weitergabe an Strafverfolgungsorgane.

14 Vgl. dazu den Beitrag von OPEL, ASA 86 (2017/2018), S. 433 ff.

15 Vgl. dazu ausführlich, OPEL, ASA 86 (2017/2018), S. 469 ff.

16 = Pra 107 (2018) Nr. 127.

17 Das Bundesgericht stützt seine massgebliche Erwägung offenbar auf beide Rechtsgrundlagen ab.

über Bankangestellte und Rechtsvertreter haben laut Bundesgericht «rien à voir avec la question fiscale qui motive les demandes».[18] Es sei – so die Lausanner Richter weiter – nicht ersichtlich, inwieweit die Schwärzung der Namen der Bankangestellten sowie von Anwälten und Notaren in den zu übermittelnden Akten diese unverständlich mache oder ihnen die Beweiskraft nehme. Zwar könne der Umstand, ob der Steuerpflichtige von sich aus oder auf Anraten oder unter Mitwirkung Dritter gehandelt hat, Auswirkung auf die Höhe einer möglichen Steuerbusse haben. Hierfür genüge aber die Information darüber, ob und inwieweit Dritte beteiligt waren – deren Identität sei ohne Belang. Weiter betont das Höchstgericht, dass zwischen Amts- und Rechtshilfe zu unterscheiden ist. Amtshilfe dürfe nicht zweckentfremdet werden, um Informationen über die Identität von mutmasslichen Komplizen des Steuerpflichtigen zu erlangen, sofern diese Informationen nicht erheblich seien für die Abklärung der steuerlichen Situation des Steuerpflichtigen selbst. Das Bundesgericht kam zum Schluss, dass die Namen von Bankmitarbeitern sowie von Anwälten und Notaren in den zu übermittelnden Unterlagen zu schwärzen sind – «*sous réserve de situations où l'Etat requérant demanderait expressément ces données et que celles-ci présenteraient un caractère nécessaire avéré*».[19] Dem Entscheid lässt sich also entnehmen, dass Namen von Dritten in aller Regel zu schwärzen sind.

3. Exkurs: Zivilrechtliche Rechtsprechung

Das Bundesgericht hatte sich schon wiederholt mit der Frage zu befassen, ob die Namen und Funktionen von Bankmitarbeitern gestützt auf sog. Non-Prosecution Agreements (NPA)[20] zwischen Schweizer Banken und dem US-Justizdepartement preisgegeben werden dürfen.[21] In einem Leitentscheid aus

---

18 BGE 144 II 29, E. 4.3.

19 BGE 144 II 29, E. 4.3 in fine. Vgl. zu diesem Urteil OPEL, ASA 86 (2017/2018), S. 471 f.

20 Vgl. zu den Einzelheiten «Rohstoff» des EFD vom 5.5.2014, zu finden unter <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-50049.html>.

21 Dazu sind die Banken gemäss II.D.2.v des US-Programms verpflichtet: Zu übermitteln sind «the name and function of any relationship manager, client advisor, asset manager, financial advisor, trustee, fiduciary, nominee, attorney, accountant, or other individual or entity functioning in a similar capacity known by the Bank to be affiliated with said account at any time during the Applicable Period». Die abgeschlossenen NPA sind zugänglich unter: <https://www.justice.gov/tax/swiss-bank-program>. Nicht Gegenstand der NPA sind demgegenüber Kundendaten – die Einverlangung solcher Informationen hat über den Amtshilfeweg zu erfolgen.

dem Jahr 2017 hat die I. zivilrechtliche Abteilung des Bundesgerichts dies untersagt.[22] Es schützte damit das Urteil der Vorinstanz, wonach die Datenweitergabe gestützt auf Art. 6 Abs. 1 des Datenschutzgesetzes (DSG)[23] unzulässig ist, da der Datenschutz in den USA nicht als genügend eingestuft werden kann.[24] Mit im Wesentlichen gleicher Argumentation hatte das Höchstgericht dasselbe bereits ein Jahr vorher in Bezug auf die Namen von Anwälten entschieden.[25] Diese Rechtsprechung ist inzwischen wiederholt bestätigt worden.[26] Es lässt sich somit feststellen, dass die Gerichte die Risiken für die betroffenen Bankmitarbeiter oder Anwälte grundsätzlich als gewichtiger einstufen als die Interessen der involvierten Banken.[27] Dies führt zu einer eigentümlichen Wertungsdisparität: Amtshilfeweise Datenübermittlungen (ggf. sogar über Bankmitarbeiter) an die USA sind uneingeschränkt zulässig, da sich das StAhiG als lex specialis zum DSG versteht,[28] wohingegen der Informationstransfer gestützt auf die NPA aus datenschutzrechtlichen Gründen ausgeschlossen wird. Im soeben dargelegten Urteil BGE 144 II 29 hat das Bundesgericht übrigens auch die Frage aufgeworfen, ob es nicht treuwidrig scheint, wenn die USA Informationen zu Bankangestellten über den Amtshilfeweg einverlangen, obschon hierfür ja mit den NPA eine eigene Rechtsgrundlage geschaffen wurde.[29]

---

22 BGer 4A_73/2017 vom 26.7.2017.

23 Bundesgesetz über den Datenschutz vom 19.6.1992, SR 235.1.

24 Die Frage, ob die Daten gestützt auf Art. 6 Abs. 2 lit. d DSG ausnahmsweise «für die Wahrung eines überwiegenden öffentlichen Interesses» dennoch weitergegeben werden dürfen, lässt das Bundesgericht offen (da nicht rechtsgenüglich gerügt). Es hinterfragt, ob in dieser Konstellation überhaupt von einem öffentlichen Interesse an der Bekanntgabe der Daten ausgegangen werden kann oder nicht doch nur von einem privaten Interesse der betroffenen Bank an ihrem Weiterbestehen, zumal es sich in casu um eine nicht «systemrelevante» Bank handelte.

25 BGer 4A_83/2016 vom 22.9.2016.

26 Vgl. u.a. BGer 4A_294/2018 vom 20.6.2018; BGer 4A_250/2018 vom 1.10.2018; BGer 4A_522/2017 vom 10.4.2018; BGer 4A_516/2017 vom 10.4.2018; BGer 4A_514/2017 vom 10.4.2018; BGer 4A_390/2017 vom 23.11.2017; BGer 4A_355/2017 vom 29.11.2017.

27 PLÜSS, AJP 2015, S. 1368.

28 So ausdrücklich BGer 2C_619/2018 vom 21.12.2018, E. 4.4 betreffend Amtshilfe an Indien. Indien wird in der Liste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) wie die USA als Staat ausgewiesen, der nicht über einen angemessenen Datenschutz im Sinne von Art. 6 Abs. 1 DSG verfügt.

29 BGE 144 II 29, E. 4.3: «C'est donc par le biais du Programme de régularisation permettant la conclusion de NPA – et non par la voie de l'assistance administrative – que les autorités américaines peuvent obtenir des informations sur les employés de banque».

4. Praxis der ESTV

Die ESTV schwärzt dem Vernehmen nach Namen von Bankmitarbeitern, Anwälten und Notaren weiterhin grundsätzlich nicht; sie informiert diese in der Regel nicht einmal über die Tatsache, dass sie in amtshilfeweise zu übermittelnden Unterlagen erwähnt werden (dazu sogleich). Als Begründung werden insbesondere Praktikabilitätserwägungen ins Feld geführt: Es sei nicht möglich, sämtliche Drittnamen in den herauszugebenden Akten zu schwärzen (auch nicht mithilfe modernster technischer Verfahren). Weiter seien Staaten wie die USA im Nachgang zur höchstrichterlichen Rechtsprechung dazu übergegangen, jeweils ausdrücklich nach den Drittnamen zu fragen.

5. Eigene Stellungnahme

Ob eine Schwärzung der Namen von nicht betroffenen Personen im Sinne von Art. 4 Abs. 3 StAhiG tatsächlich so schwer zu bewerkstelligen ist wie vorgebracht, lässt sich hier nicht abschliessend beurteilen.[30] Zwar mag diese gerade bei umfangreichen Unterlagen einen erheblichen Aufwand bedeuten, jedoch sollten zwecks Wahrung der Verfahrensrechte Drittbetroffener m.E. weder Kosten noch Mühen gescheut werden. Hinzu kommt, dass die ESTV erfahrungsgemäss auch bei Unterlagen geringeren Umfangs konsequent keine Schwärzungen vornimmt; sie praktiziert damit immerhin eine Art «Gleichbehandlung im Unrecht». Weiter liesse sich darüber nachdenken, ob die Schwärzungspflicht nicht auch bei der Informationsinhaberin liegen könnte. Sofern diese mit den betroffenen Dritten in einem vertraglichen Verhältnis steht – wie dies bei einer Bank und ihren Mitarbeitern regelmässig zutrifft –, dürfte die Informationsinhaberin rechtlich allenfalls sogar dazu gehalten sein, die Abdeckungen von sich aus vorzunehmen (Fürsorgepflichten des Arbeitgebers).[31]

---

30 Anzumerken ist, dass im Publikum in Zweifel gezogen wurde, dass dies tatsächlich nicht möglich sein soll.

31 Dieser Frage wird vorliegend nicht vertieft nachgegangen. Die ESTV selbst kann die Informationsinhaberin aber nicht dazu verpflichten (vgl. BGer 2C_653/2017 vom 13.5.2019, E. 6.2 in fine).

IV. Frage 2: Sind Bankmitarbeiter von Amtes wegen zu informieren?

1. Gesetzliche Grundlage

Art. 14 Abs. 1 und 2 StAhiG lauten wie folgt:

> [1] Die ESTV informiert die betroffene Person über die wesentlichen Teile des Ersuchens.
>
> [2] Sie informiert die weiteren Personen, von deren Beschwerdeberechtigung nach Artikel 19 Absatz 2 sie aufgrund der Akten ausgehen muss, über das Amtshilfeverfahren.

Art. 14 Abs. 1 StAhiG ordnet die Information der betroffenen Person an. Ebenso sind die weiteren Personen zu informieren, von deren Beschwerdeberechtigung aufgrund der Akten auszugehen ist. Der (klare) Wortlaut von Abs. 1 und Abs. 2 stimmt insoweit («informiert») überein – die betroffenen Personen sind ebenso wie die beschwerdeberechtigten Dritten von Amtes wegen zu unterrichten. Es wird mithin *kein Ermessensspielraum zuhanden der Behörden* eingeräumt. Dies unterstreichen die Gesetzesmaterialien.[32]

2. Leitentscheid des Bundesgerichts (BGE 143 II 506[33])

Vorliegend hatte das Bundesgericht ebenfalls ein Amtshilfeersuchen seitens der USA zu beurteilen. Strittig war die Beschwerdeberechtigung eines ehemals leitenden Bankmitarbeiters, auf dessen Begehren, sein Name sei zu schwärzen, die ESTV nicht eingetreten war. Wie sich aus den Akten ergibt, hatte der betroffene Bankmitarbeiter unabhängig davon ein Zivilurteil erwirkt, das der kontoführenden Bank untersagte, seinen Namen in Erfüllung des NPA den USA gegenüber bekannt zu geben. Das Bundesgericht kam zum Schluss, dass die ESTV einzutreten hat, da der Bankmitarbeiter beschwerdeberechtigt ist. Er verfüge aufgrund von Art. 4 Abs. 3 StAhiG über ein schutzwürdiges Interesse im Sinne von Art. 48 VwVG.[34] In zweiter Linie ergebe sich die Beschwerdebefugnis auch gestützt auf das Datenschutzrecht.[35] Die

---

32 Botschaft StAhiG, BBl 2011 6215 f.; siehe auch Botschaft ÜAS, BBl 2015 5623, wonach den Dritten eine Beschwerdemöglichkeit zuzugestehen ist (was die vorgängige Information bedingt).

33 = Pra 107 (2018) Nr. 70.

34 Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, VwVG) vom 20.12.1968, SR 172.021.

35 BGE 143 II 506, E. 5.2.2.

Lausanner Richter hielten weiter fest, dass die ESTV grundsätzlich dafür sorgen muss, die Namen von Bankangestellten in übermittelten Unterlagen zu schwärzen, ausser diese Namen scheinen aus irgendeinem Grund voraussichtlich erheblich und ihre Übermittlung ist verhältnismässig. In diesem Fall könne der betreffende Angestellte durchaus ein schutzwürdiges Interesse im Sinne von Art. 48 VwVG geltend machen, und sei es auch nur, um zu überprüfen, dass die Schweizer Behörden die Angaben zu seiner Person nicht in Verletzung von Art. 4 Abs. 3 StAhiG liefern. Das Bundesgericht betonte unter Verweisung auf Art. 19 Abs. 2 StAhiG: «Une possibilité de recours *doit* donc aussi lui être accordée».[36]

Die Lausanner Richter äusserten sich weiter zur Vereinbarkeit des innerstaatlichen Verfahrens mit der abkommensrechtlichen Amtshilfeverpflichtung:[37] Die Gewährung der Verfahrensrechte behindert nach höchstrichterlicher Ansicht nicht in unangemessener Weise die Herausgabe von Informationen an den ersuchenden Staat. Es sei nicht einzusehen, warum die Unterrichtung und die Beschwerdemöglichkeit des Bankangestellten, dessen Namen die ESTV in den zu übermittelnden Unterlagen nicht schwärzen will, die Übermittlung von Informationen auf ungebührliche Weise erschweren sollen. Dieses Verfahren, dessen Gegenstand begrenzt sei, dürfte wohl kaum die Amtshilfe verhindern oder ungebührlich verzögern. Das Bundesgericht hielt abschliessend fest, dass es überdies denkbar sei, die Auskünfte vorerst mit den geschwärzten Namen zu erteilen, bis das Urteil betreffend die Übermittlung der Namen vorliegt.[38]

3. Praxis der ESTV

Wie bereits erwähnt, schwärzt die ESTV Informationen über Dritte nach gegenwärtiger Praxis grundsätzlich dennoch nicht. Zudem werden Drittbetroffene in aller Regel nicht einmal darüber informiert, dass ihre Namen in den zu übermittelnden Unterlagen erscheinen.[39] Parteistellung wird ihnen nur eingeräumt, wenn sie sich der Datenübermittlung *vorsorglich widersetzen*.

---

36 BGE 143 II 506, E. 5.2.1 in fine (Hervorhebung hinzugefügt).

37 Vgl. auch zum Folgenden BGE 143 II 506, E. 5.3.

38 BGE 143 II 506, E. 5.3: «Il est du reste envisageable, si toutes les conditions sont réunies, que les renseignements, avec les noms caviardés, soient remis, jusqu'à droit jugé sur la transmission de ceux-ci».

39 Vgl. hierzu und zum Folgenden die Folien von OPEL/SAXER, IFF-Seminar zur Amtshilfe vom 12./13. Juni 2018.

Zu diesem Zwecke führt die ESTV offenbar eine interne Liste mit den Namen derjenigen Personen, die sich von sich aus gemeldet haben.[40]

Die ESTV *begründet* ihre Vorgehensweise einerseits mit dem (insoweit veralteten) Urteil BGE 139 II 404 aus dem Jahr 2013 betreffend ein Gruppenersuchen gestützt auf das DBA-USA von 1996. Darin verwies das Bundesgericht in einem obiter dictum auf seine Rechtsprechung zur internationalen Rechtshilfe in Strafsachen (!), nach welcher beschwerdebefugt nur unmittelbar betroffene natürliche oder juristische Personen sind, nicht aber bloss indirekt Betroffene. Andererseits werden – wie bereits erwähnt – Praktikabilitätsgründe angeführt. Es sei nicht machbar, sämtliche Drittbetroffenen zu informieren[41] oder (vorerst) zu schwärzen, jedenfalls nicht innerhalb der seitens der OECD geforderten 90-Tage-Frist für die Behandlung von Amtshilfeersuchen.

4. Eigene Stellungnahme

Die Haltung der ESTV ist m.E. gleich aus mehreren Gründen *rechtsstaatlich* nicht vertretbar:

Art. 14 Abs. 2 StAhiG verlangt eine Information der beschwerdeberechtigten Dritten ex officio – der *Gesetzeswortlaut* lässt hieran keinen Zweifel. Solche Dritte sind ebenso wie die betroffene Person über das Amtshilfeersuchen zu orientieren. Die aktuelle Behördenpraxis erweist sich damit als gesetzeswidrig, was – wie dargelegt – durch die Materialien unterstrichen wird.

Die höchstrichterliche *Rechtsprechung* fällt ebenfalls eindeutig aus und lässt keinen Interpretationsspielraum offen. Das Bundesgericht hält im Entscheid BGE 143 II 506 explizit fest, dass Dritten eine Beschwerdemöglichkeit gewährt werden *muss*, was deren Information voraussetzt. Weiter nimmt es auf seine Ausführungen in BGE 139 II 404 (E. 11.1) Bezug und verneint deren

40 Dem Vernehmen nach ist das Führen dieser Liste kürzlich wieder eingestellt worden.

41 Gerne wird das «Hans Meier»-Beispiel bemüht: Erscheine ein Hans Meier oder sonstiger Allerweltsname in den Unterlagen, so sei unmöglich herauszufinden, um welchen Hans Meier es sich tatsächlich handle. Indes liegen mangels Bestimmtheit und Bestimmbarkeit (vgl. hierzu etwa BGE 136 II 508, E. 3.2) der Person in diesem Fall keine Personendaten im Sinne von Art. 3 lit. a DSG vor. Dem wahren Hans Meier erwächst aus der offenen Datenübermittlung auch kein Nachteil.

Einschlägigkeit hinsichtlich der in den Unterlagen erwähnten Bankmitarbeiter ausdrücklich.[42] Dieses Urteil eignet sich daher offensichtlich nicht als Rechtfertigungsgrundlage für die derzeitige Praxis.

Auch das Schrifttum macht sich stark dafür, dass den Drittbetroffenen die Beschwerdelegitimation nach Art. 19 Abs. 2 StAhiG zugestanden wird.[43]

Weiter erscheint es geradezu stossend, dass derzeit nur diejenigen Drittbetroffenen informiert werden, die sich bei der ESTV vorsorglich melden. Es fehlt für diese Vorgehensweise nicht nur an einer gesetzlichen Grundlage (oder an einer offiziellen Verlautbarung seitens der ESTV) – sie ist eines Rechtsstaates schlechterdings nicht würdig. Es kann nicht angehen, dass das rechtliche Gehör nur denjenigen Personen zugestanden wird, die mehr oder weniger zufällig von der «semi-transparenten» Behördenpraxis erfahren haben. Rechtsungleichheiten sind vorprogrammiert. Aus *verfassungsrechtlichen Gründen* (Art. 29 BV und Art. 8 BV) sollte daher dringend von dieser Praxis Abstand genommen werden.

Ferner greift auch das Argument der ESTV, dass die Wahrung der Verfahrensrechte der Betroffenen einer «*OECD-konformen*» *Amtshilfepraxis* entgegenstünde, nicht. Im OECD-Musterkommentar wird seit 2005 vielmehr ausdrücklich festgehalten, dass es Staaten gibt, die von Amtshilfeersuchen Betroffenen das rechtliche Gehör gewähren.[44] Es wird sogar anerkannt, dass die vorgängige Unterrichtung dabei helfen kann, Fehler zu vermeiden oder den

---

42 «L'Administration fédérale se prévaut de l' ATF 139 II 404 consid. 11.1. Contrairement à ce qu'elle soutient, cette jurisprudence ne permet pas d'en conclure qu'un employé de banque dont le nom ne serait pas caviardé dans le cadre d'une procédure d'assistance administrative internationale en matière fiscale ne devrait pas être informé ni qu'il ne pourrait recourir. Cet arrêt refuse certes d'entrer en matière sur une conclusion prise par les recourants tendant à obliger les autorités à informer les personnes dont les données ne sont pas caviardées, afin que celles-ci puissent s'en plaindre. Toutefois, si la Cour de céans a refusé d'entrer en matière, ce n'est pas parce qu'elle a considéré que les personnes dont les données n'étaient pas caviardées n'avaient pas d'intérêt - question qu'elle n'a pas tranchée -, mais parce que les recourants n'étaient eux-mêmes pas directement concernés et ne pouvaient donc faire valoir les intérêts de tiers sous l'angle de l'art. 89 al. 1 let. c LTF. *En l'occurrence, la situation est différente, puisque la personne qui se plaint du non-caviardage de ses données est précisément l'ex-collaborateur de la banque, de sorte qu'il est directement concerné*» (BGE 143 II 506, E. 5.4.1 [Hervorhebung hinzugefügt]). Die Ausführungen lassen m.E. nichts an Deutlichkeit vermissen.

43 BEHNISCH, in: Aktuelle Fragen, S. 136 f., SCHODER, Komm. StAhiG, Art. 19 N 254. Beide Autoren äussern sich nicht näher zur Frage, ob Dritte (konsequenterweise) ex officio zu orientieren sind (vgl. SCHODER, Komm. StAhiG, Art. 14 N 162). Anzumerken ist, dass beide Literaturstimmen aus einer Zeit vor diesem Urteil (BGE 143 II 506) stammen.

44 OECD-MK zu Art. 26 Ziff. 14.1.

Informationsaustausch zu erleichtern. Letztlich sollte das Unterrichtungsverfahren den wirkungsvollen Informationsaustausch aber nicht verhindern oder unangemessen verzögern – es seien mithin Ausnahmen vorzusehen. Genau zu diesem Zweck wurde Mitte 2014 das Verfahren mit nachträglicher Information der beschwerdeberechtigten Personen (Art. 21a StAhiG) implementiert. Was die Effektivität des Informationsaustauschs anbelangt, so wird diese seitens des Global Forum an einer 90-Tage-Frist gemessen, die freilich einzig in der OECD-Mustervorlage für Steuerinformationsabkommen (TIE-MA)[45] niedergelegt ist.[46] Hinzu kommt, dass selbst dort die Frist nicht als bindend ausgewiesen wird. Gemäss Art. 5 Abs. 6 lit. b TIE-MA hat der ersuchte Staat den Ersucherstaat vielmehr unverzüglich zu informieren und über die Gründe zu unterrichten, wenn er dem Ersuchen nicht innerhalb von 90 Tagen nachkommen kann. Dass solche «status updates» zulässig sind, hat das Bundesgericht im Urteil BGE 144 II 130 festgehalten. Folglich ist nicht ersichtlich, weshalb dieser Weg seitens der ESTV nicht beschritten werden könnte.

Schliesslich ist darauf hinzuweisen, dass die *provisorische Schwärzung* sämtlicher Drittnamen einen Ausweg böte, um Ersuchen speditiver nachkommen zu können – die technische Machbarkeit vorausgesetzt.

In einem kürzlich publizierten französischsprachigen Urteil vom April dieses Jahres hat das Bundesverwaltungsgericht der hier vertretenen Ansicht Nachdruck verliehen:[47] Demnach führt die Nichtinformation der Drittbetroffenen nicht nur zur Anfechtbarkeit der Schlussverfügung, sondern sogar zu deren *Nichtigkeit* («nullité»), da es sich hierbei um eine besonders gravierende (nicht heilbare) Gehörsverletzung handle. Das Verfahren ist inzwischen beim Bundesgericht anhängig. Weniger dezidiert äussert sich das Bundesver-

45 Model Agreement on Exchange of Information in Tax Matters (Model TIEA) von 2002 (zu finden unter: <http://www.oecd.org/ctp/exchange-of-tax-information/taxinformation exchangeagreementstieas.htm>).

46 Im Musterkommentar wird die Vereinbarung von zeitlichen Grenzen für die Datenübermittlung demgegenüber als optional ausgewiesen (OECD-MK Art. 26 Ziff. 10.4). Zugleich wird ein differenzierter Vorschlag für eine mögliche Regelung unterbreitet: Demnach sollen sich primär die zuständigen Behörden der Vertragsstaaten auf Fristen einigen, wobei die Informationen mangels einer solchen Abrede so rasch als möglich auszutauschen sind – vorhandene Informationen innerhalb von zwei Monaten, noch zu beschaffende Informationen innerhalb von sechs (!) Monaten. Vorbehalten bleibt stets ein Verzug aus rechtlichen Gründen, etwa wegen einer hängigen Rechtsstreitigkeit. Weiter werden die Behörden zu einer gewissen Flexibilität angehalten, insbesondere bei komplexen Anfragen (OECD-MK Art. 26 Ziff. 10.5).

47 BVGer A-6871/2018 vom 8.4.2019, vgl. insb. E. 4, E. 6.5.

waltungsgericht demgegenüber in seiner deutschsprachigen Rechtsprechung: Von Nichtigkeit will es höchstens dann ausgehen, wenn die formell betroffene Person nicht gehörig informiert worden ist. Werden indes lediglich materiell Betroffene (=Drittbetroffene) nicht angemessen unterrichtet, ist eine Heilung laut Gericht denkbar.[48] Das wiederum heisst handkehrum aber auch, dass die Nichtinformation Dritter als grundsätzlich verfassungswidrig eingestuft wird.

V. Praxis der sog. sekundären Verwendung

1. Grundsatz der Spezialität

Der in Art. 26 Abs. 2 OECD-MA verankerte Grundsatz der Spezialität besagt, dass die erlangten Informationen nur für die erwähnten *Steuerzwecke* verwendet werden dürfen.[49] Untersagt ist es, die amtshilfeweise erlangten Informationen anderen als steuerlichen Zwecken (etwa gemeinstrafrechtlichen Zwecken) zuzuführen. Der Spezialitätsvorbehalt dient primär der Wahrung der Souveränität des ersuchten Staates, um dessen Herrschaft über die übermittelten Informationen in einem gewissen Ausmass zu sichern, und sekundär dem Interesse der Betroffenen.[50]

Im Rahmen des 2012 veröffentlichten Updates von Art. 26 OECD-MA ist der Absatz 2 um einen Satz 4 ergänzt worden. Demnach können Informationen auch zu *anderen, nicht steuerlichen Zwecken* verwendet werden, sofern diese Informationen nach dem Recht beider Staaten zu diesen anderen Zwecken verwendet werden dürfen und die zuständige Behörde des datenliefernden Staates dies erlaubt. Vor dem Update von 2012 wurde diese Möglichkeit schon im OECD-MK erwähnt und seitens der Schweiz bereits in zahlreiche DBA aufgenommen.

2. Verständnis der ESTV

Die ESTV stellte sich bis vor kurzem auf den Standpunkt, dass amtshilfeweise erlangte Informationen nur Personen gegenüber verwendet werden dürfen,

---

48 Vgl. zuletzt BVGer A-1275/2018 vom 23.5.2019, E. 4.2.9 ff. m.w.H. (beim Bundesgericht angefochten). Aus der früheren Rspr. BVGer A-6314/2015 vom 25.2.2016.

49 Vgl. ausführlich OPEL, S. 453 ff.

50 DONATSCH/HEIMGARTNER/MEYER/SIMONEK, S. 117 (bezogen auf die Rechtshilfe). Auch im Rechtshilfebereich ist der Spezialitätsgrundsatz fest verwurzelt.

für die sie explizit verlangt worden sind; vom ersuchenden Staat wurde praxisgemäss eine dahingehende Zusicherung einverlangt. Von dieser Vorgehensweise hat sich die ESTV – dem Vernehmen nach im Zusammenhang mit dem Listenersuchen seitens Frankreichs betreffend UBS-Kundendaten – im Jahr 2018 verabschiedet.[51] Nunmehr werden solche Zusicherungen nicht mehr eingefordert. Die ESTV stellt sich auf den Standpunkt, dass eine sog. sekundäre Verwendung amtshilfeweise erlangter Informationen *auch Dritten und Informationsinhabern (insbesondere Banken) gegenüber* zulässig sei.

Begründet wird diese Praxisänderung dem Vernehmen nach[52] – eine offizielle Stellungnahme nach aussen hin ist bis heute nicht erfolgt – mit einer besseren Erkenntnis der «ratio legis» und unter Hinweis darauf, dass bislang keine wirkliche materielle Auseinandersetzung mit dem Spezialitätsprinzip erfolgt sei. Art. 26 Abs. 2 OECD-MA lässt sich nach Ansicht der ESTV keine Einschränkung der Verwendung der übermittelten Informationen gegenüber Personen, für die Amtshilfe geleistet wurde, entnehmen. Weiter sei eine solche sekundäre Verwendung durch die Schweiz gestützt auf Art. 21 StAhiG ebenfalls zulässig – es mute treuwidrig an, gegenüber dem Ersucherstaat eine Verwendungsbeschränkung geltend zu machen, die selbst im Inland nicht eingehalten werde. Schliesslich vertritt die ESTV die Ansicht, bei der bisherigen Praxis habe es sich um eine unzulässige unilaterale Einschränkung des OECD-Standards gehandelt.

3. Eigene Stellungnahme

Fraglich ist, ob die Praxis der sekundären Verwendung einer vertieften Überprüfung standhält.

---

51 Vgl. BVGer A-1488/2018 vom 30. Juli 2018, E. 4.1 (das Bundesverwaltungsgericht musste sich inhaltlich nicht mit der Praxis befassen, da es die Amtshilfeleistung in casu für unzulässig hielt; der Fall ist derzeit vor Bundesgericht hängig). Siehe zur Praxis der sekundären Verwendung auch OPEL, NZZ vom 14.8.2018, sowie Folien von OPEL/SAXER, IFF-Seminar zur Amtshilfe vom 12./13. Juni 2018.

52 Vgl. wiederum die Folien von OPEL/SAXER, IFF-Seminar zur Amtshilfe vom 12./13. Juni 2018.

a) Rechtsprechung des Bundesgerichts

Das Bundesgericht hat in seiner Rechtsprechung zu Art. 26 DBA-USA 1996[53] sowie auch zu den dem OECD-Standard entsprechenden Amtshilfebestimmungen wiederholt festgehalten, dass das Spezialitätsprinzip so zu verstehen ist, dass Informationen Dritten gegenüber nicht verwendet werden dürfen. Im Entscheid BGE 142 II 161 (zum DBA-F) liest sich etwa Folgendes:

> «*Les tiers dont les noms apparaissent sur de tels documents sont au demeurant protégés*. A la clôture de la procédure, l'autorité requise doit en effet rappeler à l'autorité requérante les restrictions à l'utilisation des renseignements transmis et l'obligation de maintenir le secret (cf. art. 20 al. 2 LAAF)».[54]

Die ESTV ist nach Ansicht des Bundesgerichts also dazu gehalten, den Ersucherstaat über diese Restriktion in Kenntnis zu setzen.

Bestätigt findet sich dies auch im bereits erwähnten Urteil BGE 143 II 506, in welchem das Bundesgericht in den zu übermittelnden Unterlagen erwähnten Drittpersonen die Beschwerdelegitimation zugesteht. Es betont, dass diesen ein schützenswertes Interesse an der Überprüfung der Übermittlung von Angaben zu ihrer Person zukommt, obschon sie durch das Spezialitätsprinzip an sich geschützt sind.[55]

---

53 BGer 2A.551/2001 vom 12. April 2002, E. 6a. Siehe auch BVGer A-6505/2012 vom 29. Mai 2013, E. 9.4; BVGer A-6242/2010 vom 11. Juli 2011, E. 11.4; BVGer A-6705/2010 vom 18. April 2011, E. 5.2; BVGer A-6176/2010 vom 18. Januar 2011, E. 2.5.

54 E. 4.6.1 (Hervorhebung hinzugefügt).

55 E. 5.4.2: «On ne voit pas davantage que le respect du principe de la spécialité justifie de priver l'intimé de tout droit de procédure garanti par la législation nationale, contrairement à ce qu'affirme la recourante. Il n'est pas contesté que les Etats-Unis se sont engagés à respecter ce principe, qui est expressément décrit à l'art. 26 CDI CH-US, et que l'Administration fédérale a rappelé, conformément à l'art. 20 al. 2 LAAF, dans sa décision du 1er décembre 2015, soulignant que les renseignements fournis ne pouvaient être utilisés que dans la procédure contre le contribuable visé. Le fait que les tiers dont les noms sont transmis *soient en principe protégés par le principe de spécialité, comme le Tribunal fédéral l'a relevé* (ATF 142 II 161 consid. 4.6.1 p. 180 s.), ne justifie pas pour autant de priver ces tiers de tous droits de procédure garantis par le droit interne. Une telle justification reviendrait du reste, comme l'a pertinemment retenu le Tribunal administratif fédéral, à rendre vide de sens l'art. 4 al. 3 LAAF. Elle permettrait à l'Administration fédérale, sous le couvert du principe de spécialité, de renoncer à caviarder les données des collaborateurs des banques détentrices d'information de manière discrétionnaire, sans que les intéressés n'en sachent rien et bien que ceux-ci disposent d'un intérêt digne de protection à ce que les conditions permettant, selon le droit suisse, de transmettre de telles données puissent être contrôlées» (Hervorhebung hinzugefügt).

b) Lehre

In der sich hierzu äussernden Lehre wird in Übereinstimmung mit der bundesgerichtlichen Rechtsprechung die Ansicht vertreten, dass eine sekundäre Verwendung amtshilfeweise erlangter Informationen Dritten gegenüber unzulässig ist.[56] So hält insbesondere HOLENSTEIN unmissverständlich fest, dass das Spezialitätsprinzip die Verwendung der ausgetauschten Informationen auf Personen oder Handlungen begrenzt, für welche sie der ersuchende Staat verlangt und der ersuchte Staat sie gewährt hat. Und weiter:

> «Die Verwendung in einem Verfahren gegen andere Personen ist ausgeschlossen […]. Verlangt der ersuchende Staat in einem Amtshilfeersuchen Informationen über eine Drittperson, darf er diese Informationen nur in Bezug auf von der Amtshilfe betroffene Personen verwenden. Er darf sie jedoch insbesondere nicht dazu nutzen, um abzuklären, ob die Drittperson im ersuchenden Staat beschränkt oder unbeschränkt steuerpflichtig ist».[57]

c) Verständnis der OECD

Bei der Auslegung von Doppelbesteuerungsabkommen kommt nach bundesgerichtlicher Rechtsprechung und herrschender Lehre dem OECD-MA und insbesondere dem zugehörigen Kommentar ein grosser Stellenwert zu.[58] Im OECD-Kommentar gelangt deutlich zum Ausdruck, was die OECD unter Amtshilfe versteht: Diese richtet sich ausschliesslich gegen im ersuchenden Staat Steuerpflichtige.[59] Folglich hat nebst den Behörden, welche im Ersucherstaat die Steuern veranlagen, nur die steuerpflichtige Person Zugang zu den ausgetauschten Informationen.[60] Dies spricht gegen eine (sekundäre) Verwendung der erhobenen Informationen gegenüber nicht vom Amtshilfeersuchen betroffenen Dritten. Im OECD-Kommentar findet sich überdies kein Hinweis für die Zulässigkeit einer sekundären Verwendung. Aus dem Musterkommentar geht somit hervor, dass sich die Amtshilfe nach Auffassung der OECD als ein Instrument versteht, das sich stets und *ausschliesslich gegen den/die betroffenen Steuerpflichtigen* richtet.

---

56 HOLENSTEIN, in: Zweifel/Beusch/Matteotti, Art. 26 OECD-MA, N 243; OPEL, NZZ vom 14.8.2018.

57 HOLENSTEIN, in: Zweifel/Beusch/Matteotti, Art. 26 OECD-MA, N 243.

58 Vgl. BGE 143 II 136, E. 5.2.3. Während sich das Bundesgericht für eine subsidiäre Berücksichtigung ausspricht, misst die herrschende Lehre den Werken der OECD sogar eine primäre Bedeutung zu. Vgl. dazu eingehend OPEL, S. 74 ff.

59 OECD-MK zu Art. 26 Ziff. 5, Ziff. 5.2 sowie Ziff. 15.2. Vgl. dazu auch OPEL, ASA 86 (2017/2018), S. 467 f.

60 So ausdrücklich OECD-MK zu Art. 26 Ziff. 12.

Weiter ist zu betonen, dass das Global Forum im Rahmen seiner bisherigen Peer-Reviews die frühere Praxis der ESTV nie beanstandet hat. Es darf folglich davon ausgegangen werden, dass die OECD keinen Anstoss daran nimmt, die Verwendung der amtshilfeweise erlangten Daten auf die anvisierten Steuerpflichtigen zu beschränken.

d) Innerstaatliche Rechtslage

Die ESTV gibt vor, dass das innerstaatliche Recht eine sekundäre Verwendung gestattet oder gar vorsieht. Sie beruft sich hierzu offenbar auf Art. 21 StAhiG. Diese Norm ist jedoch *nicht einschlägig*. Art. 21 StAhiG befasst sich mit indirekt angefallenen Informationen, d.h. solchen, welche die schweizerischen Steuerbehörden zwecks Übermittlung ins Ausland gesammelt haben. Es geht also gerade nicht (!) um Informationen, die amtshilfeweise erlangt worden sind. Folglich ist unklar, weshalb sich die ESTV für eine sekundäre Verwendung im Inland auf diese Norm beruft.

Einschlägig ist vielmehr *Art. 22 Abs. 5 StAhiG* (4. Abschnitt: Schweizerische Amtshilfeersuchen). Dort wird festgehalten, dass die ESTV amtshilfeweise erlangte Informationen an die interessierten Steuerbehörden weiterleitet. Gleichzeitig hat sie auf die Einschränkungen bei deren Verwendung und die Geheimhaltungspflichten nach den Amtshilfebestimmungen des anwendbaren Abkommens zu verweisen. Damit bringt der Gesetzgeber zum Ausdruck, dass die abkommensrechtlichen Schranken – namentlich das Spezialitätsprinzip – bei der Verwendung der Informationen zu beachten sind. Aus dem Gesetz geht zwar nicht explizit hervor, wie das Spezialitätsprinzip auszudeuten ist. Es ist jedoch davon auszugehen, dass die Steuerbehörden dem von der herrschenden Lehre und Rechtsprechung entwickelten Verständnis folgen, d.h. die Informationen nur dem betroffenen Steuerpflichtigen gegenüber verwenden. Das Spezialitätsprinzip unterschiedlich zu verstehen je nachdem, ob Informationen vereinnahmt oder herausgegeben werden, widerspräche dem Grundsatz von Treu und Glauben.

e) Stellung der Dritten im Amtshilfeverfahren

Wie gezeigt, werden gemäss gegenwärtiger Praxis der ESTV Drittpersonen, deren Namen in den zu übermittelnden Unterlagen erscheinen, grundsätzlich nicht über das Amtshilfeersuchen informiert. Ursprünglich pflegte die ESTV

diese Vorgehensweise damit zu begründen, dass Dritte aufgrund des Spezialitätsprinzips ja geschützt seien.[61] Die neue Praxis zur sekundären Verwendung entzieht dieser Argumentation nun aber die Grundlage. Werden Dritte nicht informiert, können sie ihre Rechte nicht geltend machen – sie sind damit verfahrensrechtlich schlechter gestellt als die Steuerpflichtigen, auf die das Amtshilfeersuchen eigentlich abzielt. Ihnen wird mithin das rechtliche Gehör abgeschnitten (Art. 29 Abs. 2 BV) und die Rechtsweggarantie versagt (Art. 29a BV). Die rechtsstaatliche Pflicht zur Wahrung der verfassungsmässigen Rechte der Dritten lässt keine andere Auffassung des Spezialitätsprinzips zu, als dass die Verwendung von auf dem Amtshilfeweg erlangten Informationen ihnen gegenüber nicht zugelassen werden darf. Überhaupt dürfte es auf eine verpönte «fishing expedition» hinauslaufen, wenn der Ersucherstaat in den mit Blick auf eine bestimmte Person übermittelten Unterlagen beliebig nach weiteren Personen forschen darf, gegen die überhaupt kein Verdacht im Raum steht.

f) Fazit

Die Praxis der sekundären Verwendung der ESTV verstösst m.E. gegen die aktuelle höchstrichterliche Rechtsprechung, widerspricht der im Schrifttum geäusserten Ansicht, lässt sich nicht aus den Mustervorlagen der OECD herleiten und ergibt sich auch nicht aus dem innerstaatlichen Recht. Schliesslich ist die neue Praxis auch unter grundrechtlichen Gesichtspunkten entschieden abzulehnen.

VI. Ausblick

1. Hängige Gerichtsverfahren

Es ist zu erwarten, dass einige der hier aufgeworfenen Rechtsfragen in Bälde eine (erste) Klärung erfahren. So geht der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) derzeit gegen die Praxis der ESTV, Dritte nicht zu informieren, vor; eine entsprechende Beschwerde ist vor Bundesverwaltungsgericht hängig.[62] Wie dargelegt, hat das nämliche Gericht ausserdem

[61] Vgl. BGE 143 II 506, E. 3.2.

[62] Vgl. die Empfehlung des EDÖB vom 18. Dezember 2017 (greifbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/empfehlungen.html>). Da die ESTV die Empfehlung ablehnte, legte sie der EDÖB mit Eingabe vom 13. Februar

kürzlich entschieden, dass eine Schlussverfügung der ESTV ohne Information der Drittbetroffenen nichtig sei – dieser Entscheid dürfte richtungsweisend sein, bedarf aber noch der höchstrichterlichen Bestätigung.

Weiter ist der Pilotfall in Sachen Listenersuchen seitens Frankreichs betreffend UBS-Kundendaten vor Bundesgericht hängig. Wie erwähnt, ist die Praxis der sekundären Verwendung offenbar anhand dieses Falles entwickelt worden. Tritt das Bundesgericht auf die Beschwerde ein, ist es nicht unwahrscheinlich, dass es sich auch mit der Zulässigkeit dieser Praxis befassen wird.

2. Anpassung des StAhiG

Als Reaktion auf den Bericht der OECD zur Phase 2 des Peer Review Prozesses sieht der Bundesrat (weiteren) gesetzgeberischen Handlungsbedarf im Bereich der Gehörsgewährung. Vorab ist festzuhalten, dass die Informationspflicht nach Art. 14 StAhiG nicht angerührt werden soll; das hierzu Gesagte behält folglich seine Relevanz. In der am 22. November 2018 veröffentlichten Botschaft zur Umsetzung der Empfehlungen des Global Forum samt Gesetzesentwurf wird hingegen eine Revision von Art. 15 Abs. 2 StAhiG, der sich zum Mitwirkungsrecht und zur Akteneinsicht äussert, wie folgt vorgeschlagen:

> «Einsicht in das Ersuchen und in die Korrespondenz mit der ausländischen Behörde gewährt die ESTV nur, wenn die ausländische Behörde damit einverstanden ist. Andernfalls informiert sie die beschwerdeberechtigten Personen über die wesentlichen Teile des Ersuchens und der Korrespondenz.»[63]

Nach Ansicht des Bundesrats soll es also dem ersuchenden Staat überlassen werden, ob den beschwerdeberechtigten Personen Einsicht in die Akten gewährt wird oder nicht – und zwar *ohne Angabe von Gründen*. Widerspricht dieser der Offenlegung, wird die Akteneinsicht verweigert und nur über den wesentlichen Inhalt der Unterlagen informiert.[64] Zweck dieser Neufassung von Art. 15 Abs. 2 StAhiG ist es, den «Empfehlungen bzw. dem Standard so weit wie möglich zu entsprechen und die Beziehungen zu den Partnerstaaten nicht weiter zu belasten».[65] Dabei handelt es sich um eine Kompromisslösung: Der

2018 dem EFD zum Entscheid im Sinne von Art. 27 Abs. 5 DSG vor. Dieses verfügte am 20. September 2018 die Ablehnung.

63 Art. 15 Abs. 2 E-StAhiG, BBl 2019 346.

64 Siehe Botschaft Global Forum, BBl 2019 331.

65 Botschaft Global Forum, BBl 2019 306.

Bundesrat ist nämlich der Ansicht, dass ein genereller Ausschluss des rechtlichen Gehörs «aus Sicht des schweizerischen Rechts als willkürlich betrachtet werden» könnte.[66]

Die Verweigerung der Akteneinsicht *ohne Geltendmachung von Geheimhaltungsinteressen* durch die ausländische Behörde verstösst gegen die schweizerische Grundordnung im Verwaltungsverfahren (vgl. Art. 27 VwVG). Sie dürfte m.E. weiter einen nicht zu rechtfertigenden Eingriff in den verfassungsrechtlich verbürgten Anspruch auf Gewährung des rechtlichen Gehörs (Art. 29 Abs. 2 BV) darstellen.[67] Ferner würde es – je nach Ersucherstaat – zu einer sachlich nicht zu begründenden Ungleichbehandlung der Betroffenen in verfahrensrechtlicher Hinsicht kommen (siehe insb. auch Art. 29 Abs. 1 BV i.V.m. Art. 8 BV).

Kurz gesagt, diese Neuregelung stellt m.E. ein «rechtsstaatliches Unding» dar – es kann nicht angehen, die Rechtsstaatlichkeit des Verfahrens dem Ermessen oder gar der Willkür ausländischer Steuerbehörden anheimzustellen, *auch nicht ansatzweise*.

VII. Fazit: Zwei Antworten und ein Anliegen

Zweck der Amtshilfe ist es, dass sich die Staaten bei der Durchsetzung ihrer Steueransprüche gegenseitig unterstützen. Gegenstand der Amtshilfe sind daher nur Informationen über im Ersucherstaat zumindest potenziell Steuerpflichtige. Amtshilfe ist nicht zu verwechseln mit Rechtshilfe – sie dient nicht dazu, allfällig involvierte Bankmitarbeiter informationell auszuliefern. Angaben über Bankmitarbeiter müssen in amtshilfeweise zu übermittelnden Unterlagen vielmehr grundsätzlich geschwärzt werden (*erste Antwort*). Geschieht dies im begründeten Einzelfall nicht, so sind die betroffenen Bankmitarbeiter ex officio über das Ersuchen zu unterrichten (*zweite Antwort*). Das Bundesgericht hat diese zwei Fragen schon in seinen beiden Leiturteilen aus dem Jahr 2017 glasklar beantwortet. Die Praxis der ESTV ist vor diesem Hintergrund nicht haltbar. Es kann nicht angehen, dass Dritte schlechter gestellt sind als die amtshilfeweise anvisierten Steuerpflichtigen selbst. Drittbetroffenen ihre Verfahrensrechte zuzugestehen, gebietet sich ebenso aus verfassungsrechtlichen Gründen.

Die auszuarten drohende Amtshilfepraxis der ESTV bedarf dringend einer rechtsstaatlichen Disziplinierung. Und falls die Zeit kommt, in der das

---

66 Botschaft Global Forum, BBl 2019 306.

67 Dazu ausführlich OPEL, ASA 83 (2014/2015), S. 267 ff.

Wünschen wieder hilft, wäre es mein vordringlichstes Anliegen, dass eine Regelung wie Art. 15 Abs. 2 E-StAhiG nie zur Rechtswirklichkeit wird. Dieser Wunsch ist zwischenzeitlich in Erfüllung gegangen. National- und Ständerat haben in der Schlussabstimmung vom 21. Juni 2019 (und damit nach Abfassung dieses Textes) eine Anpassung von Art. 15 StAhiG verworfen. Damit bleibt es – zumindest vorerst – beim status quo.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 22. Juni 2019.

BEHNISCH URS R., Amts- und Rechtshilfe in Steuersachen: Rechtsschutzdefizite, in: Stephan Breitenmoser/Bernhard Ehrenzeller (Hrsg.), Internationale Amts- und Rechtshilfe in Steuer- und Finanzmarktsachen – Aktuelle Fragen und Entwicklungen in der Praxis, Zürich/St. Gallen 2017, S. 117 ff. (zit. BEHNISCH, in: Aktuelle Fragen).

DONATSCH ANDREAS/HEIMGARTNER STEFAN/MEYER FRANK/SIMONEK MADELEINE, Internationale Rechtshilfe unter Einbezug der Amtshilfe im Steuerrecht, 2. Aufl., Zürich 2015.

HOLENSTEIN DANIEL, Kommentierung von Art. 26 OECD-MA, in: Martin Zweifel/Michael Beusch/René Matteotti (Hrsg.), Kommentar zum schweizerischen Steuerrecht, Internationales Steuerrecht, Basel 2015 (zit. HOLENSTEIN, in: Zweifel/Beusch/Matteotti).

OPEL ANDREA, Neuausrichtung der schweizerischen Abkommenspolitik in Steuersachen: Amtshilfe nach dem OECD-Standard – eine rechtliche Würdigung, Habil. Basel, Bern 2015.

– Informationsaustausch über Bankmitarbeiter – das Janusgesicht der Steueramtshilfe, ASA 86 (2017/2018), S. 433 ff.
– Amtshilfe ohne Information der Betroffenen – eine rechtsstaatlich bedenkliche Neuerung, ASA 83 (2014/2015), S. 265 ff.
– Trau, schau, wem – Zum Grundsatz von Treu und Glauben im internationalen Steueramtshilfeverkehr, ASA 86 (2017/2018), S. 257 ff.
– Zu Verfahrensobjekten degradiert – Schweizer Amtshilfe ohne Information Drittbetroffener, NZZ vom 14.8.2018.

OPEL ANDREA/SAXER MICHÈLE, Folien zum Referat «Amtshilfe auf Ersuchen – Verfahrensfragen», gehalten am St. Galler Seminar zum Internationalen Informationsaustausch in Steuersachen am 12./13. Juni 2018, Universität St. Gallen.

PLÜSS ADRIAN, Datenlieferungen im Rahmen des sogenannten US-Programms, AJP 2015, S. 1360 ff. (zit. PLÜSS, AJP 2015).

SCHODER CHARLOTTE, Praxiskommentar zum Bundesgesetz über die internationale Amtshilfe in Steuersachen (Steueramtshilfegesetz, StAhiG), Zürich 2014 (zit. SCHODER, Komm. StAhiG).

VOGEL KLAUS/LEHNER MORIS, Doppelbesteuerungsabkommen (DBA) der Bundesrepublik Deutschland auf dem Gebiet der Steuern vom Einkommen und Vermögen, 6. Aufl., München 2014.

Materialien

Abkommen zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika zur Vermeidung der Doppelbesteuerung auf dem Gebiete der Steuern vom Einkommen vom 2. Oktober 1996 (SR 0.672.933.61).

Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Union über den automatischen Informationsaustausch über Finanzkonten zur Förderung der Steuerehrlichkeit bei internationalen Sachverhalten vom 26. Oktober 2004 (AIA-Abkommen mit der EU; SR 0.641.926.81).

Botschaft zum Erlass eines Steueramtshilfegesetzes vom 6. Juli 2011, BBl 2011 6193 ff. (zit. Botschaft StAhiG).

Botschaft zur Genehmigung des Übereinkommens des Europarats und der OECD über die gegenseitige Amtshilfe in Steuersachen und zu seiner Umsetzung (Änderung des Steueramtshilfegesetzes) vom 5. Juni 2015, BBl 2015 5585 ff. (zit. Botschaft ÜAS).

Botschaft zur Genehmigung und Umsetzung eines Protokolls zur Änderung des Zinsbesteuerungsabkommens zwischen der Schweiz und der EU vom 25. November 2015, BBl 2015 9199 ff. (zit. Botschaft AIA-Abkommen-EU).

Botschaft zur Umsetzung der Empfehlungen des Globalen Forums über Transparenz und Informationsaustausch für Steuerzwecke im Bericht zur Phase 2 der Länderüberprüfung der Schweiz vom 21. November 2018, BBl 2019 279 ff. (zit. Botschaft Global Forum).

Bundesgesetz über das Verwaltungsverfahren vom 20.12.1968 (Verwaltungsverfahrensgesetz, VwVG; SR 172.021).

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

Bundesgesetz über die internationale Amtshilfe in Steuersachen vom 28. September 2012 (Steueramtshilfegesetz, StAhiG; SR 651.1).

Bundesgesetz zur Umsetzung von Empfehlungen des Globalen Forums über Transparenz und Informationsaustausch für Steuerzwecke (Entwurf), BBl 2019 339 ff. (zit. E-StAhiG).

Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV; SR 101).

Model Agreement on Exchange of Information in Tax Matters (Model TIEA) von 2002 (zu finden unter: <http://www.oecd.org/ctp/exchange-of-tax-information/taxinforma tionexchangeagreementstieas.htm>).

OECD-Musterabkommen ab 1963 (letzte Aufdatierung 2017) zur Vermeidung der Doppelbesteuerung von Einkommen und Vermögen (= OECD Model Tax Convention on Income and on Capital, zu finden unter: <http://www.oecd.org/ctp/treaties /model-tax-convention-on-income-and-on-capital-condensed-version-20745419.htm>).

Übereinkommen über die gegenseitige Amtshilfe in Steuersachen vom 25. Januar 1988 (SR 0.652.1).

Verordnung über die internationale Amtshilfe in Steuersachen vom 23. November 2016 (Steueramtshilfeverordnung, StAhiV; SR 651.11).

Datenlieferung und Steueramtshilfe aus der Sicht der ESTV

Adrian Hug, Bern*

* Direktor der Eidgenössischen Steuerverwaltung.

I. Einleitung

In den letzten rund 10 Jahren hat sich die Amtshilfe international, aber insbesondere in der Schweiz, ausserordentlich stark entwickelt. Im Rahmen der OECD und der G20-Staaten wurden die Bemühungen, die Verschiebung von Gewinnen in Tiefsteuerländer zu verhindern (Projekt «BEPS»), massiv ausgebaut. Zentrales Element dieser Strategie ist die Sicherstellung der Transparenz über die steuerlichen Verhältnisse der Unternehmen. Bei den Massnahmen steht dabei die Amtshilfe an erster Stelle; zur Durchsetzung der Standards werden dabei auch sogenannte «schwarze» Listen verwendet, was für die Unternehmen in den betroffenen Staaten grosse Nachteile zur Folge haben kann.

In der Schweiz mussten die massgeblichen Gesetze im Bereich der Amtshilfe mehrmals angepasst werden. Insgesamt ist die Amtshilfe damit ein relativ neues Rechtsgebiet, zu dem nur teilweise eine Rechtsprechung durch die Gerichte besteht. Viele Fragen müssen von den mit dem Vollzug betrauten Behörden, insbesondere der Abteilung für Informationsaustausch in Steuersachen (SEI) der ESTV erarbeitet werden. Die intensive Diskussion über die Auslegung der gesetzlichen Bestimmungen und schliesslich die Beurteilung

der wichtigsten Rechtsfragen durch das Bundesgericht sind wesentliche Schritte, um in diesem Bereich Rechtssicherheit zu schaffen.

II. Arten der Amtshilfe

Die ESTV ist in der Schweiz die zuständige Behörde für die Amtshilfe in Steuersachen und somit für den Austausch von Informationen verantwortlich. Ihre Aufgaben und der Aufwand im Bereich der internationalen Amtshilfe haben sich aufgrund der politischen Entwicklungen in diesem Bereich stetig erhöht und es ist zu erwarten, dass diese Tendenz in den nächsten Jahren anhalten wird.

1. Amtshilfe auf Ersuchen

Es besteht einerseits die klassische Amtshilfe auf Anfrage. Bei dieser Art der Ersuchen kann der ersuchende Staat nach Informationen fragen, die zur Durchführung des Abkommens oder zur Verwaltung oder Anwendung des innerstaatlichen Rechts dienen. Die Ersuchen werden gestützt auf verschiedene gesetzliche Grundlagen gestellt. Die Schweiz hat mit sehr vielen Ländern Abkommen zur Vermeidung der Doppelbesteuerung (sog. DBA) sowie mit einigen Ländern Steuerinformationsabkommen (TIEA) abgeschlossen. Immer mehr erfolgt der Austausch gestützt auf das Übereinkommen über die gegenseitige Amtshilfe in Steuersachen (Amtshilfeübereinkommen, MAC, SR 0.652.1). Die amtshilfespezifischen gesetzlichen Grundlagen im nationalen Kontext sind das Bundesgesetz vom 28. September 2012 über die internationale Amtshilfe in Steuersachen (StAhiG, SR 651.1) sowie die dazugehörige Steueramtshilfeverordnung (StAhiV; SR 651.11).

2. Spontaner Informationsaustausch

Seit dem Jahr 2018 tauscht die Schweiz die Templates betr. Steuerrulings im Zusammenhang mit der spontanen Amtshilfe aus. Der spontane Austausch der Steuerrulings basiert auf dem am 1. Januar 2017 in Kraft getretenen Amtshilfeübereinkommen (MAC). Dieses hatte sodann auch eine Revision des Steueramtshilfegesetzes sowie der Steueramtshilfeverordnung zur Folge, die den Vollzug der spontanen Amtshilfe im internen Recht regeln.

3. Automatischer Informationsaustausch

Im Zusammenhang mit dem Automatischen Informationsaustausch über Finanzkonten (AIA) wurden per Ende September 2018 mit 36 Partnerstaaten erstmals entsprechende Informationen ausgetauscht. Die Rechtsgrundlagen für den AIA sind seit dem 1. Januar 2017 in Kraft.

Diese Informationsübermittlung findet basierend auf die folgenden Rechtsgrundlagen statt: Amtshilfeübereinkommen (MAC), Multilaterale Vereinbarung der zuständigen Behörden über den automatischen Informationsaustausch über Finanzkonten (MCAA; SR 0.653.1), Bilaterale Staatsverträge mit EU, Hongkong und Singapur, Vereinbarung zwischen der Schweiz und AIA-Partnerstaaten (Aktivierung), Bundesgesetz über den internationalen automatischen Informationsaustausch in Steuersachen vom 18. Dezember 2015 (AIAG; SR 653.1) und die dazugehörige Verordnung (AIAV; SR 653.11).

4. Country by Country Reporting

Schliesslich findet im Jahr 2020 auch der erste reguläre Austausch betr. Country by Country Reporting (CbCR) statt. Das sogenannten CbCR sieht für Grosskonzerne einen länderbezogenen Bericht vor, der Informationen über die weltweite Verteilung der Umsätze und der entrichteten Steuern, weitere Kennzahlen der nationalen Konzerne in den einzelnen Staaten und Hoheitsgebieten sowie Angaben über die wichtigsten wirtschaftlichen Tätigkeiten sämtlicher konstitutiver Rechtsträger der multinationalen Konzerne enthält. Das Country by Country Reporting stützt sich im internationalen Kontext auf das Amtshilfeübereinkommen (MAC) sowie die Multilaterale Vereinbarung der zuständigen Behörden über den Austausch länderbezogener Berichte (ALBA-Vereinbarung; SR 0.654.1). Im internen Recht ist der Vollzug mittels des Bundesgesetzes vom 16. Juni 2017 über die internationalen automatischen länderbezogenen Berichte multinationaler Konzerne (ALBAG; SR 654.1) sowie der dazugehörigen Verordnung (ALBAV; SR 654.11) geregelt.

III. Verfahren

1. Informationsaustausch auf Ersuchen und spontaner Informationsaustausch

Wenn bei der ESTV ein entsprechendes Ersuchen eines Staates eintrifft, werden die formellen Voraussetzungen wie folgt geprüft:

Gemäss Artikel 6 Absatz 1 StAhiG muss das Amtshilfegesuch schriftlich in einer schweizerischen Amtssprache oder in Englisch gestellt werden. Ferner muss es die im anwendbaren Abkommen vorgesehenen Angaben enthalten. Enthält das anwendbare Abkommen keine Bestimmungen über den Inhalt eines Ersuchens und lässt sich aus dem Abkommen nichts anderes ableiten, so muss das Ersuchen die in Artikel 6 Absatz 2 StAhiG aufgelisteten Angaben enthalten:

- Die Identität der betroffenen Person;
- Eine Beschreibung der verlangten Informationen;
- Den Steuerzweck, für den die Informationen verlangt werden;
- Die Gründe zur Annahme, dass sich die verlangten Informationen im ersuchten Staat befinden;
- Den Namen und die Adresse der mutmasslichen Informationsinhaberin;
- Eine Erklärung, dass die ersuchende Behörde die Informationen in Anwendung ihres Rechts erhalten könnte und dass sie ihre innerstaatlichen Auskunftsquellen ausgeschöpft hat.

Auf das Ersuchen wird nicht eingetreten, wenn es zum Zweck der Beweisausforschung («fishing expedition») gestellt wird, die verlangten Informationen von der Amtshilfebestimmung des anwendbaren DBA nicht erfasst werden oder das Ersuchen den Grundsatz von Treu und Glauben verletzt.

Tritt die ESTV auf das Amtshilfegesuch nicht ein, findet keine Übermittlung von Informationen statt. Das Amtshilfeverfahren wird vielmehr abgeschlossen und der Entscheid wird dem ersuchenden Staat mit entsprechenden Kommentaren mitgeteilt. Kommt die ESTV hingegen zum Schluss, dass auf das Amtshilfegesuch einzutreten ist, werden in einem nächsten Schritt die Informationen beschafft. Dazu erlässt die ESTV eine Editionsverfügung, die an die formell und/oder materiell betroffene Person (Art. 9 StAhiG), die Informationsinhaberin (Art. 10 StAhiG), an eine kantonale Steuerverwaltung (Art. 11 StAhiG) oder an eine andere schweizerische Behörde (Art. 12 StAhiG) gerichtet sein kann.

Die betroffene Person und die Informationsinhaberin müssen alle relevanten Informationen herausgeben, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden (Art. 9 Abs. 3 bzw. Art. 10 Abs. 3 StAhiG). Die kantonale Steuerverwaltung und die anderen schweizerischen Behörden müssen die Informationen, die voraussichtlich für die Beantwortung des Ersuchens erforderlich sind, herausgeben (Art. 11 Abs. 1 bzw. Art. 12 Abs. 1 StAhiG).

Der Anspruch auf rechtliches Gehör wird von Artikel 29 Absatz 2 der schweizerischen Bundesverfassung vom 18. April 1999 (BV; SR 101) garantiert. Das Steueramtshilfegesetz konkretisiert dieses Grundrecht in den Artikeln 14 und 15 StAhiG. Die ESTV informiert die betroffene Person über die wesentlichen Teile des Ersuchens sowie die weiteren beschwerdeberechtigten Personen über das Amtshilfeverfahren.

Ist eine beschwerdeberechtigte Person im Ausland ansässig, ersucht die ESTV die Informationsinhaberin, diese Person aufzufordern, eine zur Zustellung bevollmächtigte Person in der Schweiz zu bezeichnen oder eine CH-Adresse zu nennen. Kann eine beschwerdeberechtigte Person nicht erreicht werden, so kann die ESTV diese im Ausland direkt informieren, wenn es zulässig ist, Schriftstücke im betreffenden Saat durch die Post zuzustellen oder die ersuchende Behörde diesem Vorgehen im Einzelfall ausdrücklich zustimmt. Als ultima ratio wird die betroffene Person durch Veröffentlichung im Bundesblatt über das Ersuchen informiert und aufgefordert, eine zur Zustellung bevollmächtigte Person zu bezeichnen (Art. 14 Abs. 3 bis 5 StAhiG).

Die beschwerdeberechtigten Personen können sich am Verfahren beteiligen und Einsicht in die Akten nehmen (Art. 15 Abs. 1 StAhiG).

Es wird zwischen dem vereinfachten (Art. 16 StAhiG) und dem ordentlichen Verfahren (Art. 17 StAhiG) unterschieden. Vom vereinfachten Verfahren wird gesprochen, wenn die beschwerdeberechtigten Personen der Übermittlung der Informationen an die ersuchende Behörde zustimmen. Dies teilen sie der ESTV mittels Zustimmungserklärung schriftlich mit. Diese Zustimmung ist unwiderruflich. Die ESTV schliesst das Verfahren ab, indem sie die Informationen unter Hinweis auf die Zustimmung der beschwerdeberechtigten Personen an die ersuchende Behörde übermittelt. Stimmen die beschwerdeberechtigten Personen der Übermittlung der Informationen nicht zu, eröffnet die ESTV jeder beschwerdeberechtigten Person eine Schlussverfügung.

Die allfällige Beschwerde gegen die Schlussverfügung ist innert 30 Tagen beim Bundesverwaltungsgericht einzureichen. Die Beschwerde hat aufschiebende Wirkung. Dies bedeutet, dass die Informationen bis zum rechtskräftigen Entscheid nicht übermittelt werden.

Gegen einen Entscheid des Bundesverwaltungsgerichts kann auf dem Gebiet der internationalen Amtshilfe in Steuersachen innert 10 Tagen nach Eröffnung beim Bundesgericht Beschwerde in öffentlich-rechtlichen Angelegenheiten geführt werden, jedoch nur, sofern eine Rechtsfrage von grundsätzlicher Bedeutung vorliegt.

Im Unterschied zum Informationsaustausch auf Ersuchen werden beim spontanen Informationsaustausch Informationen ohne vorgängiges Ersuchen eines Staates übermittelt.

Der spontane Informationsaustausch ist auf die Mitgliedstaaten des Amtshilfeübereinkommens (MAC) begrenzt. Der Austausch zwischen den Mitgliedstaaten basiert auf Gegenseitigkeit. Die Liste aller Mitgliedstaaten sowie das jeweilige Datum des Inkrafttretens für die einzelnen Staaten sind im Amtshilfeübereinkommen (MAC) ersichtlich.

Der spontane Informationsaustausch betrifft die Steuervorbescheide («Steuerrulings») gemäss den Artikeln 8 und 9 StAhiV.

Das Verfahren richtet sich nach dem Steueramtshilfegesetz. Gemäss Artikel 22a StAhiG treffen die ESTV und die kantonalen Steuerverwaltungen die notwendigen Massnahmen, damit die Fälle identifiziert werden, in welchen spontan Informationen auszutauschen sind. Die kantonalen Steuerverwaltungen stellen der ESTV die zur Übermittlung an die zuständigen ausländischen Behörden vorgesehenen Informationen unaufgefordert und fristgerecht zu. Die ESTV nimmt eine Sichtung im Hinblick auf die Vollständigkeit der Informationen vor und übermittelt diese anschliessend.

Das weitere Verfahren stimmt weitgehend mit dem Verfahren für den Informationsaustausch auf Ersuchen überein. Die ESTV informiert die betroffene Person und weitere beschwerdeberechtigte Personen über den vorgesehenen spontanen Informationsaustausch (Art. 22b StAhiG). Kann eine beschwerdeberechtigte Person nicht erreicht werden, so informiert die ESTV sie durch Veröffentlichung im Bundesblatt über die vorgesehene Übermittlung von Informationen. Sie fordert sie auf, eine zur Zustellung bevollmächtigte Person zu bezeichnen oder eine CH-Adresse zu benennen. Betreffend das Mitwirkungsrecht, Akteneinsicht, das weitere Verfahren und das Rechtsmittelverfahren wird auf das Ausgeführte zum Informationsaustausch auf Ersuchen verwiesen.

2. Automatischer Informationsaustausch

Im Rahmen des Automatischen Informationsaustauschs über Finanzkonten (AIA), gemäss dem Gemeinsamen Meldestandard (GMS) der OECD, erfolgt

der Austausch von Identifikations-, Konto- und Finanzinformationen regelmässig und innerhalb festgelegter Fristen[1]. Die ESTV und die zuständigen Behörden der Partnerstaaten müssen die Informationen innerhalb von neun Monaten nach Ablauf des Kalenderjahres, auf das sie sich beziehen, austauschen. Grundsätzlich hat die ESTV bei der Übermittlung von AIA-Daten keinen Ermessensspielraum. Als «Notbremse» dient der sogenannte individuelle Rechtsschutz gemäss Artikel 19 Absatz 2 Satz 2 AIAG. Demnach stehen meldepflichtigen Personen gegenüber der ESTV die Ansprüche nach Artikel 25a des Bundesgesetzes über das Verwaltungsverfahren (VwVG; SR 172.021) zu, sofern die Übermittlung der Daten für die meldepflichtige Person Nachteile zur Folge hätte, die ihr aufgrund fehlender rechtsstaatlicher Garantien nicht zugemutet werden können.

Gestützt auf Artikel 19 Absatz 1 AIAG stehen den meldepflichtigen Personen die Rechte nach dem Datenschutzgesetz zu. D.h. sie haben sowohl gegenüber den Finanzinstituten als auch gegenüber der ESTV Anspruch zu erfahren, ob Daten über sie bearbeitet werden. Gegenüber der ESTV können die meldepflichtigen Personen jedoch keine Daten berichtigen, ausser die unrichtigen Daten beruhen auf Übermittlungsfehlern[2].

3. Country by Country Reporting

Der automatische Austausch länderbezogener Berichte multinationaler Konzerne (Country by Country Reporting) erfolgt wie der AIA über Finanzkonten regelmässig und innerhalb festgelegter Fristen. Die ESTV übermittelt bisher nur bei ihr freiwillig eingereichte Country by Country Berichte an die Partnerstaaten. Anders als beim AIA über Finanzkonten übermitteln die betroffenen Konzerne der ESTV keine Informationen über Dritte, sondern über sich selbst.

---

1 Vgl. Abschnitt 3 Absatz 3 der Multilateralen Vereinbarung der zuständigen Behörden über den automatischen Informationsaustausch über Finanzkonten; MCAA; SR 0.653.1.

2 Vgl. Botschaft zur Genehmigung der multilateralen Vereinbarung der zuständigen Behörden über den automatischen Informationsaustausch über Finanzkonten und zu ihrer Umsetzung (Bundesgesetz über den internationalen automatischen Informationsaustausch in Steuersachen), BBl 2015 5504.

IV. Zuständigkeiten innerhalb der ESTV

1. Abteilung Informationsaustausch in Steuersachen (SEI)

Die Aufgaben der Abteilung Informationsaustausch in Steuersachen (SEI) umfassen den Vollzug der Amtshilfe betreffend die ein- und ausgehenden Ersuchen sowie den spontanen Informationsaustausch. Im Bereich des Informationsaustauschs ist der SEI für die gesamte Schweiz im Namen der ESTV als zuständige Behörde (competent authority) tätig. Bei den eingehenden Ersuchen wickelt der SEI das gesamte Verfahren ab, vom Eingang des Ersuchens bis zur Übermittlung der Informationen an den ausländischen Staat.

Betreffend die von der Schweiz an das Ausland gerichteten Ersuchen unterstützt der SEI die Steuerbehörden bei der Ausarbeitung der Ersuchen, prüft insbesondere die Erfüllung der formellen Erfordernisse und sendet diese an den jeweiligen Staat. Die anschliessend eingehenden Informationen werden sodann den Steuerbehörden weitergeleitet.

Beim spontanen Informationsaustausch stellt der SEI die Abwicklung der eingehenden sowie der ausgehenden Steuervorbescheide sicher.

Da die Anzahl, der Umfang und die Komplexität der Ersuchen seit der Gründung des SEI im Jahr 2010 stetig zugenommen haben und seit dem Jahre 2018 auch der spontane Informationsaustausch über den SEI abgewickelt wird, ist der Personalbestand im Laufe der Jahre gewachsen und umfasst nun rund 75 Mitarbeitende.

2. Abteilung Erhebung Verrechnungssteuer und Stempelabgaben (DVS-ER)

Die DVS-ER ist im Zusammenhang mit der Datenlieferung und Steueramtshilfe in der ESTV mit dem Vollzug der Übermittlung der Identifikations-, Konto- und Finanzinformationen betreffend AIA betraut.

Die Abwicklung ist dank der Informatik zu einem grossen Teil automatisiert und grundsätzlich ist – mit Ausnahme der vorgenannten «Notbremse» – keine Teilnahme der betroffenen Personen am Verfahren vorgesehen (Art. 19 Abs. 2 Satz 2 AIAG). Aus diesen Gründen werden für die Abwicklung des AIA nur wenige personelle Ressourcen benötigt. Im Moment sind es 5 Mitarbeitende, die den Vollzug des AIA vornehmen.

V. Amtshilfe auf Ersuchen

1. Statistik

Jahr	Eingehende Ersuchen vom Ausland	Ausgehende Ersuchen ans Ausland
2012	1499	2
2013	1386	6
2014	2791	2
2015	2623	39
2016	66553	11
2017	18164	18
2018	4744	28

Wie aus der Statistik hervorgeht, hat sich die Zahl der eingereichten Ersuchen in den vergangenen Jahren insgesamt erhöht.

Der starke Anstieg im Jahr 2016 ist auf die erstmalig bei der ESTV eingegangenen Masseneinzelersuchen zurückzuführen. Im Jahr 2016 wurden mehrere solche Grossersuchen mit mehreren 10'000 betroffenen Personen eingereicht.

Die Entwicklung der eingehenden Amtshilfeersuchen ist schwierig abzuschätzen. Aufgrund von Erfahrungswerten kann jedoch festgehalten werden, dass die Anzahl Einzelersuchen nach der Anpassung eines Doppelbesteuerungsabkommens (DBA) bzw. eines Steuerinformationsabkommens (TIEA) zunimmt. Aufgrund der fortlaufenden Anpassung des Schweizer DBA- und TIEA-Netzes an den internationalen Standard und durch das Inkrafttreten des Amtshilfeübereinkommens (MAC) ist davon auszugehen, dass die Anzahl Einzelersuchen weiter zunehmen wird. Auch wenn es aus der Statistik nicht direkt ablesbar ist, erhielt die ESTV im Jahr 2018 erheblich mehr Einzelersuchen als in den Vorjahren.

2. Arten der Ersuchen

Aufgrund der inzwischen mehrjährigen Erfahrung im Bereich der Amtshilfe, können die Ersuchen aufgrund ihrer Form sowie des Inhaltes in Kategorien eingeteilt werden.

a) Form

Bei den eingegangenen Ersuchen können drei Kategorien unterschieden werden, die auch unterschiedliche formelle Erfordernisse mit sich bringen:

– Einzelersuchen;
– Gruppenersuchen;
– Masseneinzelersuchen (sogenannte «bulk requests»).

Einzelersuchen betreffen eine bestimmte ausländische steuerpflichtige Person. Gruppenersuchen werden in Bezug auf eine unbestimmte Anzahl ausländischer Steuerpflichtiger gestellt, die durch ein gemeinsames «Verhaltensmuster» gekennzeichnet sind. Masseneinzelersuchen wiederum betreffen eine Reihe von im Voraus bestimmten oder zumindest bestimmbaren Personen.

Diese drei Arten von Ersuchen werden unterschiedlich behandelt. Während bei den Einzelersuchen ein individuelles Verfahren geführt werden muss, werden die Gruppenersuchen aufgrund von standardisierten Vorlagen abgehandelt, was zu einer geringeren Bearbeitungszeit pro Fall innerhalb eines Gruppenersuchens führt. Wie bei den Gruppenersuchen werden auch bei den Masseneinzelersuchen relativ einfache Informationen erfragt. Die Behandlung der Gruppen- und Masseneinzelersuchen ist pro Fall deutlich weniger aufwändig als diejenige von klassischen Einzelersuchen, da für alle Fälle derselbe Tatbestand anwendbar ist.

b) Inhalt

Der Inhalt und der Umfang der erfragten Informationen variieren je nach Ersuchen sehr stark. Die im Rahmen von Bankersuchen nachgesuchten Informationen sind weitgehend standardisiert und umfassen häufig die folgenden Unterlagen:

– Kontoauszug
– Bankinformationen im Zusammenhang mit dem Inhaber
– Wirtschaftlich Berechtigter
– Inhaber einer Vollmacht auf dem Konto
– KYC-Unterlagen

Bei Ersuchen betreffend Gesellschaften werden die folgenden Informationen erfragt: Statuten, Aktionäre, tatsächliches Bestehen, Bilanzen, Erfolgsrechnungen, Transferpreise, Verträge, Rechnungen. Zusätzlich werden oftmals bei den kantonalen Steuerverwaltungen die folgenden Informationen eingeholt: Statuten, Steuerbasis, Steuersatz, Steuererklärung, Steuervorbescheide, etc.

Bei Ansässigkeitsersuchen will der ersuchende Staat wissen, ob die natürliche oder juristische Person den Sitz bzw. den Wohnsitz in der Schweiz hat. Bei den Grenzgängerersuchen wird in der Regel beim schweizerischen Arbeitgeber der Lohnausweis eingefordert. Gestützt auf die Verständigungsvereinbarung zwischen der Schweiz und der Republik Österreich im Zusammenhang mit der gegenseitigen Amtshilfe bei der Vollstreckung hinsichtlich der Lohnsteuer in Artikel 26a DBA-Österreich [SR 0.672.916.31] werden entsprechende Vollstreckungsersuchen entgegengenommen. Diese Ersuchen sind in der Regel weit weniger aufwändig, als die Ersuchen betreffend Gesellschaften.

3. Gruppenersuchen und «bulk requests»

a) Verfahren

Das Verfahren bei Gruppenersuchen läuft grundsätzlich analog dem Verfahren der Einzelersuchen ab. Aufgrund des Umstandes, dass bei Gruppenersuchen Informationen über Personen verlangt werden, die nicht namentlich bekannt sind, benötigt es für deren Information über das Amtshilfeverfahren jedoch eine andere Vorgehensweise als bei Einzelersuchen. Im Rahmen der Teilrevision des Steueramtshilfegesetzes im August 2013[3] wurde mit Artikel 14a StAhiG die Information bei Gruppenersuchen gesetzlich definiert.

Auf Verlangen der ESTV identifiziert die Informationsinhaberin die von einem Gruppenersuchen betroffenen Personen aufgrund der von der ausländischen Behörde geschilderten identischen Verhaltensmuster sowie weiterer zur Identifikation notwendiger Angaben. Nach erfolgter Identifikation der vom Gruppenersuchen betroffenen Personen durch die Informationsinhaberin informiert die ESTV die beschwerdeberechtigten Personen mit Sitz oder Wohnsitz in der Schweiz direkt über das Ersuchen (Art. 14a Abs. 2 StAhiG). Weiter ersucht die ESTV die Informationsinhaberin, die beschwerdeberech-

[3] Vgl. AS 2014 2309; BBl 2013 8369.

tigten Personen im Ausland über das Ersuchen zu informieren und sie gleichzeitig aufzufordern, eine zur Zustellung bevollmächtigte Person in der Schweiz zu bezeichnen (Art. 14a Abs. 3 StAhiG). Die ESTV kann eine im Ausland ansässige beschwerdeberechtigte Person auch direkt informieren, wenn es zulässig ist, Schriftstücke im betreffenden Staat durch die Post zuzustellen oder wenn die ersuchende Behörde einer direkten Information im Einzelfall ausdrücklich zustimmt (Art. 14a Abs. 3bis StAhiG).

Zudem informiert die ESTV die vom Gruppenersuchen betroffenen Personen ohne Namensnennung durch Publikation im Bundesblatt über:

- den Eingang und den Inhalt des Ersuchens;
- ihre Pflicht, eine allfällige inländische Adresse bei Sitz oder Wohnsitz in der Schweiz oder eine zur Zustellung bevollmächtigte Person in der Schweiz anzugeben;
- das vereinfachte Verfahren nach Artikel 16 StAhiG; und
- darüber, dass für jede beschwerdeberechtigte Person eine Schlussverfügung erlassen wird, sofern keine Zustimmung zur Übermittlung vorliegt.

Kann die ESTV eine Schlussverfügung den beschwerdeberechtigten Personen nicht zustellen, so notifiziert sie diesen die Verfügung ohne Namensnennung durch Mitteilung im Bundesblatt (Art. 14a Abs. 6 StAhiG).

b) Pilotfälle

Eine weitere Besonderheit der Gruppenersuchen und Masseneinzelersuchen (sog. «bulk requests») bildet der Umstand, dass solche Ersuchen eine Vielzahl von Fällen umfassen. Dies hat zur Folge, dass das Prozessrisiko entsprechend höher ist. Zudem stellt die Zulässigkeit des Gruppenersuchens bzw. des bulk requests in allen Verfahren eine zentrale Frage dar. Um das Prozessrisiko zu minimieren sowie diese zentrale Frage für alle betroffenen Fälle zu beantworten, definiert die ESTV daher Pilotfälle, welche abgewickelt und gerichtlich beurteilt werden, bevor die weiteren Verfahren an die Hand genommen werden. Ein Beispiel eines solchen Pilotfalls betrifft den Leitentscheid des Bundesgerichts BGE 143 II 136, worin bezüglich eines niederländischen Gruppenersuchens festgehalten wurde, dass solche gestützt auf die Verständigungsvereinbarung zwischen der Schweiz und den Niederlanden ohne Namensnennung möglich sind (vgl. E. 5.3.4 des genannten Urteils).

4. Internationaler Standard

a) Empfehlungen des Global Forum

Der Informationsaustausch auf Ersuchen ist gemäss der OECD dann effizient, wenn die Behandlung der Amtshilfeersuchen gemäss der Empfehlung des Global Forums für Transparenz und Informationsaustausch innerhalb von 90 Tagen durchgeführt wird.

Diese Empfehlung der OECD setzt die Schweiz durch Artikel 4 Absatz 2 StAhiG um, wonach Amtshilfeverfahren zügig durchzuführen sind, sowie durch Artikel 5 Absatz 2 StAhiG i.V.m. Artikel 22a Absatz 1 VwVG, wonach Gerichtsferien nicht anwendbar sind.

b) Peer review

Das Global Forum überprüft die Erfüllung der eingegangenen Verpflichtungen zur Steueramtshilfe und die Umsetzung des Standards in Länderexamen (sog. Peer Reviews).

Peer Reviews gliedern sich in zwei Phasen. In Phase 1 (Legal and Regulatory Framework) untersucht das Global Forum, ob die nötigen Rechtsgrundlagen des jeweiligen Mitgliedstaates für den Informationsaustausch nach dem OECD-Standard vorhanden sind. Nur Staaten, welche die Phase 1 bestehen, können in die Phase 2 (Implementation of the Standard) eintreten. In der Phase 2 wird die Anwendung des Informationsaustauschs, d.h. die Amtshilfepraxis der letzten 3 Jahre geprüft. Die Phase 2 gliedert sich in zwei Runden, in welchen die rechtliche wie auch die praktische Umsetzung des OECD-Standards geprüft wird. Die erste Runde fand für sämtliche OECD-Mitgliedstaaten von 2010-2016 statt und endete für die Schweiz im Juli 2016 mit der Bewertung der Amtshilfepraxis mit der Beurteilung „largely compliant“. Somit ist die Amtshilfepraxis der Schweiz weitgehend konform mit dem OECD-Standard.

Die Schweiz befindet sich derzeit in der zweiten Runde der Phase 2, welche sich auf den Beurteilungszeitraum vom 1. Juli 2015 bis 30. Juni 2018 bezieht. Die Schweiz hat dazu zu Beginn des Jahres 2019 einen Fragebogen („the Peer Questionnaire“) ausgefüllt und diesen zuhanden der OECD eingereicht. Gleichzeitig waren jene Mitgliedstaaten, welche mit der Schweiz in einem EOI-Austausch stehen, gehalten, ebenfalls einen Fragebogen im Sinne eines sog. Peer Inputs zu beantworten. Die Schweiz hat von gut 30 Partnerstaaten Rückmeldungen erhalten. In einem nächsten Schritt wird vom 13.-17. Mai

2019 die Besichtigung vor Ort stattfinden. Dabei wird das Prüfungs-Team, bestehend aus Vertretern der Global Forum-Mitgliedstaaten sowie Mitgliedern des Global Forum-Sekretariats, die Schweiz besuchen. Diese sog. on-site visit ist ein wichtiger Aspekt des Peer Reviews. Sie gewährt dem geprüften Mitgliedstaat die Möglichkeit, an seiner eigenen Evaluation teilzunehmen und erlaubt einen offenen, konstruktiven und effizienten Dialog mit dem Assessment-Team. Sog. face-to-face Dialoge helfen Missverständnisse zu verhindern und erhöhen die Qualität des Entwurf-Berichts. Im Anschluss an die vor-Ort-Besichtigung erarbeitet das OECD-Sekretariat so rasch als möglich einen Entwurf-Bericht, zu welchem sich sowohl die Assessoren als auch die Schweiz äussern können. Anlässlich des PRG-Meetings im Dezember 2019 wird der Entwurf-Bericht besprochen. Der Peer Review Report wird danach zu Beginn des Jahres 2020 an das Global Forum zur Genehmigung weitergeleitet.

VI. Stellung der Bank im Verfahren

1. Editionsfrist

Die Editionsfrist für die Lieferung der Informationen beträgt in der Regel für sämtliche Informationsinhaber 10 Tage. Die ESTV gewährt je nach Umfang der zu liefernden Informationen auf Gesuch hin Fristerstreckungen.

Bei Gruppenersuchen und den sog. Masseneinzelersuchen, bei welchen für eine grosse Anzahl von betroffenen Personen Informationen erfragt werden, wird die Frist nach Aufwand vereinbart.

2. Grundsatz: Keine Parteistellung

Die Banken haben wie alle Informationsinhaber gemäss Artikel 10 StAhiG keine Parteistellung, da sie nur Auskünfte über ihre Kunden erteilen müssen und dadurch nicht in den eigenen Interessen bzw. Aktivitäten betroffen sind. Anders verhält es sich nur, wenn im Einzelfall die Bank selbst durch die Übermittlung der Kundendaten betroffen ist.

Eine Ausnahme statuierte das Bundesverwaltungsgericht mit Urteil vom 25. Oktober 2016. Dort wurde der Bank Parteistellung eingeräumt. Die Gründe dafür waren, dass

- eine hohe, im fünfstelligen Bereich liegende Zahl Konten betroffen waren,
- davon auszugehen war, dass die Ergreifung eines Rechtsmittels gegen Schlussverfügungen der ESTV einen allfälligen Reputationsschaden der Bank zumindest hätte mindern können,

– die Aufbereitung von Datensätzen im fünfstelligen Bereich, die Information mehrerer tausend Kunden und die (über die reine Informationsbeschaffung hinausgehende) Einrichtung einer Hotline für Kunden, wie sie der betreffenden Bank von der ESTV vorgeschrieben wurden, über dem gewöhnlich für ein Amtshilfeverfahren zu treibenden Aufwand liegen, die ein Informationsinhaber auf sich nehmen muss,
– aufgrund des gegen Gesellschaften des Konzerns laufenden Strafverfahrens nicht auszuschliessen war, dass sich die schweizerische Bank mit Erfolg auf das Verbot berufen kann, sich selbst belasten zu müssen, zumal konkrete Umstände Zweifel an der Einhaltung des Spezialitätsprinzips erweckten.

3. Arten der erfragten Informationen

Der Informationsinhaber ist herausgabepflichtig, wenn sich die Informationen in der eigenen faktischen oder rechtlichen Kontrollsphäre befinden. Nach internationalem Amtshilfestandard (Art. 26 Abs. 5 OECD-MA, Art. 5 Abs. 4 TIEA-MA) kann das Bankgeheimnis der Pflicht zur Amtshilfeleistung nicht entgegengehalten werden.

Die Art und der Umfang der Unterlagen kann je nach Ersuchen stark variieren. Namentlich Konto- und Depoteröffnungsunterlagen, Formulare über die wirtschaftliche Berechtigung, Informationen zur Zeichnungsberechtigung, Unterschriftenkarten, Ausweispapiere, Konto- und Depotauszüge, Detailbelege zu einzelnen Transaktionen, Korrespondenz zwischen Bank und Bankkunde und Unterlagen zu den geführten Geschäften müssen herausgegeben werden. Insbesondere im Rahmen der US-Amtshilfe umfassen die erfragten Bankdokumente meist über mehrere 1'000 Seiten pro Amtshilfefall. Allgemein kann festgehalten werden, dass bei Gruppenersuchen und Masseneinzelersuchen jeweils relativ einfache Informationen erfragt werden.

Die Banken liefern die Informationen in guter Qualität und innert kurzer Zeit. Ohne dieses kooperative Verhalten wäre eine effiziente Amtshilfeleistung nicht möglich.

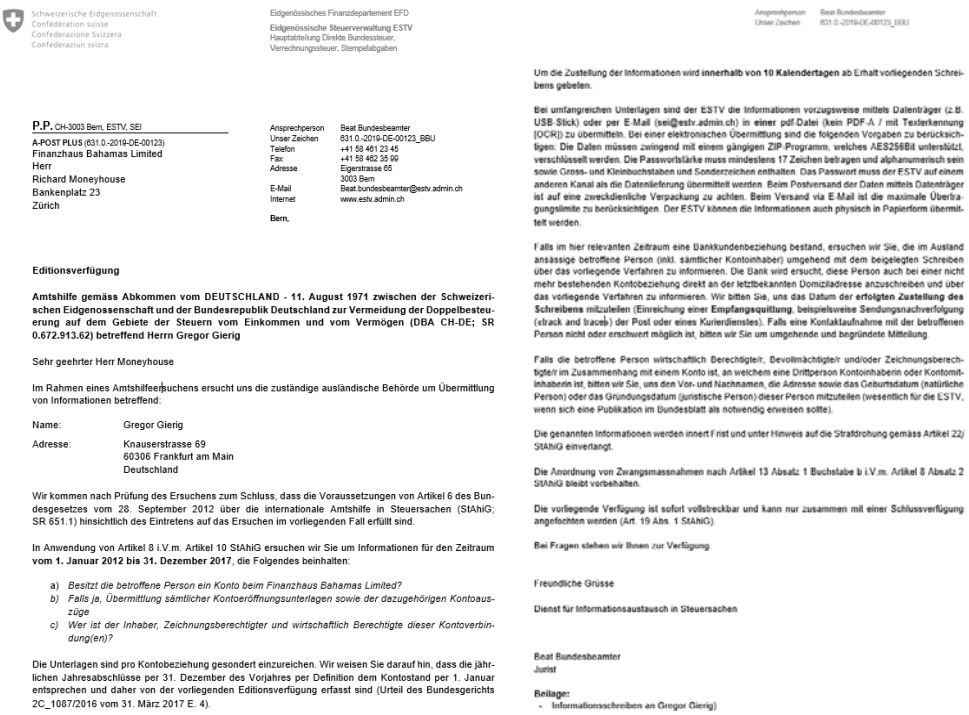
4. Notifikation der vom Amtshilfeverfahren betroffenen Person

Wenn die beschwerdeberechtigte Person den Wohnsitz resp. den Sitz im Ausland hat, gelangt die ESTV unter Fristansetzung an die Bank als Informationsinhaberin mit dem Ersuchen, die betroffene Person aufzufordern, in der Schweiz einen Zustellungsbevollmächtigten zu bezeichnen. Die ESTV legt in

diesen Fällen der Editionsverfügung Informationsschreiben bei, welche die Bank an die im Ausland ansässigen beschwerdeberechtigten Personen weiterzuleiten hat.

Die Information der Informationsinhaberin beruht auf der Erwartung, dass diese aufgrund ihrer vertraglichen Verpflichtungen gegenüber dem Kunden alles Notwendige unternimmt, um die beschwerdeberechtigte Person über ein laufendes Amtshilfeverfahren zu informieren.

5. Bsp. Editionsverfügung



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Eidgenössische Steuerverwaltung ESTV
Hauptabteilung Direkte Bundessteuer, Verrechnungssteuer, Stempelabgaben

Ansprechperson Beat Bundesbeamter
Unser Zeichen 631.0-2019-DE-00123_BBU

P.P. CH-3003 Bern, ESTV, SEI

A-POST PLUS (631.0.-2019-DE-00123)
Finanzhaus Bahamas Limited
Herr
Richard Moneyhouse
Bankenplatz 23
Zürich

Ansprechperson Beat Bundesbeamter
Unser Zeichen 631.0.-2019-DE-00123_BBU
Telefon +41 58 461 23 45
Fax +41 58 462 35 99
Adresse Eigerstrasse 65
3003 Bern
E-Mail Beat.bundesbeamter@estv.admin.ch
Internet www.estv.admin.ch

Bern,

Editionsverfügung

Amtshilfe gemäss Abkommen vom DEUTSCHLAND - 11. August 1971 zwischen der Schweizerischen Eidgenossenschaft und der Bundesrepublik Deutschland zur Vermeidung der Doppelbesteuerung auf dem Gebiete der Steuern vom Einkommen und vom Vermögen (DBA CH-DE; SR 0.672.913.62) betreffend Herrn Gregor Gierig

Sehr geehrter Herr Moneyhouse

Im Rahmen eines Amtshilfeersuchens ersucht uns die zuständige ausländische Behörde um Übermittlung von Informationen betreffend:

Name: Gregor Gierig

Adresse: Knauserstrasse 69
60306 Frankfurt am Main
Deutschland

Wir kommen nach Prüfung des Ersuchens zum Schluss, dass die Voraussetzungen von Artikel 6 des Bundesgesetzes vom 28. September 2012 über die internationale Amtshilfe in Steuersachen (StAhiG; SR 651.1) hinsichtlich des Eintretens auf das Ersuchen im vorliegenden Fall erfüllt sind.

In Anwendung von Artikel 8 i.V.m. Artikel 10 StAhiG ersuchen wir Sie um Informationen für den Zeitraum **vom 1. Januar 2012 bis 31. Dezember 2017**, die Folgendes beinhalten:

a) *Besitzt die betroffene Person ein Konto beim Finanzhaus Bahamas Limited?*
b) *Falls ja, Übermittlung sämtlicher Kontoeröffnungsunterlagen sowie der dazugehörigen Kontoauszüge*
c) *Wer ist der Inhaber, Zeichnungsberechtigter und wirtschaftlich Berechtigte dieser Kontoverbindung(en)?*

Die Unterlagen sind pro Kontobeziehung gesondert einzureichen. Wir weisen Sie darauf hin, dass die jährlichen Jahresabschlüsse per 31. Dezember des Vorjahres per Definition dem Kontostand per 1. Januar entsprechen und daher von der vorliegenden Editionsverfügung erfasst sind (Urteil des Bundesgerichts 2C_1087/2016 vom 31. März 2017 E. 4).

Ansprechperson Beat Bundesbeamter
Unser Zeichen 631.0.-2019-DE-00123_BBU

Um die Zustellung der Informationen wird **innerhalb von 10 Kalendertagen** ab Erhalt vorliegenden Schreibens gebeten.

Bei umfangreichen Unterlagen sind der ESTV die Informationen vorzugsweise mittels Datenträger (z.B. USB-Stick) oder per E-Mail (sei@estv.admin.ch) in **einer** pdf-Datei (kein PDF-A / mit Texterkennung [OCR]) zu übermitteln. Bei einer elektronischen Übermittlung sind die folgenden Vorgaben zu berücksichtigen. Die Daten müssen zwingend mit einem gängigen ZIP-Programm, welches AES256Bit unterstützt, verschlüsselt werden. Die Passwortstärke muss mindestens 17 Zeichen betragen und alphanumerisch sein sowie Gross- und Kleinbuchstaben und Sonderzeichen enthalten. Das Passwort muss der ESTV auf einem anderen Kanal als die Datenlieferung übermittelt werden. Beim Postversand der Daten mittels Datenträger ist auf eine zweckdienliche Verpackung zu achten. Beim Versand via E-Mail ist die maximale Übertragungslimite zu berücksichtigen. Der ESTV können die Informationen auch physisch in Papierform übermittelt werden.

Falls im hier relevanten Zeitraum eine Bankkundenbeziehung bestand, ersuchen wir Sie, die im Ausland ansässige betroffene Person (inkl. sämtlicher Kontoinhaber) umgehend mit dem beigelegten Schreiben über das vorliegende Verfahren zu informieren. Die Bank wird ersucht, diese Person auch bei einer nicht mehr bestehenden Kontobeziehung direkt an der letztbekannten Domiziladresse anzuschreiben und über das vorliegende Verfahren zu informieren. Wir bitten Sie, uns das Datum der **erfolgten Zustellung des Schreibens** mitzuteilen (Einreichung einer **Empfangsquittung**, beispielsweise Sendungsnachverfolgung («track and trace») der Post oder eines Kurierdienstes). Falls eine Kontaktaufnahme mit der betroffenen Person nicht oder erschwert möglich ist, bitten wir Sie um umgehende und begründete Mitteilung.

Falls die betroffene Person wirtschaftlich Berechtigte/r, Bevollmächtigte/r und/oder Zeichnungsberechtigte/r im Zusammenhang mit einem Konto ist, an welchem eine Drittperson Kontoinhaberin oder Kontoinhaberin ist, bitten wir Sie, uns den Vor- und Nachnamen, die Adresse sowie das Geburtsdatum (natürliche Person) oder das Gründungsdatum (juristische Person) dieser Person mitzuteilen (wesentlich für die ESTV, wenn sich eine Publikation im Bundesblatt als notwendig erweisen sollte).

Die genannten Informationen werden innert Frist und unter Hinweis auf die Strafdrohung gemäss Artikel 22/ StAhiG einverlangt.

Die Anordnung von Zwangsmassnahmen nach Artikel 13 Absatz 1 Buchstabe b i.V.m. Artikel 8 Absatz 2 StAhiG bleibt vorbehalten.

Die vorliegende Verfügung ist sofort vollstreckbar und kann nur zusammen mit einer Schlussverfügung angefochten werden (Art. 19 Abs. 1 StAhiG).

Bei Fragen stehen wir Ihnen zur Verfügung.

Freundliche Grüsse

Dienst für Informationsaustausch in Steuersachen

Beat Bundesbeamter
Jurist

Beilage:
- Informationsschreiben an Gregor Gierig)

VII. Bankmitarbeiter

1. Entscheidgrundlagen

Die ESTV hat beim Vollzug der internationalen Amtshilfe in Steuersachen Bestimmungen aus verschiedenen Rechtsquellen zu beachten. Es sind dies insbesondere das einschlägige Doppelbesteuerungsabkommen, das Steueramtshilfegesetz, das Verwaltungsverfahrensgesetz und das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1).

Weder das Verwaltungsverfahrens- noch das Datenschutzgesetz wurden mit Blick auf internationale Amtshilfeverfahren verabschiedet. Sie sind als allgemeine Grundlagen dennoch auch im Amtshilfeverfahren anwendbar. Die

Bestimmungen der verschiedenen Gesetze können aber bei der Anwendung in Widerspruch zueinander geraten. Dabei muss die ESTV die Amtshilfe so vollziehen, dass durch Auslegung die gesetzlichen Bestimmungen eingehalten werden und der Wille des Gesetzgebers befolgt wird. Konkret müssen die internationalen Verpflichtungen der Schweiz im Bereich der internationalen Amtshilfe in Steuersachen erfüllt werden, gleichzeitig sind aber auch die rechtsstaatlichen Prinzipien des Verwaltungsverfahrens einzuhalten.

Vor diesem Hintergrund ist die Praxis der ESTV betreffend die Rechtsstellung von Bankmitarbeitenden im internationalen Amtshilfeverfahren zu sehen.

2. Schwärzungen

Gestützt auf das einschlägige Doppelbesteuerungsabkommen müssen in der internationalen Amtshilfe in Steuersachen alle voraussichtlich erheblichen Informationen übermittelt werden. Ob eine Information erheblich ist, kann in der Regel nur der ersuchende Staat abschliessend feststellen, weshalb der ersuchte Staat nur Informationen von der Amtshilfe ausschliessen darf, die mit Sicherheit nicht erheblich sind (vgl. statt vieler Urteil des Bundesverwaltungsgerichts A-4695/2015 vom 2. März 2016 E. 9.1 m.w.H.).

Gemäss Artikel 4 Absatz 3 StAhiG ist die Übermittlung von Informationen zu nicht betroffenen Personen unzulässig, wenn diese Informationen für die Beurteilung der Steuersituation der betroffenen Person nicht voraussichtlich relevant sind oder wenn berechtigte Interessen von nicht betroffenen Personen das Interesse der ersuchenden Seite an der Übermittlung der Informationen überwiegen.

Gemäss bundesgerichtlicher Rechtsprechung hat sich die Auslegung des in Artikel 4 Absatz 3 StAhiG verwendeten Begriffs der nicht betroffenen Person massgeblich nach dem Kriterium der voraussichtlichen Erheblichkeit zu richten. Eine zu extensive Auslegung und daraus resultierende restriktive Übermittlungspraxis ist zu vermeiden, da eine solche den Zweck des Abkommens vereiteln würde (vgl. dazu BGE 141 II 436 E. 4.4 f.). Dementsprechend dürfen im Rahmen der Amtshilfe beispielsweise in Kontoauszügen enthaltene Drittpersonendaten übermittelt werden (vgl. dazu BGE 142 II 161 E. 4.6.2).

Den klassischen Amtshilfeersuchen betreffend Bankinformationen liegt der Verdacht zugrunde, dass die formell vom Ersuchen betroffene Person in der Schweiz gelegene Bankkonten nicht deklariert und somit Steuern hinter-

zogen hat. Sofern im Rahmen der Amtshilfeleistung Bankunterlagen übermittelt werden, schwärzt die ESTV allfällige Namen von Bankmitarbeitenden. Grund hierfür ist, dass der ersuchende Staat nicht explizit um diese Personendaten ersucht und sich diese nicht als voraussichtlich erheblich für die Beurteilung der Steuersituation der formell vom Ersuchen betroffenen Person erweisen (vgl. dazu Art. 4 Abs. 3 StAhiG).

Im Gegensatz zu den OECD-standardkonformen Doppelbesteuerungsabkommen der Schweiz setzt Artikel 26 DBA CH-US 1996 für den Informationsaustausch in Steuersachen im Verhältnis Schweiz – USA einen Verdacht auf die Begehung von «Betrugsdelikten und dergleichen» voraus. Gemäss konstanter Rechtsprechung durften in solchen Betrugsfällen sämtliche Bankunterlagen betreffend die Errichtung, Führung und Verwaltung von Konten US-amerikanischer Steuerpflichtiger und mit ihnen verbundenen juristischen Personen übermittelt werden (vgl. statt vieler Urteil des Bundesverwaltungsgerichts A-6933/2010 vom 17. März 2011 E. 10; Urteil des Bundesverwaltungsgerichts A-6684/2010 vom 4. Juli 2011 E. 2.4 f.). Die Übermittlung der in den ersuchten Bankunterlagen enthaltenen Namen von Drittpersonen durfte nur dann verweigert werden, wenn diese offensichtlich nicht in die dem Amtshilfeersuchen zugrundeliegende Angelegenheit verwickelt waren (vgl. dazu BGE 139 II 451 E. 2.3.3). Gestützt auf diese Rechtsprechung wurden dem Internal Revenue Service (IRS) auch Daten zu Bankmitarbeitenden und weiteren Drittpersonen übermittelt.

In einem neueren Urteil hielt das Bundesgericht fest, dass die Namen von Bankmitarbeitenden, Rechtsanwälten und Notaren zu schwärzen sind, es sei denn, der IRS ersuche explizit um diese Personendaten und könne darlegen, inwiefern sich diese als notwendig für die Ahndung von «Betrugsdelikten und dergleichen» erweisen (vgl. dazu BGE 144 II 29 E. 4.3). Seither verlangt der IRS ausdrücklich diese Personendaten und begründet deren voraussichtliche Erheblichkeit. In den Fällen, in denen ein solch explizites Gesuch zu den zusätzlichen Personendaten gestellt wird, übermittelt die ESTV dem IRS dieselben Informationen, wie sie vor dem genannten Bundesgerichtsentscheid übermittelt wurden. Darunter befinden sich auch Daten zu Drittpersonen wie z.B. Bankmitarbeitenden.

Würde die ESTV solche voraussichtlich erheblichen Drittpersonendaten schwärzen, würde damit eine Verletzung der mit Artikel 26 DBA CH-US 1996 durch die Schweiz eingegangenen völkerrechtlichen Verpflichtungen einhergehen.

3. Parteistellung

Gemäss bundesgerichtlicher Rechtsprechung ist die Beschwerdebefugnis für bloss indirekt betroffene Personen, die zwar in den erhobenen Unterlagen erwähnt werden, aber nicht direkt von Zwangsmassnahmen betroffen bzw. Inhaber von sichergestellten Dokumenten sind, grundsätzlich zu verneinen (vgl. dazu BGE 139 II 404 E. 11.1; vgl. auch Urteil des Bundesverwaltungsgerichts A-5506/2015 vom 31. Oktober 2016 E. 12.3). Gestützt auf diese Rechtsprechung räumte die ESTV solchen Drittpersonen grundsätzlich keine Parteistellung ein.

In einem neueren Urteil hat das Bundesgericht einer Drittperson Parteistellung eingeräumt, die sich in einem konkreten Verfahren an die ESTV gewendet hat und einer sie betreffenden Datenübermittlung widersetzen wollte (vgl. dazu BGE 143 II 506). Gleichzeitig hat das Gericht aber auch festgehalten, dass die Einräumung der Parteistellung nicht dazu führen darf, dass die Amtshilfeleistung dadurch auf unzulässige Weise verhindert bzw. übermässig verzögert wird (vgl. dazu BGE 143 II 506 E. 5.3).

Würde die ESTV Drittpersonen von Amtes wegen Parteistellung einräumen, müsste in einer Vielzahl von Amtshilfefällen eine so grosse Anzahl von Personen informiert werden, dass die Amtshilfe dadurch auf unzulässige Weise verhindert bzw. übermässig verzögert würde. Beispielhaft kann hier auf die US-Amtshilfe verwiesen werden, in der die ersuchte Bankdokumentation mehrere tausend Seiten pro Amtshilfefall umfassen kann. Entsprechend können in der ersuchten Bankdokumentation auch Daten zu Hunderten von Drittpersonen enthalten sein. Im Ergebnis würden mit der Einräumung der Parteistellung von Amtes wegen die internationalen Verpflichtungen der Schweiz verletzt.

Entsprechend räumt die ESTV Drittpersonen nur auf Antrag in einem konkreten Verfahren Parteistellung ein. Hingegen werden Drittpersonen nicht von Amtes wegen über ein laufendes Amtshilfeverfahren informiert. Gesuche um Einräumung der Parteistellung in einem allfälligen zukünftigen Amtshilfeverfahren werden gleichermassen abgewiesen.

Die ESTV hat den Schweizerischen Bankpersonalverband (SBPV), den Arbeitgeberverband der Banken in der Schweiz (AGV Banken) und die Schweizerische Bankiervereinigung (SBVg) über die aktuelle Praxis der ESTV informiert.

VIII. Erwartete Entwicklungen

1. Amtshilfeübereinkommen (MAC)

Mit dem multilateralen Instrument des Amtshilfeübereinkommens (MAC) wurde die Anzahl der Partnerstaaten, mit denen die Schweiz nach internationalem Standard Informationen auf Ersuchen austauscht, bereits deutlich erhöht. Zusätzliche Amtshilfeersuchen gestützt auf das Amtshilfeübereinkommen (MAC) werden voraussichtlich ab dem Jahr 2019 bei der ESTV eingehen. Ausnahmsweise ist es bei Erfüllung der Voraussetzungen möglich, dass ein Ersuchen basierend auf das Amtshilfeübereinkommen auch für frühere Jahre gestellt werden kann. Es muss sich in einem solchen Ausnahmefall aber um ein vorsätzliches Verhalten handeln, welches der strafrechtlichen Verfolgung unterliegt (sog. «criminal»). Ist diese Voraussetzung gegeben, können die Staaten basierend auf dem Amtshilfeübereinkommen Informationen bereits ab dem Jahre 2014 erfragen. Im Jahr 2018 wurde auf ein paar wenige Fälle eingetreten, die diesen Sachverhalt erfüllten.

2. Gestohlene Daten

Das Bundesgericht führte in seinem Entscheid BGE 2C_648/2017 aus, dass einerseits die blosse Verwendung von illegal erworbenen Daten kein treuwidriges Verhalten darstelle und andererseits auch nicht davon ausgegangen werden könne, dass die alleinige Verwendung von illegal erworbenen Daten per se den Grundsatz von Treu und Glauben verletze. Die Thematik stellte sich im Zusammenhang mit Amtshilfeersuchen Indiens.

Unzulässig ist die Verwendung von illegal erworbenen Daten, wenn diese vom ersuchenden Staat gekauft wurden. Davon konnte jedoch im indischen Kontext nicht ausgegangen werden[4]. Ausserdem hat sich Indien im Doppelbesteuerungsabkommen nicht dazu verpflichtet, Angaben über die Herkunft der verwendeten Informationen abzugeben. Die Weigerung einer solchen Zusicherung ist somit nicht als treuwidriges Verhalten zu werten.

Zusammengefasst darf somit grundsätzlich auf Ersuchen eingetreten werden, die sich auf Daten aus dem Ausland mit deliktischem Ursprung stützen, solange sie der ersuchende Staat nicht gekauft hat und er nicht versichert hat, solche Daten nicht zu verwenden. Die Frage, ob ein Staat den Grundsatz von Treu und Glauben verletzt hat, ist dann nach den Umständen des Einzelfalls zu beurteilen.

[4] Vgl. rechtskräftiges Urteil des Bundesstrafgerichts vorn 27. November 2016, TPF 2016 28.

3. Gruppenersuchen basierend auf FATCA

Eine bereits seit mehreren Jahren von der Schweiz bzw. der ESTV erwartete Herausforderung sind die Gruppenersuchen basierend auf FATCA.

Das geltende Abkommen zwischen der Schweiz und den Vereinigten Staaten von Amerika über die Zusammenarbeit für eine erleichterte Umsetzung von FATCA (FATCA-Abkommen nach Modell 2; SR 0.672.933.63) sieht vor, dass die US-Steuerbehörden für bestimmte Konten Gruppenersuchen stellen können. Bis heute haben die US-Steuerbehörden keine solchen Gruppenersuchen gestellt. Denn das Änderungsprotokoll zum Abkommen zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika zur Vermeidung der Doppelbesteuerung auf dem Gebiet der Steuern vom Einkommen (DBA Schweiz–USA; SR 0.672.933.61) ist als dafür notwendige rechtliche Grundlage durch die USA nach wie vor nicht ratifiziert worden. Tritt das Änderungsprotokoll zum DBA Schweiz–USA in Kraft, sind FATCA-Gruppenersuchen ab dem Meldejahr 2014 möglich. Solche Gruppenersuchen müssen gemäss der Vorgabe innerhalb von 8 Monaten behandelt werden.

Im Moment sind jedoch Verhandlungen mit den USA im Gange, wonach ein FATCA-Abkommen nach Modell 1 (automatischer Informationsaustausch zwischen den Steuerbehörden) vereinbart werden soll.

4. Folgeersuchen im Zusammenhang mit SIA und AIA

Bereits im Jahr 2018 wurden vom SEI Folgeersuchen im Zusammenhang mit dem SIA und dem AIA bearbeitet. Der AIA wird dieses Jahr auf 18 zusätzliche Partnerstaaten ausgeweitet. Dies dürfte somit ein weiteres Ansteigen der Ersuchen zur Folge haben, da die Partnerstaaten über mehr Informationen verfügen, die als Grundlage für Amtshilfeersuchen dienen können.

IX. Schlusswort

Der Vollzug der Amtshilfe bleibt eine anspruchsvolle Aufgabe. Die internationalen Entwicklungen lassen eine weitere Zunahme der Ersuchen erwarten. Zwischen internationalen Verpflichtungen der Schweiz und einzelnen Bestimmungen in gewissen Gesetzen besteht ein Spannungsfeld. Es ist Aufgabe der Vollzugsbehörden, eine Praxis zu entwickeln, die diese Bestimmungen

respektiert und zugleich die internationalen Anforderungen erfüllt. Die bisherige Rechtsprechung der Gerichte hat dabei die Praxis der ESTV bzw. des SEI weitgehend gestützt.

Banken und ihre datenschutzrechtliche Verantwortlichkeit im Verkehr mit ihren Dienstleistern

David Rosenthal/Barbara Epprecht, Zürich*

* David Rosenthal, Konsulent, Homburger AG, Zürich, david.rosenthal@homburger.ch; Barbara Epprecht, Anwältin, Homburger AG, Zürich, barbara.epprecht@homburger.ch; dieser Aufsatz basiert auf einem Vortrag von David Rosenthal an der Schweizerischen Bankrechtstagung vom 8. März 2019 in Bern; von ihm existiert auch eine vertiefte, nicht bankenspezifische Abhandlung des Themas, die im Jusletter (<www.jusletter.ch>) erschienen ist (Fn. 4).

I. Ausgangslage

Was Banken als Finanzdienstleister ihrer Kunden zu tun haben und wie sie ihnen gegenüber dafür verantwortlich sind, ist in vielen Bereichen klar. Sie nehmen Zahlungsaufträge entgegen, führen diese aus, verwalten und investieren Vermögen und dokumentieren die Entwicklung der Kundenbeziehungen in ihren Kundendatenbanken. Sie haften dabei für die geschäftsübliche Sorgfalt und sind schwergewichtig im auftragsrechtlichen Bereich tätig.

Ebenso klar ist, dass sie hierbei ihrerseits eine ganze Bandbreite von Dienstleistungen weiterer Drittanbieter in Anspruch nehmen, sei es um durch diese Kooperationen Synergien besser zu nutzen, um externes Fachwissen beizuziehen oder weil sie gewisse Dienstleistungen nicht selber anbieten. Im Resultat sieht sich eine Bank mit einem dichtmaschigen Netz an Dienstleistungen und den damit einhergehenden Datenbearbeitungen, -bekanntgaben, und -rückflüssen jeder erdenklichen Art konfrontiert. Dieses gilt selbstverständlich geregelt zu werden.

Stand in der Vergangenheit das Bankgeheimnis im Zentrum und damit die Frage, ob es sich bei einem Dienstleister im Sinne von Art. 47 Bankengesetz (**BankG**) um einen «Beauftragten» der Bank handelt oder nicht, rückt in jüngster Zeit insbesondere seit der EU-Datenschutzgrundverordnung (**DSGVO**) immer stärker auch die Frage nach der datenschutzrechtlichen Qualifikation solcher Dienstleistungsbeziehungen in den Fokus. Hier gelten jedoch andere Regeln als im Falle des Bankgeheimnisses, und sie sind – wie noch zu zeigen sein wird – etwas komplexer. Um den Anforderungen des Datenschutzes gerecht zu werden, ist es daher nicht nur entscheidend, dass eine Bank genau weiss, wo ihre Daten hingehen und wer diese wie bearbeitet, sondern auch in welcher Rolle sie und ihre Dienstleister hierbei tätig sind. Danach richtet sich auch ihre datenschutzrechtliche Verantwortlichkeit aus. Dieselben Fragen stellen sich im Übrigen auch mit Bezug auf ihr Verhältnis zu ihren Kunden, gegenüber welchen die Bank ihrerseits Dienstleisterin ist.

Die DSGVO aber auch das derzeit in Revision befindliche Datenschutzgesetz (**DSG**), welches aktuell im Entwurf dem Bundesrat vorliegt und frühestens 2020 verabschiedet wird (**E-DSG**), unterscheiden dabei zwischen dem

Verantwortlichen (oder auch *Controller* genannt) einerseits und dem **Auftragsbearbeiter** (oder auch *Processor* genannt)[1] andererseits. Weil die meisten datenschutzrechtlichen Pflichten an eine der beiden Rollen anknüpfen, ist ein klares Verständnis der für die Rollenzuteilung ausschlaggebenden Faktoren von grundlegender Bedeutung. Welche Partei Verantwortliche und welche Auftragsbearbeiterin ist, sollte daher bei jeder Datenbearbeitung, an der zwei oder mehrere Parteien involviert sind, bereits in deren Planungsphase geklärt werden. Der Vollständigkeit halber sei erwähnt, dass es auch noch eine dritte Rolle gibt, die nur in der DSGVO ausdrücklich definiert ist[2] und all jene umfasst, die wie Mitarbeiter und extern beigezogene Personen im Betrieb des Verantwortlichen oder Auftragsbearbeiters unter dessen Aufsicht tätig sind.[3]

Dieser Beitrag bietet eine Orientierungshilfe für die Beantwortung ebendieser Frage und nimmt dabei konkret Bezug auf Dienstleistungen, die den Bankenalltag bestimmen.[4] Nachdem das datenschutzrechtliche Grundkonzept der verschiedenen Beteiligten (Datensubjekt, Verantwortlicher und Auftragsbearbeiter, respektive Unter-Auftragsbearbeiter) (Kapitel II) sowie die einzelnen Merkmale der datenschutzrechtlichen Verantwortlichkeit (Kapitel III) genauer beleuchtet worden sind, werden ebendiese Rollen anhand bankentypischer Anwendungsfälle, wie z.B. das Abwickeln von Zahlungsaufträgen oder die Ausübung von Sorgfaltspflichten im Zusammenhang mit dem Geldwäschereigesetz, zugeteilt (Kapitel IV). Den Abschluss bilden einige praktische Empfehlungen für die konkrete Regelung und Pflege der Beziehung zwischen den Banken und ihren Dienstleistern (Kapitel V).

II. Datenschutzrechtliches Grundkonzept

1. Auslagerung von Datenbearbeitungen an Auftragsbearbeiter

Jede Datenbearbeitung involviert eine oder mehrere betroffene Personen. Sie werden auch Datensubjekte genannt. Es handelt sich dabei um diejenigen Personen, auf die sich die Personendaten beziehen, die bearbeitet werden.[5] Im

---

1 Im Bereich der DSGVO ist von Auftragsdatenverarbeiter die Rede. Die Bedeutung ist dieselbe.

2 Im DSG finden die Regeln für Auftragsbearbeiter auf sie analog Anwendung.

3 Art. 29 DSGVO.

4 Eine vertiefte Analyse mit sehr viel mehr Beispielen findet sich in DAVID ROSENTHAL, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter, 17. Juni 2019 (<www.jusletter.ch>).

5 Vgl. Art. 4 lit. b E-DSG; vgl. auch Art. 4 Bst. 1 DSGVO.

Bankenkontext sind das üblicherweise die Bankkunden[6]; aber auch Mitarbeiter der Bank gelten als betroffene Personen, wenn ihre Daten beispielsweise im Personaldossier bearbeitet werden oder in Kundendokumenten enthalten sind. Die Bank, konkret die jeweilige juristische Person oder deren Niederlassung, ist diesbezüglich – wie noch zu zeigen sein wird – typischerweise der Verantwortliche, der allein oder zusammen mit anderen Verantwortlichen über den Zweck und die Mittel der Daten entscheidet.[7] Der Verantwortliche einer Datenbearbeitung ist quasi der «Herr der Daten», d.h. es ist *seine* Datenbearbeitung. Daher ist in erster Linie er dafür verantwortlich, dass die Bestimmungen der anwendbaren Datenschutzgesetze eingehalten werden, und auch seitens der betroffenen Personen wird *er* als Ansprechperson wahrgenommen, sollten sie mit Bezug auf ihre Personendaten ein Anliegen haben.

Der Verantwortliche kann die Personendaten selber bearbeiten oder hierfür die Dienstleistung einer dritten Person in Anspruch nehmen. Dafür braucht er normalerweise auch keine Einwilligung der betroffenen Personen. Entscheidet die Bank beispielsweise, Daten bei einem IT-Anbieter in dessen Cloud zu speichern, so bearbeitet Letzterer die Daten im Auftrag und nach den Weisungen der Bank; in diesem Fall als Auftragsbearbeiter.[8] Solange der Auftragsbearbeiter sich an die Weisungen des Verantwortlichen hält und die Daten nur für ihn bearbeitet, bleibt es seine Datenbearbeitung.

In dieser Konstellation ist es üblich und gemäss DSGVO sogar ausdrücklich Pflicht, dass die Bank mit dem IT-Anbieter einen schriftlichen Auftragsdatenbearbeitungsvertrag (**ADV**) abschliesst und darin dem Auftragsbearbeiter klare Anweisungen gibt, wie dieser die Daten zu bearbeiten hat, nämlich nur so, wie er es als Verantwortlicher selber auch tun dürfte.[9] Das DSG ist hier weniger formal, aber es verlangt ebenfalls, dass der Verantwortliche sicherstellt, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie er dies selbst auch darf und die Datensicherheit gewährleistet bleibt.

Möchte sich der Auftragsbearbeiter seinerseits von einem externen Dienstleister unterstützen lassen, so handelt es sich dabei aus datenschutzrechtlicher Sicht um ein Unter-Auftragsbearbeitungsverhältnis, entsprechend ist der Dienstleister dann ein Unter-Auftragsbearbeiter (auch *Sub-Processor*

---

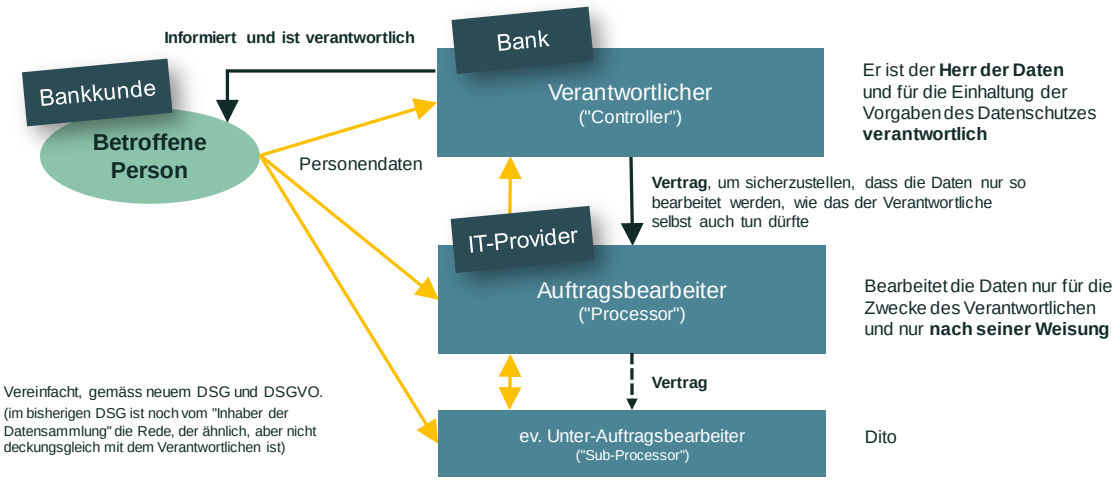
6 Während unter geltendem Datenschutzgesetz juristische Personen noch als Datensubjekte gelten (Art. 3 lit. b DSG), werden gemäss Art. 4 lit. b E-DSG nur noch natürliche Personen vom Anwendungsbereich des Gesetzes erfasst.

7 Vgl. Art. 4 lit. i E-DSG; vgl. auch Art. 4 Bst. 7 DSGVO.

8 Vgl. Art. 4 lit. j E-DSG; vgl. auch Art. 4 Bst. 8 DSGVO.

9 Vgl. Art. 8 E-DSG und Art. 28 DSGVO. Letzterer gibt einen Katalog mit acht definierten Punkten vor, welche in einem ADV abdeckt sein müssen (vgl. V.2).

genannt). In vertraglicher Hinsicht gelten hier dieselben Vorgaben wie zwischen dem Verantwortlichen und dem Auftragsbearbeiter; der Auftragsbearbeiter hat mit dem Unter-Auftragsbearbeiter einen ADV abzuschliessen oder ihn in seinen ADV mit dem Verantwortlichen aufzunehmen.[10]



2. Wer trägt welche Verantwortlichkeit

Der Katalog der datenschutzrechtlichen Pflichten, welche dem Verantwortlichen obliegen, gehen sehr viel weiter als diejenigen des (Unter-)Auftragsbearbeiters. Dies macht auch Sinn. Denn nur der Verantwortliche hat definitionsgemäss die Möglichkeiten, darüber zu entscheiden, ob und wie die Personendaten bearbeitet werden dürfen und damit hat auch nur er es faktisch und auch rechtlich in der Hand, diejenigen Faktoren zu kontrollieren, die einen entscheidenden Einfluss auf die Privatsphäre der betroffenen Personen haben können. Beteiligt sich ein Auftragsbearbeiter an diesen Entscheiden wird er – wie noch erläutert wird – selbst ebenfalls zum (Mit-)Verantwortlichen.

Gemäss DSGVO und dem E-DSG trägt der Verantwortliche folgende Pflichten:

– Sicherstellen, dass die allgemeinen datenschutzrechtlichen Grundsätze der Zweckbindung, Transparenz inkl. Informationspflichten, Verhältnis-

10 Gemäss DSGVO wird der Auftragsbearbeiter bereits im ADV mit dem Verantwortlichen verpflichtet, im Falle der Inanspruchnahme eines Unter-Auftragsbearbeiters diesem denselben Katalog von Pflichten aufzuerlegen (Art. 28 Abs. 3 Bst. d DSGVO).

mässigkeit hinsichtlich Umfang und Dauer der Datenbearbeitung, Datenrichtigkeit, Datensicherheit und Treu und Glauben eingehalten werden (Art. 5, 7 und 17 ff. E-DSG; Art. 5, 13 ff. und 32 DSGVO);

- Vorliegen – wo nötig – eines Rechtfertigungsgrundes nach revidiertem DSG respektive einer Rechtsgrundlage nach DSGVO (Art. 27 E-DSG; Art. 6 und 9 f. DSGVO);
- Nachweis, dass die datenschutzrechtlichen Vorgaben eingehalten sind (Art. 5 DSGVO);
- Einhalten der Vorgaben für die Übermittlung von Personendaten ins Ausland (Art. 13 ff. E-DSG; Art. 44 ff. DSGVO);
- Erfüllung der von den betroffenen Personen ausgeübten Rechte, insbesondere das Recht auf Auskunft, Löschung, Berichtigung und Einschränkung der Datenbearbeitung (Art. 23 und 28 E-DSG; Art. 12 und 15 ff. DSGVO);
- Einhaltung der Grundsätze von *Privacy by Default* und *Privacy by Design* (Art. 6 E-DSG; Art. 25 DSGVO);
- Durchführen einer Datenschutz-Folgeabschätzung und ggf. Konsultation der Datenschutzbehörde (Art. 20 f. E-DSG; Art. 35 f. DSGVO);
- Einhalten der gesetzlichen Vorgaben, insbesondere der Abschluss eines ADV und, falls nötig, die entsprechende Überwachung und Kontrolle, bei einer Übertragung der Datenbearbeitung an einen Auftragsbearbeiter (Art. 8 E-DSG; Art. 28 DSGVO);
- Meldung von Verletzungen der Datensicherheit (Art. 22 E-DSG; Art. 33 f. DSGVO);
- Bestellung eines betrieblichen Datenschutzbeauftragten und eines Vertreters im EWR (Art. 27 und 37 DSGVO);
- Führen eines Verzeichnisses der Bearbeitungstätigkeiten (Art. 11 E-DSG; Art. 30 DSGVO); und
- Kooperation mit den Datenschutzaufsichtsbehörden (z.B. Art. 21 f. E-DSG; Art. 58 DSGVO).

Im Gegensatz dazu sind die Pflichten, die das Gesetz dem Auftragsbearbeiter auferlegt, wesentlich schlanker gehalten:

- Gewährleistung der Datensicherheit (Art. 7 E-DSG; Art. 32 DSGVO);
- Einhalten der Vorgaben für die Übermittlung der Daten ins Ausland; inkl. allfälliger Informationspflichten (Art. 13 f. E-DSG; Art. 44 ff. DSGVO);

- Abschluss eines ADV, welcher wiederum diverse Pflichten vorsieht, u.a. auch der Unterstützung des Verantwortlichen (Art. 8 E-DSG; Art. 28 DSGVO);
- Meldung einer Verletzung der Datensicherheit (Art. 22 Abs. 3 E-DSG; Art. 33 Abs. 2 DSGVO);
- Bestellung eines betrieblichen Datenschutzbeauftragten und Vertreters im EWR (Art. 27 und 37 f. DSGVO);
- Führen eines Verzeichnisses der Bearbeitungstätigkeiten (Art. 11 E-DSG; Art. 30 DSGVO); und
- Kooperation mit den Datenschutzaufsichtsbehörden (z.B. Art. 21 f., 43 f. E-DSG; Art. 31 und 58 DSGVO).

Pflicht gemäss DSGVO (seit Mai 2018) und revidiertes DSG (ab 2020/21)	Verantwortlicher	Auftragsbearbeiter
Transparenz, Information der betroffenen Personen, Zweckbindung		
Verhältnismässigkeit (inkl. Datenminimierung, Dauer der Aufbewahrung)		
Rechtsgrundlage nach DSGVO, Rechtfertigungsgrund gemäss DSG		
Datenrichtigkeit		
Datensicherheit		
Rechenschaftspflicht betr. Einhaltung der Vorgaben		Unterstützung
Vorgaben für Übermittlungen ins Ausland		
Erfüllung der Rechte der betroffenen Personen (Auskunft, Löschung, etc.)		Unterstützung
Privacy by Default, Privacy by Design		
Durchführung von Datenschutz-Folgenabschätzungen		Unterstützung
Pflichten betr. Auftragsbearbeitung (Vertrag, etc.)		
Meldung von Verletzungen der Datensicherheit		
Bestellung eines betrieblichen Datenschutzbeauftragten nach DSGVO		
Verzeichnis der Bearbeitungstätigkeiten		
Kooperation mit den Aufsichtsbehörden		

3. Vorteile der Auftragsbearbeitung

Das dargelegte datenschutzrechtliche Grundkonzept ist einfach und entspricht vermutlich weitgehend der gelebten Praxis, sobald externe Dienstleister beigezogen werden. Dies ist denn auch nicht erstaunlich, birgt es für die Beteiligten doch viele Vorteile:

Erstens kann ein Verantwortlicher dem Auftragsbearbeiter seine Personendaten grundsätzlich «privilegiert» bekanntgeben. Das bedeutet, dass er hierfür keine Einwilligung der betroffenen Personen einholen oder einen anderen Rechtfertigungsgrund oder Rechtsgrundlage begründen muss.[11] Dies

[11] Dies gilt nur aber immerhin dann, wenn die Auslagerung der Datenbearbeitung mit den allgemeinen Grundsätzen des Datenschutzes, insbesondere dem Grundsatz der Verhält-

gilt deshalb, weil der Auftragsbearbeiter datenschutzrechtlich nicht als sogenannter «echter» Dritter gilt[12], sondern stattdessen zur Sphäre des Verantwortlichen hinzugezählt wird. Dank den im ADV abzusichernden Weisungs- und Kontrollrechten gegenüber dem Auftragsbearbeiter, kann der Verantwortliche den betroffenen Personen gegenüber weiterhin die Einhaltung des Datenschutzes garantieren. Demgegenüber ist die Weitergabe von Personendaten an einen anderen Verantwortlichen etwas komplizierter. So erfordert beispielsweise der Grundsatz der Transparenz, dass die Weitergabe der Daten für die Zwecke eines Dritten bei Erhebung der Daten gegenüber den betroffenen Personen zumindest erkennbar gemacht werden muss (was sich freilich aus der Natur des Bearbeitungszwecks ergeben kann[13]). In manchen Fällen kann die Weitergabe auch eine Zweckänderung bedeuten. Beides liesse sich nach dem E-DSG mit der Begründung eines Rechtfertigungsgrundes lösen. Nach DSGVO ist dies allerdings nicht möglich, erfordert doch jede Datenbearbeitung, also auch die Bekanntgabe, einen eigenen Rechtsgrund (wie beispielsweise eine Einwilligung, das Erfordernis einer Vertragsabwicklung, eine gesetzliche Pflicht oder ein berechtigtes Interesse).

Zweitens ist auch die vertragliche Umsetzung einfach und meist ohne grossen Widerstand der Dienstleister möglich, denn ADVs sind inzwischen weit verbreitet und stehen – ähnlich wie Allgemeine Geschäftsbedingungen – in standardisierter Form für jedermann frei zur Verfügung.[14]

Drittens kann der Auftragsbearbeiter, der eine Dienstleistung anbietet, seinerseits einen wesentlichen Teil des mit einer Datenbearbeitung verbundenen Haftungsrisikos auf den Verantwortlichen übertragen. Dies ist durchaus praktisch, da er so die vielen aufwändigen regulatorischen Anforderungen, die das Datenschutzrecht dem Verantwortlichen auferlegt (vgl. oben II.2) grösstenteils von sich abwenden kann; der Auftragsbearbeiter kann sich im

---

nismässigkeit und des angemessenen Schutzes der betroffenen Personen durch eine Gesetzgebung mit entsprechenden Garantien, einhergeht und, gemäss dem revidierten DSG, zumindest allgemein über eine Auslagerung vorgängig informiert worden ist.

12 Auch gemäss Art. 4 Bst. 10 DSGVO gilt der Auftragsbearbeiter nicht als Dritter. Die DSGVO äussert sich aber nicht ausdrücklich dazu, wie weit dieses Bekanntgabeprivileg geht.

13 Bei einem Zahlungsauftrag ist klar, dass eine Bank die nötigen Angaben zur Durchführung der Zahlung an weitere Stellen leiten muss (die dann datenschutzrechtlich als eigenständige Verantwortliche gelten).

14 Vgl. Beispiele von Vorlagen unter: <https://iapp.org/resources/article/sample-addendum-addressing-article-28-gdpr-and-incorporating-standard-contractual-clauses-for-controller-to-processor-transfers-of-personal-data/>; oder unter: <https://gdpr.eu/data-processing-agreement/>.

Wesentlichen darauf beschränken das zu tun, was der Verantwortliche ihm vorgibt und die Datensicherheit gewährleisten. So sind auch Konstellationen denkbar, in denen sich der Auftragsbearbeiter im Wissen um gewisse datenschutzrechtliche Schwächen seines Produkts (z.B. Software) mit der Übertragung der Hauptverantwortung auf den Verantwortlichen den möglichen Konsequenzen zu entziehen versucht.[15]

Angesichts dieser Vorteile, erstaunt es nicht, dass immer wieder Dienstleister fälschlicherweise als Auftragsbearbeiter qualifiziert werden. Denn weder das Vorliegen eines ADV noch eine anderweitige Überbindung der Haftung auf den Auftraggeber führt dazu, dass der Dienstleister seinerseits automatisch zum Auftragsbearbeiter wird. Was zählt sind die gelebten Verhältnisse. Für die Parteien ist es deshalb wichtig die Regeln zu kennen, auf die es bei der Rollenverteilung tatsächlich ankommt.

III. Wann ist der Dienstleister selbst Verantwortlicher

1. Allgemein

Nicht jede Dienstleistung, die für eine andere Partei erbracht wird, ist eine Auftragsbearbeitung; selbst dann nicht, wenn es sich rein vertragsrechtlich um ein Auftragsverhältnis handelt. Der Grund dafür ist, dass aus Perspektive des Datenschutzes andere Regeln gelten, die darüber entscheiden, wer in Bezug auf die Datenbearbeitung im «Lead» steht und dadurch auch gegenüber den betroffenen Personen geradestehen muss, etwa wenn diese eine Auskunft über ihre Daten wünschen oder Haftungsansprüche geltend machen wollen.

Ausgangspunkt für diese datenschutzrechtliche Beurteilung ist immer die der Dienstleistung zu Grunde liegende Datenbearbeitung. Viele Dienstleistungen setzen sich aus mehreren Datenbearbeitungsvorgängen zusammen und nicht selten kommt es vor, dass ein Dienstleister in Bezug auf gewisse Datenbearbeitungen Verantwortlicher und in Bezug auf andere Auftragsbearbeiter ist (vgl. III.5.c).

---

[15] Indem der Dienstleister eine Lösung entwickelt, die auch datenschutzwidrig eingesetzt werden kann, es aber dem Kunden überlässt, die nötigen Einstellungen vorzunehmen und zu bestimmen, wie sie benutzt wird. Regelmässig wird es auch dem Kunden überlassen zu beurteilen, ob die vom Dienstleister fix vorgegebene Datensicherheit für seine Anforderungen genügt, auch wenn dieser gar nicht das Fachwissen dazu hat. Hierbei kann es sich daher empfehlen, den Auftragsbearbeiter mindestens vertragsrechtlich nicht aus der Verantwortung zu lassen.

Vorweggenommen werden können zwei Aussagen, die der Natur der Sache nach auf jede Datenbearbeitung zutreffen: *Erstens* gibt es immer mindestens einen Verantwortlichen, sobald Personendaten bearbeitet werden und *zweitens* kann nur Auftragsbearbeiter sein, wer nicht selber in Bezug auf die gleiche Datenbearbeitung auch Verantwortlicher ist.

Die DSGVO wie auch der E-DSG definieren den Verantwortlichen als diejenige Partei, die über «die Zwecke und die Mittel» der Datenbearbeitung entscheidet.[16] Wer also entweder über den Zweck (dazu Kapitel III.2) der Datenbearbeitung oder deren Mittel – also die weiteren relevanten Parameter einer Datenbearbeitung (dazu Kapitel III.3) – entscheidet, kann nicht Auftragsbearbeiter sein, sondern ist immer selber Verantwortlicher. Verantwortlicher ist selbst diejenige Partei, die nicht alleine, sondern zusammen mit ihrem Auftraggeber über den Zweck oder die Mittel entscheidet. In diesem Fall handelt es sich um eine sogenannte gemeinsame Verantwortlichkeit (dazu Kapitel III.4).

2. Entscheid über die Zwecke der Bearbeitung

Jede Datenbearbeitung erfolgt für einen oder mehrere bestimmte «Zwecke». Der Zweck wurde von der Artikel-29-Datenschutzgruppe (einem Gremium der EU-Datenschutzbehörden[17]), die sich in einer Empfehlung ausführlich mit der Definition des Verantwortlichen und des Auftragsbearbeiters auseinandersetzt, als «erwartetes Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet» verstanden.[18] Der Zweck ist die Antwort auf die Frage, *weshalb* die Datenbearbeitung überhaupt stattfindet.[19] Entsprechend ist die Person, welche entscheidet, dass die Datenbearbeitung stattfindet und für welches Ziel diese erfolgt, diejenige Person, die über den Zweck bestimmt. Mit anderen Worten handelt es sich dabei um den Verantwortlichen.[20]

---

16 Art. 4 lit. i E-DSG; Art. 4 Bst. 7 DSGVO.

17 Die Datenschutzgruppe ging unter die DSGVO in den Europäischen Datenschutzausschuss (EDSA, <https://edpb.ero pa.eu/edpb_de>) über.

18 Vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 1|2010 zu den Begriffen «für die Verarbeitung Verantwortlicher» und «Auftragsverarbeiter» vom 16. Februar 2010 (WP 169), 16. Die Empfehlung erging noch unter dem alten Datenschutzrecht der EU, kann aber auch für die Auslegung der DSGVO herangezogen werden, da sich das Begriffsverständnis nicht verändert hat.

19 WP 169 (Fn. 18), 16.

20 WP 169 (Fn. 18), 16.

Es ist demnach weder entscheidend, woher die Personendaten stammen (d.h. ob diese beispielsweise von einem anderen Verantwortlichen oder einem anderen Auftragsbearbeiter zur Bearbeitung zu Verfügung gestellt worden sind) noch für wen das mit der Datenbearbeitung erzielte Resultat letztlich nützlich oder wer daran wirtschaftlich berechtigt ist. Entscheidend ist stattdessen, dass der Verantwortliche definiert, wie das Resultat erreicht werden soll; d.h. wie die Daten bearbeitet werden müssen, damit dieses entsprechend erreicht wird. Dies gilt auch dann, wenn das Resultat der Datenbearbeitung letzten Endes den Interessen eines anderen Verantwortlichen (das typische Beispiel hierfür ist der Anwalt, der für seinen Klienten tätig wird und dessen Informationen entsprechend seinem eigenen Wissen und Erfahrung bearbeitet, strategische Entscheide trifft etc.) oder einem Endnutzer (der Zeitungsabonnent, der den Artikel eines Journalisten liest, aber deswegen nicht zum Verantwortlichen wird) dient.

Entscheidend ist auch nicht, dass der Verantwortliche lediglich aufgrund eines konkreten Auftrags für eine andere Person eine Dienstleistung erbringt. Auch ein Dienstleister, der klare Anweisungen seines Auftraggebers hinsichtlich der Erfüllung seines Auftrags befolgt, kann Verantwortlicher sein, wenn er selbst die Datenbearbeitung veranlasst oder steuert, welchen Zwecken sie dient, es sei denn, der Auftraggeber lässt ihm durch konkrete Weisungen zur Datenbearbeitung keinen wirklichen Spielraum mehr und macht ihn so bloss zum Ausführenden.

Wird dies auf die Praxis umgesetzt, kann es zur Bestimmung der Verantwortlichkeit helfen, Dienstleistungen in die folgenden zwei Kategorien einzuteilen:

– *Datenbearbeitung ist die Dienstleistung*: Bei gewissen Dienstleistungen ist der Inhalt der zu erbringenden Dienstleistung mit der Datenbearbeitung identisch, wobei der Zweck der Datenbearbeitung sowohl vom Dienstleister als auch vom Kunden (oder von beiden gemeinsam) festgelegt werden kann. Ein Beispiel für eine solche Dienstleistung, bei welcher der Kunde den Zweck festlegt, ist die Speicherung und sonstige Bearbeitung von Daten in der Cloud; wozu der Kunde dies tut, ist seine Sache – der Dienstleister betreibt nur die Infrastruktur und stellt ihm deren Funktionalität ohne Vorgabe hinsichtlich des Nutzungszwecks zur Verfügung. Ein Beispiel für eine Dienstleistung, bei welcher der Dienstleister den Zweck definiert, sind die öffentlichen Social-Media-Plattformen: Er gibt vor, welche Datenbearbeitung stattfinden, und es ist «seine» Plattform, auch wenn die Nutzer entscheiden, wie sie sie nutzen wollen (was nicht ausschliesst, dass

sie diesbezüglich ebenfalls zu Verantwortlichen werden). Ist der Kunde selbst betroffene Person der Datenbearbeitung, muss der Dienstleister im Übrigen zwingend Verantwortlicher sein.[21]

– *Datenbearbeitung dient der Dienstleistung*: Bei anderen Dienstleistungen dient die Datenbearbeitung lediglich hilfsweise der eigentlichen Leistungserbringung (z.B. Abgabe von Investitionsempfehlungen durch Kundenberater, Ausführen eines Zahlungsauftrags).[22] In diesen Fällen tätigt der Dienstleister typischerweise seine eigene Datenbearbeitung und ist damit auch immer derjenige, der deren Zweck bestimmt.

Demnach kann der Dienstleister nur dann ein Auftragsbearbeiter sein, wenn die Datenbearbeitung vom Kunden veranlasst wird und deren Ausführung in der Folge an den Dienstleister delegiert wird. Werden dem Dienstleister hingegen lediglich Daten übertragen, weil die Ausführung seines Auftrags diese erfordert, und bestimmt er selbst, was er damit tut, dann stellt die Datenbearbeitung lediglich die Grundlage für das Erbringen der eigentlichen Leistung dar, ist also bloss Mittel zum Zweck. Mit anderen Worten findet zwar eine *Übertragung der Daten*, aber keine *Übertragung der Datenbearbeitung* statt. Folglich ist der Dienstleister als Verantwortlicher anzusehen.

Das Bayerische Landesamt für Datenschutzaufsicht hat einen illustrativen Katalog mit zahlreichen Beispielen von typischen Dienstleistungen und wann deren Erbringer als Auftragsbearbeiter oder Verantwortliche die Daten bearbeiten.[23] Darin wird mitunter erläutert, dass eine Auftragsbearbeitung nur dann vorliege, wenn eine Partei die Andere *im Schwerpunkt* mit einer Datenbearbeitung beauftragt (z.B. bei einer Auslagerung einer Back-up-Sicherheitsspeicherung), wohingegen bei der Inanspruchnahme einer fremden Fachleistung aus datenschutzrechtlicher Perspektive niemals die Datenbearbeitung an sich im Vordergrund stehen könne. Die deutsche Lehre spricht in diesem Zusammenhang auch von der Funktionsübertragungstheorie.[24] Diese

---

21 Ein Dienstleister kann nur Auftragsbearbeiter sein, wenn er die Daten eines Verantwortlichen bearbeitet. Der Kunde kann jedoch nicht Verantwortlicher der Bearbeitung seiner eigenen Daten sein. Begrifflich bezieht sich die Verantwortlichkeit immer auf die Bearbeitung von Daten dritter betroffener Personen.

22 Anstatt vieler: DAVID ROSENTHAL, Handkommentar DSG, Zürich 2008, Art. 10a N 14; ROLF SCHWARTMANN|MAXIMILIAN HERMANN, in: Schwartmann|Jaspers|Thüsing|Kugelmann (Hrsg.), Heidelberger Kommentar. Datenschutz-Grundverordnung Bundesdatenschutzgesetzt, Heidelberg 2018, Art. 4 N 134 f.

23 Bayerisches Landesamt für Datenschutzaufsicht, FAQ zur DS-GVO, abrufbar unter: <https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf>.

24 SCHWARTMANN|HERMANN (Fn. 22), Art. 4 N 134 f.

geht allerdings auf das alte deutsche Datenschutzrecht zurück und ist überholt, wie im Übrigen auch gewisse andere Ausführungen der Behörde. Trotzdem trifft ihre Qualifikation im Ergebnis in den meisten Fällen zu.[25] Unter der DSGVO nicht mehr richtig ist allerdings ihre Aussage, bei Prüfung und Wartung von IT-Systemen genüge die Möglichkeit des Zugriffs auf Personendaten, um einen Dienstleister zum Auftragsbearbeiter werden zu lassen:[26] Die Möglichkeit des Zugriffs stellt noch keine Datenbearbeitung dar. Greift der Dienstleister weisungswidrig trotzdem auf die Daten zu und bearbeitet sie, wird er zum Verantwortlichen. Das gilt auch für jeden Auftragsbearbeiter, der die Daten seines Kunden für eigene Zwecke oder sonst weisungswidrig bearbeitet. Das kann rechtlich durchaus gewollt sein: Der Hosting-Provider, der auf Verfügung einer Behörde hin Daten eines Kunden herausgibt, handelt diesbezüglich trotz seiner sonstigen Stellung als Auftragsbearbeiter als Verantwortlicher.

Daraus sind zwei weitere Folgerungen möglich: Für einen Dienstleister kann es erstens durchaus von Interesse sein, selbst als Verantwortlicher zu gelten, denn dies eröffnet ihm die Möglichkeit, die Personendaten seiner Kunden auch für eigene Zwecke zu verwenden und neue Nutzungszwecke einzuführen. Zweitens ist nicht ausschlaggebend, wie die Zuständigkeiten auf dem Papier geregelt sind: Entscheidend ist die *gelebte* Realität, wozu auch die Realität gehört, welche die betroffenen Personen wahrnehmen. Wer in ihren Augen im Zusammenhang mit einer Datenbearbeitung als primärer Ansprechpartner für datenschutzrechtliche Anliegen erscheint und dabei im eigenen Namen handelt, ist in der Regel auch Verantwortlicher.

3. Entscheid über die Mittel der Bearbeitung

Die «Mittel» einer Datenbearbeitung beziehen sich nicht auf die Personendaten an sich, sondern auf das *wie* und *auf welche Art* diese bearbeitet werden, um das beabsichtigte Ziel zu erreichen.[27] Hierbei können die Mittel in zwei Gruppen eingeteilt werden:

– Die *wesentlichen Mittel* einer Datenbearbeitung: Dabei handelt es sich um all jene Aspekte einer Datenbearbeitung, die – abgesehen von deren

25 Zahlreiche weitere Beispiele mit Erläuterungen finden sich in ROSENTHAL (Fn. 4).

26 Der Hinweis auf die Prüfung und Wartung geht auf eine Sonderbestimmung unter dem alten BDSG zurück, die jedoch mit der DSGVO hinfällig geworden ist. Vgl. zum Ganzen m.w.H.: JÜRGEN HARTUNG, in: Kühling|Buchner (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. Kommentar, 2. Aufl., München 2018, Art. 28 N 53.

27 WP 169 (Fn. 18), 16.

Zweck – entscheidend dafür sind, ob eine Datenbearbeitung den datenschutzgesetzlichen Vorgaben entspricht oder nicht. Dies beinhaltet beispielsweise Aspekte wie (i) welche Datenkategorien bearbeitet werden, (ii) deren Herkunft, (iii) welche Parteien Zugriff auf die Daten haben, (iv) wie lange die Daten bearbeitet und gespeichert werden sowie wann diese gelöscht werden, oder (v) in welche Länder die Daten übermittelt werden.

– *Alle anderen Mittel* einer Datenbearbeitung: Dies umfasst Aspekte der Datenbearbeitung, wie die verwendeten technischen Mittel (z.B. Hardwarelösung oder Applikation) sowie weitere technischen und organisatorischen Massnahmen, die getroffen werden (z.B. zulässige Datenformate, Prozesse wie auf Auskunftsbegehren geantwortet wird, mit welchen konkreten Vorkehrungen die erforderliche Datensicherheit erreicht wird).

Angesichts der Funktion der Figur des Verantwortlichen, nämlich die Einhaltung der datenschutzrechtlichen Grundsätze sicherzustellen, obliegen all jene Entscheide über die *wesentlichen* Mittel der Datenbearbeitung abschliessend dem Verantwortlichen. Demgegenüber kann auch ein Auftragsbearbeiter über *anderen* Mittel der Datenbearbeitung entscheiden, was in der Praxis auch oft vorkommt.[28] Das bedeutet, dass auch ein Auftragsbearbeiter entsprechend seinem Fachwissen, um das er letztlich auch ersucht wird, gewisse Entscheide, wie er seine Datenbearbeitung durchführt, selber treffen kann. Dies gilt aber nur soweit, als seine Entscheide keinen Einfluss auf die datenschutzrechtlich relevante Ausgestaltung der Datenbearbeitung (nicht Ausgestaltung deren Umsetzung) und damit letztlich auf die Rechte der betroffenen Personen haben. Mischt er sich in die Entscheide bezüglich der wesentlichen Mittel mit ein oder legt er diese – mangels eines vom Kunden abgesteckten Rahmens – selbst fest, wird er (auch wider Willen) ebenfalls zum Verantwortlichen.

Darum kann ein Auftragsbearbeiter selbst ebenfalls ein Interesse daran haben, dass der Kunde und nicht er die datenschutzrechtlichen Eckdaten der von ihm ausgeführten Bearbeitung festlegt, ADV hin oder her und egal, ob er die Daten nur für die Zwecke des Kunden bearbeitet. Solange eine Partei in Bezug auf die wesentlichen Mittel der Datenbearbeitung die tatsächliche (Mit-)Bestimmungshoheit hat, ist es auch unerheblich, ob sie faktischen Zugang zu den Personendaten hat oder nicht.[29]

---

28 WP 169 (Fn. 18), 16.

29 Urteil des EuGH vom 5. Juni 2019 (C-210|16) i.S. Wirtschaftsakademie Schleswig-Holstein.

4. Alleiniger oder gemeinsamer Entscheid über die Zwecke und Mittel

Dass ein Dienstleister Verantwortlicher ist, bedeutet noch nicht automatisch, dass der Auftraggeber nicht auch (Mit-)Verantwortlicher sein kann. Sind zwei verantwortliche Parteien involviert, gilt die Frage zu klären, ob diese *eigenständige* oder *gemeinsame* Verantwortliche sind. Je nachdem ist das Verhältnis zwischen den Parteien anders auszugestalten.

Legen zwei Verantwortliche gemeinsam den Zweck oder die wesentlichen Mittel der Datenbearbeitung fest, gelten sie als gemeinsame Verantwortliche (auch sogenannte **Joint-Controller**).[30] Demgegenüber sind mehrere Verantwortliche, die zwar Vertragspartner sein können, aber den Zweck und die wesentlichen Mittel der eigenen Datenbearbeitung festlegen, eigenständige Verantwortliche. Die Beziehung zwischen ihnen ist datenschutzrechtlich ein **Controller-Controller-Verhältnis**.

Um zu definieren, ob zwei Verantwortliche gemeinsam über Zweck oder Mittel entscheiden, muss in einem *ersten Schritt* die relevante Datenbearbeitung bestimmt werden. Gemäss der Artikel-29-Datenschutzgruppe gilt es dies auf Makro-Ebene zu entscheiden.[31] Demnach handelt es sich um ein und dieselbe Datenbearbeitung, falls – aus der Mikro-Ebene betrachtet – viele einzelne Bearbeitungsschritte aneinandergereiht zu einem logischen Ganzen zusammengefasst werden können.[32] Setzt eine Bank einen Dienstleister ein, der eine Finanztransaktion durchführt, so setzt sich die Datenbearbeitung in Bezug auf ebendiese Transaktion aus einzelnen Bearbeitungsschritten der Bank und aus Bearbeitungen des Übermittlungsdienstes zusammen. Wird jede dieser Datenbearbeitungen für sich betrachtet, erfolgen sie zwar je für die eigenen Zwecke der beteiligten Parteien, doch die einzelnen Bearbeitungsschritte sind miteinander so eng verknüpft und bilden ein logisches Ganzes. Für sich alleine betrachtet, haben sie demgegenüber kaum eigenständige Bedeutung.[33]

Die Ausführungen der Artikel-29-Datenschutzgruppe greifen allerdings etwas zu kurz. Zu berücksichtigen ist auch das sog. *Ebenenmodell*.[34] Neben der horizontalen Verkettung von Datenbearbeitungen muss geprüft werden, ob auch in vertikaler Hinsicht zwischen zwei Datenbearbeitungen eine logische

30 WP 169 (Fn. 18), 25.
31 WP 169 (Fn. 18), 25.
32 WP 169 (Fn. 18), 25.
33 Vgl. Beispiel 10: Finanztransaktionen, WP 169 (Fn. 18), 25.
34 Vgl. ROSENTHAL (Fn. 4), Abschnitt 14.

Einheit besteht, oder aber ob sie auf verschiedenen Ebenen stattfinden. Beispiel dafür ist die Datenbearbeitung durch einen Internet-Provider: Seine Datenbearbeitung – die Übermittlung der Datenströme seiner Kunden – findet auf der Netzwerkebene statt, während die Kunden auf Basis seiner Übermittlungsdienste eigenständige Datenbearbeitungen durchführen können (z.B. eine Vernetzung der Kundendatenverwaltung an zwei Betriebsstandorten). Die Datenbearbeitung – die Kundendatenverwaltung – findet auf der Applikationsebene statt. Die beiden Datenbearbeitungen überlagern sich, sind aber logisch zwei voneinander getrennte Einheiten.

In einem *zweiten Schritt* ist zu prüfen, ob entweder der Zweck oder die Mittel der betrachteten Datenbearbeitung von den Verantwortlichen gemeinsam festgelegt werden oder anders gesagt, ob an der Datenbearbeitung mehrere mitbestimmen. Hierbei ist zu entscheiden, wie viel gemeinsames Bestimmen notwendig ist, damit von einem Joint-Controllership gesprochen werden kann. Viel ist es nicht: Der Europäische Gerichtshof (**EuGH**) orientiert sich in einem Urteil vom 5. Juni 2018 i.S. Facebook Fanpages an einem breiten Begriff der gemeinsamen Verantwortlichkeit.[35] Dies wird mit dem bestmöglichen Schutz der betroffenen Personen begründet.[36] Konkret ging es darum, dass ein Unternehmen, welches auf Facebook eine Seite zur Eigenwerbung («Fanpage») betreibt, von Facebook in anonymisierter Form statistische Auswertungen der Benutzer ihrer Fanpage erhält. Das Unternehmen kann vorab auswählen, an welchen Auswertungen es konkret interessiert ist, z.B. ob es wissen möchte, welche Benutzer typischerweise die Seite besuchen. Der Gerichtshof kam zum Schluss, dass sich der Entscheid des Unternehmens an welchen Auswertungen es Interesse hat, auf die Erhebung der Personendaten durch Facebook auswirkt und das Unternehmen damit – obschon es keinen eigentlichen Zugang zu den Personendaten hat – den Zweck der Datenbearbeitung durch Facebook mitbestimmt.[37] Ein Mitbestimmen an der Datenbearbeitung durch die Beteiligten liegt vor, wenn der Zweck oder gewisse andere datenschutzrechtlich relevante Mittel der Datenbearbeitung gesteuert werden. Es muss sich im Minimum um eine Einflussnahme handeln, die in einer konkreten Datenbearbeitung resultiert. Dabei muss die Datenbearbeitung aber nicht zwingend unmittelbar gesteuert werden; eine mittelbare Einflussnahme reicht gemäss einem nur einen Monat später ergangenen weiteren Urteil des

35 Urteil des EuGH vom 5. Juni 2018 (C-210|16) i.S. Wirtschaftsakademie Schleswig-Holstein, Rz. 42.

36 Ebd., Rz. 42.

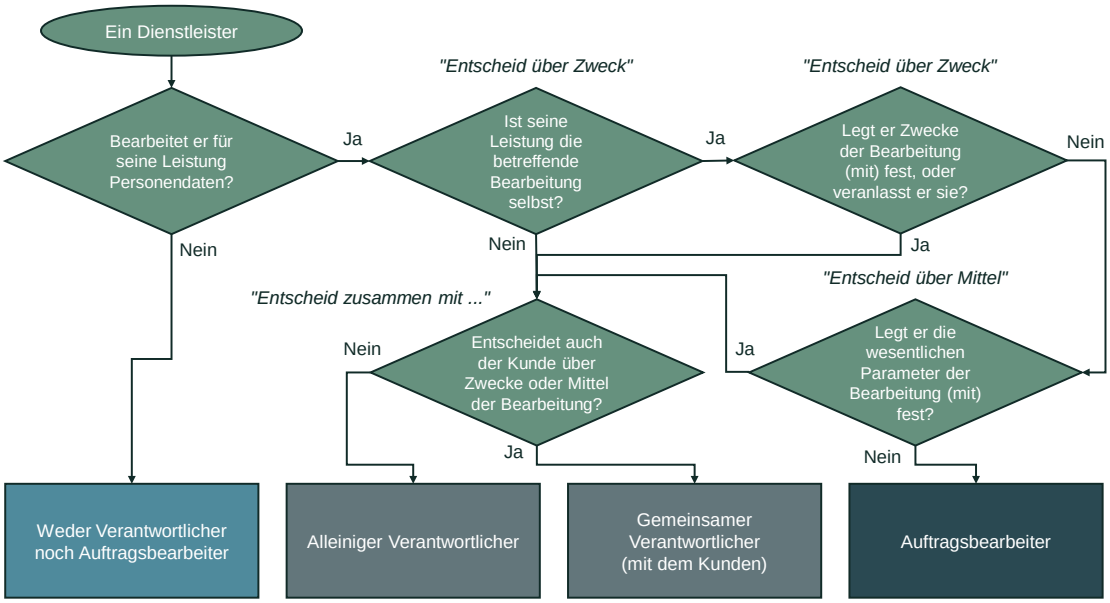
37 Ebd., Rz. 36 f.

EuGH aus.[38] Konkret ging es um die Zeugen-Jehovas, welche im Rahmen ihrer Verkündigungstätigkeit ihre Mitglieder von Tür zu Tür ziehen lässt. Als Gedächtnisstütze erheben diese Informationen über die besuchten Personen (z.B. wo es sich bei einem späteren Besuch wieder lohnt vorbeizugehen). Das Gericht kam zum Schluss, dass es für ein Mitbestimmen von Zweck und Mitteln ausreiche, wenn die Datenbearbeitung in der Umsetzung eines gemeinschaftlichen Ziels (i.c. der Verbreitung des gemeinschaftlichen Glaubens) «organisiert und koordiniert und zu ihr ermuntert» werde.[39] Aus beiden Urteilen geht auch hervor, dass gemeinsame Verantwortlichkeit nicht bedeutet, dass die Entscheide zusammen getroffen werden müssen und alle Beteiligten dieselbe Stellung und denselben Einfluss haben müssen. Auch zeitlich kann ihre Mitbestimmung versetzt sein.

Falls ein Mitbestimmen von Zweck oder Mitteln zweier Parteien bejaht werden kann, sind sie gemeinsame Verantwortliche und es ist in einem *dritten Schritt* – zumindest nach den Vorgaben von Art. 26 DSGVO – die Aufteilung ihrer Verantwortlichkeiten in einem Vertrag zu regeln. Das DSG bzw. E-DSG kennt keine explizite Regelung; eine Regelung der internen Zuständigkeit drängt sich aber bereits aufgrund der Pflicht auf, angemessene technische und organisatorische Massnahmen zu treffen, um eine unbefugte Datenbearbeitung zu verhindern, aber auch des Grundsatzes des *Privacy by Design* auf (Art. 6 f. E-DSG).

38 Urteil des EuGH vom 10. Juli 2018 (C-25|17) i.S. Zeugen Jehovas, Rz. 73.

39 Ebd., Rz. 73.



5. Spezielle Anwendungsfälle

a) Vorbemerkung

Die rechtlichen Anforderungen sind grundsätzlich klar: Sobald der Dienstleister entweder Zweck oder sonst datenschutzrechtlich wesentliche Aspekte der Datenbearbeitung kontrolliert, wird er zum Verantwortlichen. Doch in der Praxis ist die Rollenzuteilung trotz des einfachen Grundprinzips nicht immer ganz einfach. Das hat verschiedene Gründe. Zwei der typischen Problemkonstellationen werden sogleich herausgegriffen.[40] Die Ursachen sind allerding vielfältig. Teilweise sind die tatsächlichen Verhältnisse nicht klar, oder sie weichen vom gewollten Zustand ab. Auch die Grenze zwischen wesentlichen und nicht wesentlichen Aspekten der Datenbearbeitung ist fliessend. Manchmal verändern sich die Verhältnisse auch über die Zeit, oder es bereitet Mühe, die einzelnen Datenbearbeitungen voneinander abzugrenzen, was aber für die Bestimmung der Verantwortlichkeit von entscheidender Bedeutung ist.

40 Weitere finden sich in ROSENTHAL (Fn. 4).

b) Anbieter von Standardlösungen

In gewissen Fällen scheint die Qualifikation auf den ersten Blick klar, erweist sich aber auf den zweiten Blick als falsch. Anbieter von Cloud-basierten IT-Standardlösungen – ein typisches Beispiel hierfür ist «Office365» von Microsoft – stellen ihren Kunden Produkte zur Verfügung, bei denen wesentliche Parameter der Datenbearbeitung (z.B. wo die Daten gespeichert werden, wie die Datenbearbeitung durchgeführt werden können, wie lange Daten aufbewahrtet werden können) bereits vollständig vordefiniert zu sein scheinen.

Weil es aber letztlich der Kunde ist, der entscheidet, ob er und wie er die Dienstleistung für seine Datenbearbeitungen nutzen möchte und wie er sie im Rahmen der von Microsoft definierten Möglichkeiten konfiguriert bzw. einsetzt, wird Microsoft nicht zum Verantwortlichen, sondern bleibt Auftragsbearbeiter. Es ist ausreichend, dass der Kunde das Angebot *tel quel* in Anspruch nimmt und damit die datenschutzrechtlich vordefinierten Parameter auf *seine* Datenbearbeitung anwendet. Obschon der Kunde keinen Einfluss darauf nehmen kann, welche Art von Produkt Microsoft auf dem Markt anbietet, steht es ihm frei, überhaupt einen Vertrag mit Microsoft abzuschliessen und ihr seine Daten anzuvertrauen. Er kann die Datenbearbeitung ungeachtet der kommerziellen Folgen auch jederzeit wieder beenden.

Gemäss herrschender Lehre reicht diese Entscheidungsmöglichkeit aus, damit der Kunde alleiniger Verantwortlicher seiner Daten bleibt und der Dienstleister zum Auftragsbearbeiter wird.[41] Der E-DSG und die DSGVO sehen beide vor, dass der Verantwortliche die «Oberkontrolle» über seine Datenbearbeitung behalten muss. Demgegenüber ist es nicht zwingend, dass der Kunde bei der Nutzung des Angebots die Art und Weise der Datenbearbeitung individuell ausgestalten kann. Konkret bedeutet dies, dass der Kunde jederzeit über den Verbleib seiner Daten die Kontrolle behalten muss und diese vom Auftragsbearbeiter mitunter auch tatsächlich gelöscht werden, sobald der Kunde dies verlangt.

Die Situation ist vergleichbar mit dem Bestellen eines Gerichts im Restaurant: Die Menükarte gibt vor, welche Gerichte zur Auswahl stehen. Die Küche definiert sie, und sie sind für alle Gäste dieselben. Es ist jedoch der einzelne Gast, der entscheidet, welches davon er haben möchte und was serviert wird; dies ist *sein* Essen, nicht dasjenige des Restaurants und nicht dasjenige eines anderen Gastes. Die Küche macht zwar Vorschläge, was sie zubereiten

---

41 WP 169 (Fn. 18), 32; ebenso: RUDI KRAMER, in: Gierschmann|Schlender|Stentzel|Veil (Hrsg.), Kommentar. Datenschutz-Grundverordnung, Köln 2018, Art. 28 N 16.

könnte, führt aber lediglich aus und auch dies nur falls und wenn ein Gast dies wünscht. Entscheidend ist, dass alle wesentlichen Aspekte des Gerichts zum Zeitpunkt der Bestellung durch den Gast definiert sind und diese damit zu seiner Anweisung an die Küche werden; die Details sind der Küche überlassen.

Der Anbieter einer Standardlösung bleibt aber nur solange Auftragsbearbeiter, als er sich an die Parameter seiner angebotenen Leistung hält. Er kann demnach nicht einfach nach eigenem Gutdünken die vom Kunden ausgewählten Parameter ändern. Sobald er sein Produkt so weiterentwickelt, dass dies die datenschutzrechtlich wesentlichen Parameter der Datenbearbeitung seiner Kunden tangiert, wird er den Kunden aus der Datenbearbeitung aussteigen lassen müssen, ansonsten riskiert er, zum (Mit-)Verantwortlichen zu werden.

c) Dienstleister ist gleichzeitig Auftragsbearbeiter und Verantwortlicher

Würde der Anbieter einer Standardlösung aus eigenem Antrieb die ihnen von ihren Kunden anvertrauten Personendaten für andere Zwecke auswerten (z.B. der Anbieter einer Mail-Virusscanning-Lösung, welche Mails mit Viren auch seiner Forschungsabteilung zur Verfügung stellt), selbst wenn dies zu nicht personenbezogenen Zwecken geschehen würde, so würde er in Bezug auf diese Bearbeitungsvorgänge zum (Mit-)Verantwortlichen. Dienstleister sind somit nicht entweder nur Verantwortliche oder nur Auftragsbearbeiter, sondern können zugleich beides sein.

In der Praxis kommt dies laufend vor, auch wenn es häufig nicht realisiert wird, weil die damit verbundenen Datenbearbeitungen als nebensächlich erachtet werden. Ein typisches Beispiel sind Software-as-a-Service Lösungen, auf die online zugegriffen wird: Der Kunde nutzt diese Dienstleistung für seine Datenbearbeitung und entscheidet entsprechend selber, welche seiner Inhalte er damit wie bearbeitet. In Bezug auf dieses Angebot ist der Dienstleister Auftragsbearbeiter (vgl. voranstehen zu den Standardlösungen III.5.b). Derselbe Dienstleister ist jedoch Verantwortlicher, soweit er als Mittel zum Zweck der Erbringung der Dienstleistungen Personendaten des Kunden bearbeitet, etwa indem er ein Verzeichnis der Mitarbeiter führt, die auf den Dienst online zugreifen dürfen oder wenn er eine Hotline für Fragen und Störungsmeldungen betreibt und in diesem Zusammenhang Daten der Mitarbei-

ter des Kunden aufnimmt. Auch bezüglich der Administration der Dienstleistung (z.B. Erstellen der Rechnung, die ggf. Personendaten enthält) ist er Verantwortlicher.

IV. Bedeutung für die Bankenwelt

1. Beispiele aus der Informatik

Wird die Theorie auf IT-Dienstleistungen angewandt, welche Banken von Drittanbietern konzernintern oder extern in Anspruch nehmen, zeigt sich hierbei bereits ein breites Feld an möglichen Konstellationen:

– *Betrieb von Servern durch IT-Dienstleister für Bank:* Lagert die Bank beispielsweise die Speicherung von Daten an einen Dienstleister aus, so handelt es sich bei diesem um einen **Auftragsbearbeiter**. Diese Anbieter sind typischerweise Cloud-Anbieter oder andere Hosting-Provider, die ihre Rechnerkapazitäten Dritten zur Verfügung stellen. Die Bank entscheidet, ob diese Dienstleistungen in Anspruch genommen werden, in welcher Form dies erfolgt – ob die Daten beispielweise verschlüsselt übertragen werden – und sie kann insbesondere jederzeit die Daten auf den externen Servern ändern oder löschen (lassen). Der Dienstleister kann selbst dann als Auftragsbearbeiter gelten, wenn er der Bank keine konkreten Auswahlmöglichkeiten anbietet (z.B. ob die Daten in der Schweiz oder im Ausland gespeichert werden sollen). Es reicht, dass die Bank im Vorfeld oder auch während der Vertragsbeziehung jederzeit entscheiden kann, ob sie den Service für ihre Datenbearbeitung nutzen möchte oder nicht, auch wenn der Dienstleister der einzige auf dem Markt mit einem vergleichbaren Angebot ist.

– *Wartung von Software oder Hardware durch externen Dienstleister:* Hier gilt vorab zu unterscheiden, ob der Dienstleister überhaupt Zugriff auf Personendaten erlangt, um seine Wartungsleistung erbringen zu können. Hat er keinen Zugriff auf Personendaten, liegt seinerseits auch keine Bearbeitung von Personendaten vor und er **scheidet als Auftragsbearbeiter aus**. Hat der Dienstleister zwar Zugang zu Personendaten, ist deren Bearbeitung aber nicht Teil der Dienstleistung (z.B. der IT-Spezialist kann im Rahmen seines Remote-Zugriffs unter Umständen Daten der Kundendatenbank zu Kenntnis nehmen), so ist er nach der hier vertretenen Ansicht ebenfalls **kein Auftragsbearbeiter**, weil die Wahrnehmung von Personen-

daten bei Gelegenheit noch nicht als Bearbeitung von Personendaten qualifiziert wird.[42] Aufgrund des Bankkundengeheimnisses ist die Bank aber dennoch verpflichtet, die Dienstleister eine Geheimhaltungserklärung unterzeichnen zu lassen, da diese «Beauftragte» i.S.v. Art. 47 BankG sind und eine Wahrnehmung der Daten i.S. des BankG dennoch stattfindet.

– *Übertragung von verschlüsselten oder sonst pseudonymisierten Kundendaten an einen Dienstleister zur Bearbeitung:* Verbleibt der Schlüssel der Daten bei der Bank, so gilt auch hier der Dienstleister **nicht als Auftragsbearbeiter**, da die Daten aus seiner Sicht keine Personendaten darstellen und er somit keine Personendaten bearbeitet; nach der geltenden «relativen Methode» muss jeweils aus der Perspektive desjenigen, der Zugriff zu den Daten hat, beurteilt werden, ob er die betroffenen Personen identifizieren kann und den hierzu erforderlichen Aufwand betreiben will.[43] Das Datenschutzrecht kann immerhin indirekt zur Anwendung gelangen, da seine Handlungen trotz allem Auswirkungen auf die Datenbearbeitung seines Kunden haben können; daher ist zwar kein ADV nötig, aber eine vertragliche Regelung der Handlungen des Dienstleisters trotz allem angezeigt. Der Dienstleister kann für seine Mitwirkung an der Datenbearbeitung auch zur Verantwortung gezogen werden.
– *Der Dienstleister erstellt für die Bank Analysen über das Nutzerverhalten ihrer Webseiten:* Der Dienstleister gilt dann als **Auftragsbearbeiter**, wenn er die Daten nicht auch für eigene Zwecke erhebt, sondern diese Daten lediglich dazu dienen, der Bank nach ihren Vorgaben Statistiken über die Nutzung ihrer Webseite zu liefern und die Daten nicht auch für eigene Zwecke genutzt werden. Es handelt sich damit um ihre Datenbearbeitung. Auf dem Markt werden auch Analysedienste angeboten, bei denen der Analysedienst die Resultate der Analysen für eigene Zwecke verwendet und entsprechend dann als **Verantwortlicher** zu qualifizieren ist (ein typisches Beispiel ist die Reichweitenforschung, die über mehrere Angebote hinweg erfolgt). Im Übrigen kann die relevante Datenbearbeitung im Einzelfall

---

42 Wobei darauf hinzuweisen ist, dass in der Lehre auch Gegenteiliges vertreten wird und insbesondere in der von deutschen Autoren geprägten Literatur zur DSGVO die Meinung vertreten wird, dass es sich bei Dienstleistern, die ihm Rahmen der Prüfung und Wartung von Datenverarbeitungsanlagen Personendaten zu Kenntnis nehmen, Auftragsverarbeiter sind. Ausführlich hierzu: KRAMER (Fn. 41), Art. 28 N 21 ff.

43 Zum Begriff Personendaten, vgl. DAVID ROSENTHAL, Personendaten ohne Identifizierbarkeit?, in: digma 2017|4, 198-203.

auch so ausgestaltet sein, dass die erhobenen und analysierten Daten aufgrund des fehlenden Personenbezugs gar keine Personendaten darstellen und der Dienstleister damit **weder zum Auftragsbearbeiter noch Verantwortlichen** wird.

– *Übermittlung von Zahlungsaufträgen an andere Banken per SWIFT:* SWIFT und die Bank gelten als **gemeinsame Verantwortliche**. SWIFT ist unter anderem deshalb Verantwortliche, weil sie entscheidet, welche Daten von der Bank an sie übermittelt werden müssen. Ähnlich wie die Post, welche ihren Kunden vorgibt, welche Informationen sie benötigt, damit sie den Brief seinem Empfänger zuordnen kann, legt auch SWIFT fest, welche Informationen sie von den Banken braucht, um die Zahlungsaufträge über ihre Systeme abwickeln zu können. Dabei handelt es sich nicht bloss um Vorgaben in Bezug auf zulässige Dateiformate, sondern auch um solche inhaltlicher Natur (z.B. indem Standards festgelegt werden, welche die Überweisungsdaten enthalten müssen). Darüber hinaus entscheidet SWIFT über weitere Aspekte der Datenbearbeitung, wie etwa die Überprüfung der Richtigkeit der Daten, den Zeitraum über den die Daten auf ihren Systemen gespeichert werden, wo diese Daten gespeichert werden, und die Weitergabe von Daten aus ihrem Netzwerk an die US-Behörden.[44] Letzteres war auch der Anlass, dass sich die Artikel-29-Datenschutzgruppe in einer Stellungnahme mit der Rolle der SWIFT auseinandersetzte, da SWIFT ursprünglich nur Auftragsbearbeiterin sein wollte. Sie war hierfür jedoch zu stark in die Datenbearbeitungen involviert. SWIFT ist – anders als im genannten Beispiel der Post – mit den Banken *gemeinsame* Verantwortliche, weil unter Anwendung des Ebenenmodells (III.4) die Datenbearbeitungen der Banken und jene der SWIFT sich nicht wirklich getrennt betrachten lassen; sie umfassen beide die Abwicklung von Zahlungsaufträgen zwischen zwei Finanzinstituten. Hinzu kam die genossenschaftlichen Struktur von SWIFT, deren Mitglieder die einzelnen Banken sind.[45]

---

44 Vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 10|2006 zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunciation (SWIFT) vom 22. November 2006 (**WP 128**), 14.

45 WP 128 (Fn. 44), 17.

2. Beispiele aus der restlichen Bankenwelt

Im Nicht-Informatik-Bereich können die Anwendungsfälle in zwei Gruppen aufgeteilt werden. Einerseits ist die Bank Dienstleisterin ihrer Kunden, indem sie für diese Zahlungsaufträge ausführt oder sie bei der Verwaltung ihrer Vermögen unterstützt. Andererseits nimmt die Bank wiederum Dienstleistungen von Drittanbietern in Anspruch. Zu denken ist etwa an die Agentur, mit deren Hilfe jedes Jahr die Generalversammlung der Bank organisiert wird.

In ihrer Rolle als Dienstleisterin agiert die Bank hauptsächlich in folgenden Funktionen:

- *Ausführen von Zahlungsaufträgen:* Die Bank ist alleinige **Verantwortliche**. Sie bearbeitet die Daten des Bankkunden zwecks Ausführung des Zahlungsauftrags. Die Datenbearbeitung dient damit lediglich der Erfüllung des Auftrags, stellt aber im Kern nicht diejenige Leistung dar, die für den Kunden erbracht wird. Dem Kunden ist wichtig, dass die Zahlung erfolgt. Wie dies geschieht und welche Daten dabei konkret bearbeitet werden, ist dem Kunden in der Regel egal und selbst wenn ihn dies interessieren würde, kann er die Datenbearbeitung weder unmittelbar noch mittelbar mitbestimmen. Die Abwicklung der Zahlung und die damit verbundene Datenbearbeitung liegt damit in der Verantwortung der Bank, wobei das Verhältnis Kunde und Bank ein **Controller-Controller-Verhältnis** ist.
- *Anbieten von Firmenkreditkarten oder Online-Tools zur Abwicklung des Ausgabenmanagements:* Hierbei stellt die Bank (als sogenannter *Issuer*) den Mitarbeitern von ihren Unternehmenskunden Kreditkarten aus, die auf den Namen der Mitarbeiter lauten. Die Kreditkartenrechnungen werden von den Unternehmenskunden bezahlt. In Bezug auf die Herausgabe der Kreditkarten handelt die Bank als **Verantwortliche**, weil sie als Bank selber entscheidet, welche Daten sie für die Abwicklung der Zahlungen bearbeiten muss. Bietet die Bank ihren Kunden zusätzliche Informationen für die Erleichterung ihrer Spesenabrechnung an, so muss differenziert werden: Soweit es sich lediglich um die Lieferung zusätzlicher Angaben zur Rechnung geht (z.B. bei Flugbuchungen Angaben zum Flug, Klasse und Platz), bleibt die Bank **Verantwortliche**, selbst wenn sie diese Informationen über ein Online-Portal zur Verfügung stellt. Wenn die Bank hingegen weitergehende Online-Tools zu Verfügung stellen würde, mit denen zum Beispiel Mitarbeiter ihre Spesen erfassen und die internen Stellen deren Erstattung freigeben können, würde die Bank zur **Auftragsbearbeiterin**, weil sie mit dem Tool auch die Durchführung einer Datenbearbeitung übernimmt, die jene des Kunden ist.

– *Kundenberater berät Kunde, z.B. im Rahmen der Vermögensverwaltung:* Die Bank gilt hier als **Verantwortliche**. Der Kunde nimmt die Leistung der Bank in Anspruch, weil er sich das Fachwissen der Bank, respektive deren Mitarbeiter, zu Nutze machen möchte. Er bestimmt gerade nicht darüber, wie die Bank die anvertrauten Informationen bearbeiten soll, sondern erhofft sich von deren eigenen Datenbearbeitung einen persönlichen Nutzen. Der Kundenberater handelt hierbei **unter Aufsicht der Bank**. Dies wird so in Art. 29 DSGVO ausdrücklich festgehalten, ist aber – obschon im DSG und E-DSG nicht explizit geregelt – auch nach Schweizer Verständnis im Grunde nicht anders.[46] Der Kundenberater ist an die Weisungen der Bank gebunden. Deren Weisungsrecht erstreckt sich auch auf die Einhaltung des Datenschutzes bei der Bearbeitung von Personendaten. Zum Kreise der Mitarbeiter im Sinne dieser Bestimmung gehören dabei nicht nur klassische Mitarbeiter einer Bank, sondern auch externe Berater, die zum Beispiel für einzelne oder mehrere Projekte auf Mandatsbasis arbeiten und in die Organisation der Bank eingebunden sind.[47] Entscheidend ist, dass die Personen unter der Aufsicht und Weisungsgewalt des Verantwortlichen stehen und ihre Datenbearbeitungen auch einzig jene der Bank sind.[48] Dies trifft typischerweise auch auf Mitarbeiter von Anwaltskanzleien oder Beratungsunternehmen zu, die ein *Secondment* bei einer Bank absolvieren und daher in deren Arbeitsorganisation eingegliedert sind.

Typische Dienstleistungen die eine Bank im Geschäftsalltag von Drittanbietern in Anspruch nimmt, respektive an solche delegiert, sind:

– *Delegation von KYC-Pflichten:* Delegiert ein Finanzintermediär, der aufgrund des Geldwäschereigesetzes einen potenziellen Kunden identifizieren muss, diese Abklärung an eine Bank, bei welcher dieselbe Person bereits Kunde ist, so sind beide **eigenständige Verantwortliche**. Die Bank, welche die Dienstleistung erbringt, bearbeitet die Daten basierend auf ihrer eigenen gesetzlichen Pflicht und bestimmt in diesem Zusammenhang allein über den Zweck und die Mittel der Datenbearbeitung. Daran ändert

---

46 Die Regeln für die Auftragsbearbeitung finden analog Anwendung. Allgemein gilt, dass das arbeitsrechtliche Weisungsrecht dem vertraglich zu vereinbarenden Weisungsrecht i.S. von Art. 8 E-DSG entspricht.

47 HARTUNG (Fn. 26), Art. 29 N 13; MARIO MARTINI, in: Paal|Paal (Hrsg.), Datenschutzgrundverordnung Bundesdatenschutzgesetz. Beck'sche Kompakt Kommentare, 2. Aufl., München 2018, Art. 29 N 14.

48 HARTUNG (Fn. 26), Art. 29 N 17 f.

sich auch nichts, dass der Finanzintermediär, welcher um die Information ersucht, das Ergebnis der Datenbearbeitung der Bank erfährt. Entscheidend ist, dass der Finanzintermediär keinen Einfluss auf die wesentlichen datenschutzrechtlichen Parameter der Bank nimmt; diese findet überdies auch ohne das konkrete Informationsersuchen statt.

– *Teilnahme an Wertpapierbörse:* Die Börse gilt als **Verantwortliche**, weil sie im Wesentlichen darüber entscheidet, was auf ihrer Plattform passiert. Selbst wenn die teilnehmenden Banken bis zu einem gewissen Punkt über die Inhalte, die sie einbringen, mitbestimmen, entscheidet die Betreiberin der Wertpapierbörse, ob es die Datenbearbeitung gibt, welche Inhalte sie zulässt, und wozu die Daten genutzt werden können. Im Gegensatz zu reinen Hosting-Anbieter stellen Wertpapierbörsen nicht nur die Infrastruktur zum Hochladen von Daten zur Verfügung, sondern geben den Rahmen der von ihnen durchgeführten Datenbearbeitungen vor. Was mit den zur Verfügung gestellten Daten auf der Plattform der Börse geschieht, entscheidet ebenfalls die Wertpapierbörse und nicht deren Teilnehmer. Deshalb handelt es sich auch nicht um einen Anwendungsfall einer Standardlösung, die der Kunde auf seine eigene Datenbearbeitung anwendet. Dies bedeutet aber nicht zwingend, dass die Wertpapierbörse alleinige Verantwortliche sein muss. Die Banken können mit der Börse je nach zusammenwirken als **gemeinsame Verantwortliche** agieren, oder sie sind für ihre Datenbearbeitungen im Rahmen des Ebenenmodells eigenständige Verantwortliche.
– *Beauftragung eines Anwalts:* Der Anwalt handelt als **eigenständiger Verantwortlicher**, obschon er bei seiner Tätigkeit gänzlich die Interessen der Bank vertritt. Die Dienstleistung wird insbesondere deshalb in Anspruch genommen, um externes Fachwissen hinzuzuziehen. Entsprechend soll der Anwalt unabhängig und in Bezug auf die Datenbearbeitung weisungsungebunden seine Erfahrung und sein Know-how auf den Fall anwenden und die ihm von Klienten oder selber zusammengesammelten Informationen entsprechend bearbeiten. Auch hier kann allerdings der konkrete Auftrag so ausgestaltet sein, dass der Anwalt die Daten in der Rolle des **Auftragsbearbeiters** bearbeitet. Ein möglicher Anwendungsfall ist der Anwalt, der für die Bank grosse Datenmengen auf bestimmte Kriterien durchsucht und sie entsprechend den genauen Vorgaben der Bank bearbeitet (z.B. Schwärzungen von Kundennamen in Dokumenten, die an eine ausländische Behörde geliefert werden müssen). Auch **gemeinsame**

Verantwortlichkeiten sind denkbar, wenn der Anwalt an der Ausgestaltung einer Datenbearbeitung der Bank faktisch in datenschutzrechtlich relevanten Punkten mitentscheidet.

- *Datenbearbeitungen durch Kreditkartennetzwerke:* Die Kreditkartennetzwerke sehen sich zwar in der Regel als Auftragsbearbeiter der Banken in deren Rolle als Kartenherausgeber, legen aber wesentliche datenschutzrechtliche Parameter der von ihnen durchgeführten Datenbearbeitungen selbst fest (z.B. welche Kategorien von Personendaten wo und wie gesammelt werden dürfen bzw. müssen). Sie sind daher in diesen Fällen typischerweise **Verantwortliche**.
- *Vetting künftiger Mitarbeiter durch einen Dienstleister:* Überlässt es die Bank dem Dienstleister, Personensicherheitsprüfungen seiner eigenen Mitarbeiter vorzunehmen, bevor er diese im Rahmen eines Auftrags der Bank zum Einsatz bringt, so handelt der Dienstleister als alleiniger **Verantwortlicher**. Er führt die Datenbearbeitung für seinen Zweck durch, und bestimmt selbst, wie er dies tut, wenngleich die Bank ihm gewisse inhaltliche Mindeststandards vorgeben wird. Verlangt die Bank die Mitteilung personenbezogener Ergebnisse, so ist diese ebenfalls **Verantwortliche**.
- *Aktionärsbetreuung:* Beauftragt die Bank einen Dienstleister, ihr Aktionärsregister zu führen, so handelt diese als **Auftragsbearbeiterin**. Der Auftrag ist die Datenbearbeitung an sich, welche an den Dienstleister übertragen wird. Übernimmt der Dienstleister zusätzlich noch die Aufgabe, jedes Jahr die Generalversammlung der Bank zu organisieren und durchzuführen (z.B. Einladungen verschicken, Lokalitäten und Bewirtung der Aktionäre organisieren, etc.), so handelt sie diesbezüglich als **Verantwortliche**. Dann entscheidet nämlich dieser selber darüber, welche Datenbearbeitungen nötig sind, um die Dienstleistung (welche nicht mit der Datenbearbeitung deckungsgleich ist) erbringen zu können.
- *Dienstleister erledigt die Geschäftsführung der Pensionskasse von Bankangestellten:* Pensionskassen bzw. die diesbezüglichen Stiftungen übertragen die Geschäftsführung häufig integral an einen Dienstleister. Dieser entscheidet, welche Datenbearbeitungen er zu diesem Zweck vornimmt, auch wenn sie in der Natur der Sache teilweise vorgegeben sind. Er und nicht die Pensionskasse legt damit den Zweck der Datenbearbeitungen fest und bestimmt überdies ihre Mittel. Der Dienstleister gilt daher in der Regel als alleiniger **Verantwortlicher**. Soweit dem Stiftungsrat der Pensionskasse Dossiers von Versicherten zugänglich gemacht werden (z.B. in einem Rekursfall), so wird dieser ebenfalls zum **Verantwortlichen**. Allerdings hat

ein Stiftungsrat normalerweise keinen Zugang zu den Personendaten im Rahmen der Geschäftsführung und macht dieser in aller Regel auch keine datenschutzrechtlichen Vorgaben.

– *Geschenkeversand für gute Kunden:* Beauftragt eine Bank eine Konditorei damit, bestimmten Kunden zu einem besonderen Anlass eine Schachtel Pralinen zu schicken, ist die Konditorei in der Regel eigenständige **Verantwortliche**. Die angebotene Dienstleistung ist das Versenden ihrer Pralinen in eigenem Namen an Personen nach Wahl des Unternehmens. Diese Dienstleistung bedingt Datenbearbeitungen, welche in der Regel die Datenbearbeitungen der Konditorei sind, da diese lediglich der Ausführung der Dienstleistung dienen und damit Mittel zum Zweck sind. So ist die Konditorei Verantwortliche in Bezug auf die Datenbearbeitungen, die sie durchführt, um ihre Dienstleistung erbringen zu können. Der nach aussen gleichlautende Auftrag – das Versenden von Pralinen an Kunden eines Unternehmens – kann im konkreten Einzelfall aber auch so ausgestaltet werden, dass die Konditorei **Auftragsbearbeiterin** ist. Hierbei wird das Unternehmen der Konditorei in Bezug auf die Datenbearbeitungen klare Anweisungen geben müssen, welche Adressen sie wie auf ihre Pralinenschachteln anzubringen hat und dass sie die Schachteln an entsprechende Adressen zu verschicken hat. Von dieser datenschutzrechtlichen Qualifikation unabhängig ist notabene die Beurteilung aus Sicht des Bankgeheimnisses: So kann auch ein Beauftragter i.S.v. Art. 47 BankG ein Verantwortlicher i.S. des Datenschutzes sein. Das heisst, dass selbst dann wenn der Dienstleister ein Verantwortlicher ist, mit ihm womöglich eine Bankgeheimnisvereinbarung abgeschlossen und er verpflichtet werden muss, die Daten nicht nur vertraulich zu behandeln, sondern auch nicht für andere Zwecke zu verwenden.

V. Empfehlungen für die Praxis

1. Ausgestaltung der Dienstleistung im konkreten Einzelfall

Das letztgenannte Beispiel zeigt auf, dass die Parteien eine Dienstleistung nicht selten so ausgestalten können, dass ein Dienstleister entweder Verantwortlicher oder Auftragsbearbeiter wird. In letzterem Fall muss sichergestellt werden, dass der Dienstleister sich bei der Bearbeitung der Personendaten an die Weisungen des Auftragsgebers hält und keinerlei Gestaltungsfreiheit bezüglich der datenschutzrechtlich wesentlichen Aspekte der Datenbearbeitung hat.

Das Ergebnis hat freilich diverse Konsequenzen, und diese beschränken sich nicht nur auf die Frage, ob ein ADV abgeschlossen werden muss oder nicht. Das Ergebnis ist zum Beispiel auch für das Risk Management der Parteien von entscheidender Bedeutung: Ist der Dienstleister einer Bank nämlich deren Auftragsbearbeiter, übernimmt sie mit der Beauftragung unter Umständen ein viel grösseres datenschutzrechtliches Risiko, als wenn er eigenständiger Verantwortlicher ist: Sie wird ihn im ersten Fall nicht nur instruieren, sondern auch überwachen müssen und dafür einstehen, dass er sich an den ADV hält – also zum Beispiel stets eine angemessene Datensicherheit aufweist.

Parteien, welche versuchen, eine Dienstleistung in diese Richtung zu «lenken», sollten auch beachten, dass gemäss Art. 55 E-DSG künftig eine vorsätzlich falsch getroffene Qualifizierung einer Auftragsbearbeitung und die damit einhergehende Datenbekanntgabe unter Missachtung der Vorgaben von Art. 8 E-DSG strafrechtlich sanktioniert werden kann.[49]

Umgekehrt kann aber auch ein Auftragsbearbeiter zum Verantwortlichen werden, wenn er sich nicht an die Weisungen des Auftraggebers hält, weil er etwa versucht, einen Prozess eigenmächtig zu optimieren. Ein bewusster Entscheid ist hierzu nicht nötig. Der Auftragsbearbeiter begeht dann unter Umständen nicht nur eine Vertragsverletzung, sondern wird in Bezug auf diese Datenbearbeitung als (Mit-)Verantwortlicher gegenüber den betroffenen Personen direkt haftbar und hat weitere Pflichten gemäss Gesetz, denen er sich aber gar nicht bewusst sein mag. Auch dies kann wiederum zu Sanktionen führen.

2. Auftragsdatenbearbeitungsvertrag (ADV)

Bevor die Verträge aufgesetzt werden, sollte daher stets sauber abgeklärt werden, ob sämtliche Aspekte der Dienstleistung tatsächlich als Auftragsbearbeitung gelten, oder ob der Dienstleister gewisse Personendaten beispielsweise auch für eigene Zwecke nutzt oder gewisse Datenbearbeitungen selbst kontrolliert. In jedem Fall ist der Anwendungsbereich eines mit ihm abzuschliessenden ADV sachlich entsprechend auf die betroffene(n) Datenbearbeitung(en) zu beschränken.

Dies sollte im Sinne einer positiven Auflistung der konkreten Datenbearbeitungen, die dem ADV unterstehen, erfolgen; auch Art. 28 DSGVO verlangt, dass die Eckpunkte der Datenbearbeitung umschrieben sind (Gegenstand

[49] Mit einer Busse in der Höhe von bis zu CHF 250'000. Allerdings wird Vorsatz verlangt.

und Dauer der Verarbeitung, Art und Zweck der Bearbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen).

In der Praxis kommen allerdings immer wieder auch Situationen vor, in denen sich die Parteien nicht darauf einigen können, ob bzw. inwieweit ein Dienstleister als Auftragsbearbeiter zu qualifizieren ist. Kann hier keine Einigkeit erzielt werden und beharrt der Kunde auf einem ADV, kann es – als eher pragmatische denn als saubere Lösung – aus Sicht des Dienstleisters helfen, den Geltungsbereich des ADV negativ einzuschränken, indem er nur aber immerhin soweit Anwendung finden soll, «als der Dienstleister die Daten des Kunden als Auftragsbearbeiter bearbeitet». Der Dienstleister wird sich in einer solchen Situation darauf einstellen müssen, im Zweifel als Verantwortlicher zu gelten und sich entsprechend zu verhalten. An sich ist eine vernünftige Datenschutz-Compliance ohne Einigung auf die datenschutzrechtlichen Rollen aber nicht möglich.

In Bezug auf die konkrete Ausgestaltung eines ADV, geben der E-DSG und die DSGVO unterschiedliches vor. In Art. 28 DSGVO sind acht Punkte definiert, die in jedem ADV abgedeckt sein müssen. Das revidierte DSG wird hierbei viel weniger weit gehen und diese Punkte bis auf zwei Ausnahmen nicht übernehmen.[50] Auch bei Schweizer Unternehmen kommen ADV nach den Vorgaben der DSGVO relativ häufig zum Einsatz. Das hat einerseits damit zu tun, dass sie sich absichern wollen, falls sie mit gewissen Daten selbst unter die DSGVO fallen sollten, andererseits damit, dass viele Dienstleister standardmässig mit solchen Klauseln arbeiten oder aufgrund ihrem eigenen Sitz im EWR sogar dazu verpflichtet sind. Aus Sicht des DSG bzw. E-DSG schadet der Abschluss eines ADV nach Art. 28 DSGVO nicht, solange die Bestimmungen auch auf die Schweizer Verhältnisse angepasst sind (z.B. Verweise nicht nur auf die DSGVO).

Die besagten acht Punkte sind:

- Weisungsrecht betr. Bearbeitung von Personendaten, einschliesslich mit Bezug auf Auslandsexporte;
- Verpflichtung aller involvierten Personen auf das Datengeheimnis;
- Angemessene technische und organisatorische Massnahmen der Datensicherheit;

[50] In Art. 8 E-DSG ist grundsätzlich vorgesehen, dass der Verantwortliche sicherstellen muss, dass der Auftragsbearbeiter die Daten nur so bearbeitet, wie der Verantwortliche dies auch tun dürfte. Sodann sind die Regelungen der Datensicherheit und die Kontrolle über die Unterbeauftragung separat zu regeln.

- Regelung zum Beizug von Unterauftragsbearbeitern, wobei wie in der Schweiz auch hier gilt, dass ein solcher nur mit Genehmigung des Verantwortlichen zulässig ist;
- Pflicht zur Unterstützung des Verantwortlichen bei der Erfüllung der Rechte der betroffenen Personen (Auskunftsrecht, Löschrecht, etc.);
- Pflicht zur Unterstützung des Verantwortlichen bei der Erfüllung der Meldepflicht von Verstössen gegen die Datensicherheit und Datenschutz-Folgenabschätzungen;
- Rückgabe bzw. Löschung der Daten nach Ende der Auftragsbearbeitung;
- Auditrecht des Verantwortlichen.

Die Umsetzung dieser acht Punkte erfolgt heute in der Regel über Standardverträge, die von kurz und knapp gehaltenen Verträgen mit ein bis zwei Seiten bis hin zu umfangreichen Regelwerken reichen können. Diese lassen sich, meist im Rahmen eines Anhangs, auf den konkreten Einzelfall anpassen, indem die Datenbearbeitungen, die zu bearbeitenden Personendaten, die Zwecke, die Aufbewahrungsfristen etc. definiert werden. Eine vermehrte Standardisierung der ADV birgt selbstredend auch die Gefahr, dass sich die Parteien immer weniger mit deren Inhalt auseinandersetzen – weder bei deren Erstellung noch nach Vertragsschluss – und diese zu einem Papiertiger bzw. reiner Bürokratie verkommen.

Ein ADV muss gemäss DSGVO zwingend schriftlich abgefasst sein, wobei die elektronische Form mitumfasst ist. Möglich ist dabei auch, dass der ADV über Allgemeine Geschäftsbedingungen einbezogen wird. Es ist aber darauf zu achten, dass der ADV ebenfalls vom Konsens der Parteien mitumfasst wird. Weil es sich beim ADV um einen Vertrag handelt, reicht eine blosse Kenntnisnahme der Parteien nicht aus, um dessen Inhalt Bindungswirkung zu verleihen.

Kein ADV muss demgegenüber abgeschlossen werden, wenn der die Daten bearbeitende Dienstleister der eigene Mitarbeiter ist; ebenso wenig, wenn es sich dabei um einen externen Berater handelt, der gleichsam in die Arbeitsorganisation eingegliedert ist und damit dem allgemeinen Weisungsrecht der Bank untersteht (vgl. Beispiel des Kundenberaters in IV.2 und I.).

3. Controller-Controller-Verhältnis

Werden Daten einem anderen Verantwortlichen übergeben, so werden die Daten aus datenschutzrechtlicher Perspektive einem «echten» Dritten bekannt gegeben. Dies ist mitunter nur dann zulässig, wenn die Bekanntgabe

mit dem Zweck, der bei der Beschaffung der Daten erkennbar war, respektive der den betroffenen Personen damals angegeben wurde[51], übereinstimmt oder zumindest vereinbar ist. Stellt die Weitergabe demgegenüber eine nachträgliche Zweckänderung dar, so ist dies nach E-DSG möglich, wenn ein Rechtfertigungsgrund vorliegt (z.B. Vertragserfüllung oder überwiegende private Interessen). Ohnehin immer gerechtfertigt werden muss eine Weitergabe von besonders schützenswerten Personendaten an einen anderen Verantwortlichen; also z.B. Angaben über die Religion, sexuelle Orientierung, etc.[52] Nach DSGVO muss zusätzlich für jede Datenbearbeitung, einschliesslich die Bekanntgabe von Daten, eine Rechtsgrundlage[53] begründet werden; diese Pflicht trifft demnach auch den Verantwortlichen, der die Daten für die Erbringung einer Dienstleistung vom Auftraggeber erhält oder diese in dessen Auftrag selber erhebt.

Anders als bei einer Auftragsbearbeitung, können Personendaten sowohl nach E-DSG als auch unter der DSGVO ohne Vertrag an einen anderen Verantwortlichen weitergegeben werden, jedenfalls sofern sich dieser in einem Land mit angemessenem gesetzlichen Datenschutz befindet. Erlaubt sind Vereinbarungen zwischen zwei unabhängigen Controllern aber trotzdem; sie sind in der Praxis sogar üblich und weit verbreitet.

Diese vertraglichen Vereinbarungen weisen oft dieselben Inhalte wie Vereinbarungen über die Auftragsbearbeitung auf (einschliesslich einer strengen Zweckbindung[54]), mit dem wesentlichen Unterschied, dass der Empfänger der Daten bezüglich ihrer Bearbeitung nicht weisungsgebunden ist bzw. die Weisungen nicht so weit gehen dürfen, dass der Verantwortliche seine Pflichten als Verantwortlicher nicht mehr erfüllen kann. Alleine der Umstand, dass ein Verantwortlicher kontrolliert, wie ein Datenempfänger mit den ihm bekanntgegebenen Daten umgeht, bedeutet umgekehrt denn auch noch nicht, dass es sich um eine Auftragsbearbeitung handelt.

---

51 Aufgrund der gemäss DSGVO und auch mit dem revidierten Datenschutz geltenden Informationspflichten, wird diese Information in der Praxis meist über die Datenschutzerklärungen erfolgen.

52 Vgl. Art. 26 Abs. 2 lit. c E-DSG.

53 Gemäss Art. 6 DSGVO sind die am meisten zu Anwendung gelangenden Rechtsgrundlagen für nicht sensitive Personendaten z.B. berechtigte Interessen, die Vertragserfüllung und die Einwilligung; Art. 9 f. DSGVO kommen für sensitive Personendaten zur Anwendung.

54 Dies ermöglicht wiederum, dass sich der die Daten empfangende Datenbearbeiter in der Regel auf den gleichen Rechtsgrund abstützen kann wie die ihm die Daten übergebende Person.

Konkret kann es sinnvoll sein, wenn sich die Bank gewisse Kontrollrechte ausbedingt, wie beispielsweise eine Informationspflicht bei Datenverlust durch den Dienstleister oder bei unerlaubten Zugriffen auf die Daten, ein Auditrecht, ein Verbot der Auslagerung der Daten in ein Land ohne angemessenen Datenschutz oder ein Verbot der Datennutzung für Dritte. Ebenso sinnvoll sind Vorgaben bezüglich der Datensicherheit und Hinweise auf die Pflicht der Geheimhaltung der Informationen. Selbst wenn die Bank z.B. das Bankkundengeheimnis auf den Dienstleister überbindet und sich konkrete Kontrollmöglichkeiten ausbedungen hat, kann ein konkreter Verdachtsfall auf Datenmissbrauch im Vorfeld der Bekanntgabe oder in Bezug auf eine erneute Bekanntgabe trotz Kenntnis eines Vorfalls, gleichermassen datenschutzrechtliche aber auch strafrechtliche Konsequenzen nach sich ziehen. In jedem Fall stellen solche Vorkommnisse immer auch ein Reputationsrisiko für die Bank dar.

Der Vollständigkeit halber sei hier noch anzufügen, dass Art. 26 DSGVO in Bezug auf das Verhältnis zwischen zwei gemeinsamen Verantwortlichen vorschreibt, dass deren Beziehung zwingend vertraglich geregelt sein muss. Insbesondere ist in einem schriftlichen Vertrag zu klären, wer (Haupt-)Ansprechpartner der betroffenen Personen ist, wer die Erfüllung der Betroffenenrechte und die weiteren datenschutzrechtlichen Pflichten sicherstellt (z.B. Meldung von Datensicherheitsverstössen) und wer dabei wie unterstützt. Auch diese Verträge können ähnlich wie ein ADV ausgestaltet sein bzw. ähnliche Regelungsinhalte aufweisen; eine genaue inhaltliche Vorgabe gibt es hier allerdings nicht. Das DSG und E-DSG kennen gar keine Regelung dazu.

VI. Schlussbemerkungen

Wenn eine Bank einem Dienstleister Personendaten seiner Kunden oder Mitarbeiter übergeben muss, gehen viele intuitiv von einer Auftragsbearbeitung aus und verlangen den Abschluss eines ADV. Wie gezeigt, ist dies oftmals nicht angemessen. Eine vertiefte Auseinandersetzung mit der Abgrenzung zwischen der Rolle des Auftragsbearbeiters und des Verantwortlichen aber auch mit dem Konstrukt der gemeinsamen Verantwortung ist daher wichtig, auch wenn die Materie vielschichtig ist und scharfe Abgrenzungen nicht immer möglich sind.

Noch komplizierter wird die Frage der Rollenzuteilung dann, wenn die Betroffenen wenig Kenntnis von der inneren Ausgestaltung des Auftrags haben. Gerade im IT-Bereich ist es nicht immer einfach zu verstehen, inwiefern

eine Weisung des Auftraggebers tatsächlich eine Datenbearbeitung beeinflusst. Zwar muss nicht im Detail verstanden werden, wie die Datenbearbeitung technisch genau abläuft. Ein gutes inhaltliches Verständnis von der der Dienstleistung zugrundeliegenden Datenbearbeitung ist dennoch unabdingbar. Insbesondere sollte die für die datenschutzrechtliche Compliance zuständige Person in jedem Fall die beiden Fragen beantworten können, (i) welches die relevanten Datenbearbeitungen sind, die eine logische Einheit bilden, und (ii) wer eigenverantwortlich festlegt, wozu die Datenbearbeitungen dienen oder mindestens Einfluss auf ihre datenschutzrechtlich relevanten Eckwerte hat.

Biometrische Daten im Bankkundenverkehr am Beispiel der Stimmauthentifizierung

Susan Emmenegger/Martina Reber*

* Prof. Dr. iur. Susan Emmenegger, LL.M., Direktorin des Instituts für Bankrecht, Universität Bern. Martina Reber, Rechtsanwältin, MLaw, wissenschaftliche Assistentin und Doktorandin am Institut für Bankrecht, Universität Bern.

I. Einleitung

Das Bankgeschäft ist ein Risikogeschäft. Das gilt nicht nur für die Makroperspektive, es gilt auch auf der Mikroebene und es gilt – noch kleinteiliger – für die Kommunikation und die Transaktion mit der einzelnen Bankkundin. Zu den Risiken im letztgenannten Bereich zählen die sogenannten Legitimationsmängel, bei denen ein betrügerisch handelnder Zahlungsempfänger eine Zahlung an sich selbst bewirkt, ohne dass diese Zahlung von der Kontoinhaberin autorisiert war.[1] Aber auch die Erfragung von Kontoständen oder anderen kontorelevanten Informationen steht unter dem Risiko eines Zugriffs durch vertragsfremde Dritte.

Eine mögliche Abhilfe zur Vermeidung von solchen Vorfällen sind Authentifizierungsmechanismen, die auf biometrische Erkennungsmerkmale abstellen.[2] Dabei sind allerdings die rechtlichen Rahmenbedingungen für die Verwendung von biometrischen Authentifizierungsverfahren zu beachten.

---

1 Zum Begriff des Legitimationsmangels etwa SCHALLER, Legitimationsmängel, 49 f.

2 Beispielhaft folgende Klausel: «Die Bank kann zu Sicherheitszwecken (z.B. Schutz des Kunden und der Bank vor missbräuchlichen oder deliktischen Aktivitäten) den Kunden betreffende biometrische Daten sowie Bewegungs- und Transaktionsdaten und entsprechende Profile des Kunden erheben und bearbeiten.»

II. Biometrische Daten

1. Begriff

Bestimmte Körpermerkmale sind bei jedem Menschen einzigartig. Dazu gehören etwa der Fingerabdruck oder das Irismuster, nicht aber die Körpergrösse oder die Augenfarbe.[3] Sind diese Körpermerkmale überdies messbar und nur mit erheblichem Aufwand veränderbar, handelt es sich um biometrische Merkmale.[4]

Biometrische Daten sind Angaben über biometrische Merkmale.[5] Sie dienen in der Regel der Überprüfung, ob eine Person tatsächlich diejenige ist, für die sie sich ausgibt (Verifizierung) oder dem Abgleich mit einer Gesamtdatenbank zwecks Findung der Identität einer Person (Identifizierung).[6]

2. Funktionsweise biometrischer Verfahren

Biometrische Verfahren laufen in zwei Phasen ab. Zuerst erfolgt eine Registrierungsphase (Enrollment), in der die Identität der betroffenen Person erfasst und das biometrische Merkmal mehrmals und unter veränderten Bedingungen gemessen wird.[7]

> Beispiel: Bei der Einrichtung der Fingerabdruck-Authentifikation auf dem Smartphone muss der Benutzer seinen Finger mehrmals aus unterschiedlichen Winkeln und in unterschiedlichen Positionen auf den Fingerabdrucksensor des Smartphones legen.

Anschliessend werden die relevanten Merkmale aus den Rohdaten extrahiert und als biometrisches Template zusammen mit den Angaben zur Identität des Benutzers gespeichert.[8]

Die zweite Phase wird als Erkennungsphase bezeichnet. Erneut wird das entsprechende biometrische Merkmal gemessen und daraus ein biometrisches Template erstellt, welches mit den gespeicherten Referenztemplates

---

3 HK DSG-ROSENTHAL, Art. 3 N 42.

4 BLONSKI, Biometrische Daten, 6.

5 BLONSKI, Biometrische Daten, 6.

6 BLONSKI, Biometrische Daten, 6; EDÖB, Leitfaden zu biometrischen Erkennungssystemen, 5.

7 BLONSKI, Biometrische Daten, 11, m.w.H.; EDÖB, Leitfaden zu biometrischen Erkennungssystemen, 5.

8 Vgl. EDÖB, Leitfaden zu biometrischen Erkennungssystemen, 12; BLONSKI, Biometrische Daten, 11.

verglichen wird.[9] Bei der Verifizierung findet dieser Vergleich nur mit den Referenzdaten derjenigen Person statt, als die sich eine Person ausgibt.[10] Bei der Identifizierung wird das aktuell erstellte Template hingegen mit einer Vielzahl von Referenztemplates verglichen mit dem Ziel, herauszufinden, welcher Person das biometrische Merkmal zugeordnet werden kann.[11]

3. Die Stimmerkennung im Besonderen

Bei der Stimmerkennung wird die Stimme mittels eines Mikrofons aufgenommen.[12] Dabei gibt es zwei mögliche Methoden. Bei der textabhängigen Methode muss die Kundin vorgegebene Wörter aussprechen, bei der textunabhängigen Methode kann die Software ein beliebiges Kundengespräch analysieren.[13] Anschliessend werden die charakteristischen Merkmale extrahiert und daraus ein Stimmabdruck erstellt.[14] Bei künftigen Gesprächen wird die Stimme der Kundin zwecks Authentifizierung mit diesem Stimmabdruck abgeglichen.[15]

4. Beispielfall für eine Stimmerkennung

In den AGB von Banken finden sich vermehrt Klauseln, wonach diese sich vorbehalten, zu Sicherheitszwecken biometrische Daten des Kunden zu erheben und zu bearbeiten. Dazu gehört auch die Erstellung eines Stimmabdrucks. Den jüngsten Anwendungsfall, der medial aufgegriffen wurde,[16] betrifft die PostFinance. Sie nutzt seit September 2018 ein Stimmauthentifizierungssystem der israelischen Firma NICE.[17] Ruft die Kundin das erste Mal bei PostFinance an, hört sie folgende automatische Ansage:

> «Dieses Gespräch wird zu Sicherheits- und Wiedererkennungszwecken aufgezeichnet. PostFinance erstellt aus der Aufnahme einen Stimmabdruck, um

9 BLONSKI, Biometrische Daten, 12.

10 BLONSKI, Biometrische Daten, 12 f.; EDÖB, Leitfaden zu biometrischen Erkennungssystemen, 5.

11 BLONSKI, Biometrische Daten, 13.

12 BLONSKI, Biometrische Daten, 19.

13 Vgl. BLONSKI, Biometrische Daten, 19.

14 Vgl. BLONSKI, Biometrische Daten, 19; zur Extraktion der charakteristischen Merkmale ausführlich TILLENBURG, DuD 3/2011, 198.

15 Vgl. BLONSKI, Biometrische Daten, 19.

16 So etwa in der SRF-Sendung «10vor10» vom 20. Mai 2019.

17 Inside-IT vom 2. Mai 2019 («PostFinance setzt auf Stimmerkennung zur Authentifizierung»), abrufbar unter: <www.inside-it.ch/articles/53194>.

> Ihre Identität bei jeden [recte: jedem] Anruf anhand Ihrer Stimme zu verifizieren. Wünschen Sie keinen Stimmabdruck, bitten wir Sie, dies dem Kundenbetreuer mitzuteilen.»

Alternativ zum Widerspruch am Telefon kann die Kundin die Stimmerkennung im Online-Banking-Portal der PostFinance (E-Finance) deaktivieren, woraufhin ein allfällig bereits erstellter Stimmabdruck gelöscht wird. Hat die Kundin der Stimmerkennung widersprochen, wird sie anhand von Fragen authentifiziert.[18]

Auf ihrer Website informiert die PostFinance namentlich darüber, dass der Stimmabdruck «auf Servern in der PostFinance-Sicherheitszone in der Schweiz gespeichert» werde «und zwar in Form eines Codewertes, das heisst ohne den Gesprächsinhalt.» Der Stimmabdruck werde ausschliesslich zu Authentifikationszwecken verwendet.[19]

Die PostFinance ist keinesfalls das einzige Unternehmen, welches die Stimmbiometrie zu Authentifizierungszwecken verwendet. Eingesetzt wurde das Verfahren auch bei der Swisscom, und zwar nach demselben Muster wie bei der PostFinance.[20] Allerdings hat die Swisscom das Experiment wieder abgebrochen.[21] Sodann sollen auch immer mehr Banken die Stimmbiometrie einsetzen.[22] Es handelt sich also keineswegs um ein Einzelphänomen, sondern um einen allgemeinen Trend. Der Eidgenössische Datenschutzbeauftragte sieht das gewählte Vorgehen beim Stimmabdruck kritisch, er fordert eine ausdrückliche Zustimmung.[23] Die PostFinance will Medienberichten zufolge am bestehenden Modell festhalten, bis das neue Datenschutzgesetz in Kraft ist.[24]

---

18 Zum Ganzen siehe die Informationen der PostFinance, abrufbar unter: <www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

19 Informationen der PostFinance, abrufbar unter: <https://www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

20 Tagesanzeiger vom 5. März 2019 («Wie unsere Stimme alles über uns verrät»), abrufbar unter: <https://www.tagesanzeiger.ch/digital/internet/wie-unsere-stimme-alles-ueber-uns-verraet/story/18087714>.

21 Inside-IT vom 2. Mai 2019 («Swisscom lässt Stimmerkennung sein»), abrufbar unter: <https://www.inside-it.ch/articles/54323>.

22 NZZ vom 24. April 2019 («Unsere Stimme sagt alles über uns – auch das, was wir gar nicht sagen wollen»), abrufbar unter: <https://www.nzz.ch/feuilleton/unsere-stimme-sagt-alles-ueber-uns-auch-das-was-wir-gar-nicht-sagen-wollen-ld.1380929>.

23 EDÖB, Erläuterungen zum Stimmerkennungsverfahren (Stand 17. April 2017).

24 Siehe dazu die Zusammenfassung der Sendung «10vor10» vom 20. Mai 2019 auf www.srf.ch. Offensichtlich wird diese Haltung auch dadurch, dass die PostFinance die Stimmerkennung nach wie vor einsetzt (Stand: 7. Mai 2019).

Bei dieser Ausgangslage lohnt sich ein vertiefter Blick auf die spezifische Frage der Zulässigkeit der Verwendung der Stimmbiometrie, wie es die PostFinance und möglicherweise auch zahlreiche andere Banken verwenden.

III. Datenschutzrechtliche Relevanz des Stimmabdrucks

1. Anwendbarkeit des Datenschutzgesetzes

Das DSG ist auf das Bearbeiten von Daten natürlicher und juristischer Personen durch private Personen und Bundesorgane anwendbar (Art. 2 Abs. 1 DSG).[25]

Die PostFinance ist eine privatrechtliche Aktiengesellschaft, an der die Schweizerische Post AG die Mehrheitsbeteiligung hält (vgl. Art. 14 Abs. 1 und 2 POG[26]). Sie erfüllt private Aufgaben und tritt ihren Kundinnen und Kunden gegenüber nicht hoheitlich, sondern privatrechtlich entgegen, weshalb sie nicht als Bundesorgan i.S.v. Art. 3 Bst. h DSG, sondern als Privatperson zu betrachten ist.[27] Das gilt entsprechend für die Kantonalbanken; bei den übrigen Banken stellt sich die Frage einer hoheitlichen Rechtsbeziehung zum Kunden nicht – und sie stellt sich auch nicht bei den Dienstleistern aus anderen Segmenten, die hier nicht im Fokus stehen.

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 Bst. a DSG). Erfasst sind sowohl Tatsachenfeststellungen als auch Werturteile, ungeachtet ihrer Erscheinungsform (z.B. Bild, Ton, Schrift).[28] Eine Person ist bestimmt, wenn sich ihre Identität aus der konkreten Information selbst ergibt.[29] Bestimmbar ist sie dann, wenn sich ihre Identität aus dem Kontext der Information ermitteln lässt, wobei der Begriff aufgrund der heutigen technischen Möglichkeiten «äusserst weit zu fassen» ist.[30]

---

25 Zu den Ausnahmen vom Geltungsbereich siehe Art. 2 Abs. 2 DSG.

26 Bundesgesetz über die Organisation der Schweizerischen Post (Postorganisationsgesetz) vom 17. Dezember 2010, SR 783.1.

27 Die PostFinance wurde auch vom EDÖB in der Affäre E-Cockpit und Bicicletta als Privatperson betrachtet, vgl. EDÖB, Schlussbericht PostFinance, S. 6. Zur Abgrenzung zwischen Bundesorganen und Privatpersonen im Rahmen des DSG vgl. z.B. HK DSG-ROSENTHAL, Art. 3 N 99 ff.

28 BSK-DSG-BLECHTA, Art. 3 N 6.

29 BSK-DSG-BLECHTA, Art. 3 N 9.

30 BSK-DSG-BLECHTA, Art. 3 N 10 f. Siehe dazu auch BGE 138 II 346 E. 6.1 S. 353 f. (Google Street View)

Eine Bearbeitung ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (Art. 3 Bst. e DSG).

Wenn die PostFinance oder ein anderer Dienstleister die Stimme ihre Kundin aufzeichnet und daraus einen Stimmabdruck erstellt, der die Identität dieser Kundin künftig verifizieren soll, bearbeitet sie deren Personendaten. Sie fällt daher in den Anwendungsbereich des DSG.

2. Bearbeitung besonders schützenswerter Personendaten

Besonders schützenswerte Personendaten sind Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative oder strafrechtliche Verfolgungen oder Sanktionen (Art. 3 Bst. c DSG).

Ob auch biometrische Daten zu den besonders schützenswerten Personendaten gehören, ist umstritten. Ein Teil der Lehre subsumiert biometrische Daten unter die Gesundheitsdaten i.S.v. Art. 3 Bst. c DSG.[31] Nach einer anderen Meinung gehören biometrische Daten nicht *per se* zu den besonders schützenswerten Personendaten, sondern nur, wenn sie Rückschlüsse auf solche zulassen.[32] Die blosse Möglichkeit eines solchen Rückschlusses scheint nach dieser Meinung auszureichen.[33] Weiter wird die Ansicht vertreten, dass es sich bei biometrischen Daten erst dann um besonders schützenswerte Personendaten handle, wenn sie gezielt hinsichtlich des betreffenden Merkmals ausgewertet würden.[34]

Die letzte Ansicht ist abzulehnen, weil es bei der Qualifikation eines Personendatums nicht auf den konkreten Bearbeitungsvorgang ankommen kann. Entscheidend ist der informationelle Gehalt des Personendatums an

---

31 SPRECHER, ZBJV 154/2018, 494.

32 HK DSG-ROSENTHAL, Art. 3 N 43.

33 Vgl. HK DSG-ROSENTHAL, Art. 3 N 43, der in seinem Beispiel den Konjunktiv verwendet: «wenn beim Irisscan aus der Iris auch Angaben über den Gesundheitszustand gewonnen werden könnten»; Gl.M. wohl auch BSK-DSG-BLECHTA, Art. 3 N 33: «Im Hinblick auf die Angaben über die Gesundheit i.S. des Gesetzes werden alle Informationen erfasst, die, auf welche Art auch immer, Rückschlüsse auf den körperlichen oder geistigen Gesundheitszustand einer Person erlauben.» Siehe zudem EDÖB, Leitfaden biometrische Daten, S. 17 N 3.3.4.

34 VASELLA, Stimmerkennung, *in fine*.

sich: Ist es möglich, daraus Informationen über den Gesundheitszustand oder ein sonstiges in Art. 3 Bst. c DSG genanntes Merkmal zu gewinnen, handelt es sich um ein besonders schützenswertes Personendatum. Die Diskussion dürfte sich ohnehin bald erledigt haben, da biometrische Daten sowohl nach DSGVO[35] als auch nach E-DSG[36] zu den besonders schützenswerten Personendaten zählen.

Anhand unserer Stimme erkennen Algorithmen mittlerweile nicht nur Alter, Geschlecht, Ethnie und regionale Herkunft der betroffenen Person,[37] sondern auch Erkrankungen wie ADHS, Depressionen und Parkinson.[38] Überdies können sie aus unserer Stimme auf Charaktereigenschaften schliessen und beispielsweise auswerten, wie neugierig, verträglich, risikofreudig, ausgeglichen und organisiert wir sind.[39] Auch unsere Emotionen bleiben ihnen nicht verborgen.[40]

Die Möglichkeit, Rückschlüsse auf besonders schützenswerte Personendaten wie namentlich die Gesundheit und Ethnie einer Person zu ziehen, weist die Stimme dem Kreis der besonders schützenswerten Personendaten zu. Entsprechend beinhaltet die Erstellung des Stimmabdrucks eine Bearbeitung besonders schützenswerter Personendaten.

---

35 Verordnung (EU) 2015/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119 vom 4.5.2016, S. 1-88, siehe Art. 9 Abs. 1 DSGVO.

36 Entwurf zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017, S. 7193-7276); siehe Art. 4 Bst. c Ziff. 4 E-DSG.

37 WELT vom 6. März 2019 («Audioprofiling, Diese Stimmanalyse entlarvt all unsere Geheimnisse»), abrufbar unter: <https://www.welt.de/wissenschaft/article138138577/Diese-Stimmanalyse-entlarvt-all-unsere-Geheimnisse.html>; Tagesanzeiger vom 5. März 2019 («Wie unsere Stimme alles über uns verrät») abrufbar unter: <https://www.tagesanzeiger.ch/digital/internet/wie-unsere-stimme-alles-ueber-uns-verraet/story/18087714>.

38 Siehe z.B. DIE ZEIT Nr. 33/2016 vom 4. August 2016 (« Stimme, Wie Krankheiten aus uns sprechen»), abrufbar unter: <https://www.zeit.de/2016/33/menschliche-stimme-lunge-sprache-krankheit-mund-kehlkopf>; WELT vom 6. März 2019 («Audioprofiling, Diese Stimmanalyse entlarvt all unsere Geheimnisse»), abrufbar unter: <https://www.welt.de/wissenschaft/article138138577/Diese-Stimmanalyse-entlarvt-all-unsere-Geheimnisse.html>.

39 WOLFANGEL, digma 2019, 28.

40 WOLFANGEL, digma 2019, 30.

3. Folgen für die Untersuchung

Mit Blick auf die vorangehenden Ausführungen kann man festhalten, dass die Anfertigung eines Stimmabdrucks eine Personendatenbearbeitung im Sinne des Datenschutzgesetzes darstellt, weshalb der Vorgang in den Anwendungsbereich des Datenschutzgesetzes fällt. Entsprechend sind die allgemeinen Voraussetzungen für die Bearbeitung von Personendaten zu beachten, namentlich darf die Bearbeitung die Persönlichkeit der betroffenen Person nicht verletzen (dazu sogleich). Weil sodann die Anfertigung eines Stimmabdrucks als Bearbeitung von besonders schützenswerten Personendaten qualifiziert, sind die zusätzlichen Voraussetzungen und Rahmenbedingungen zu beachten, welche das DSG für diese Kategorie von Personendaten vorsieht.

IV. Stimmabdruck als Persönlichkeitsverletzung?

Für jede Bearbeitung von Personendaten, also auch für solche, die nicht besonders schützenswert sind, enthält das DSG die Vorschrift, dass die Bearbeitung die Persönlichkeit der betroffenen Person nicht verletzen darf.

1. Persönlichkeitsverletzung nach DSG

Gemäss Art. 12 DSG darf, wer Personendaten bearbeitet, die Persönlichkeit der betroffenen Person nicht verletzen. Der Persönlichkeitsschutz des DSG stellt gemäss Botschaft 1988 eine «Ergänzung und Konkretisierung des Persönlichkeitsschutzes des Zivilgesetzbuches» dar und folgt «den Grundsätzen des Persönlichkeitsschutzes des Zivilgesetzbuches».[41] Wie schon im System des ZGB ist eine Persönlichkeitsverletzung widerrechtlich, wenn sie nicht aufgrund des Gesetzes, des überwiegenden öffentlichen oder private Interesses oder der Einwilligung der Verletzten gerechtfertigt ist (Art. 13 Abs. 1 DSG und Art. 28 Abs. 2 ZGB).

Sowohl Art. 12 als auch Art. 13 DSG enthalten zusätzliche Konkretisierungen. Art. 12 Abs. 2 DSG hält fest, was der Datenbearbeiter «namentlich» nicht tun darf: Er darf bestimmte Datenbearbeitungsgrundsätze[42] nicht verletzen (lit. a); er darf keine Daten entgegen dem ausdrücklichen Willen der betroffenen Person bearbeiten (lit. b); er darf nicht ohne Rechtfertigungsgrund beson-

41 Botschaft DSG, BBl 1988, 458.

42 Das Gesetz nennt Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG.

ders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekannt geben (lit. c). Art. 13 Abs. 2 DSG hält fest, wann «insbesondere» ein überwiegendes privates Interesse infrage kommt – wobei die Beispiele nicht bindend sind.[43]

Weder die persönlichkeitsverletzende Datenbearbeitung noch der Rechtfertigungsgrund des überwiegenden Interesses sind in Art. 12 Abs. 2 und 13 Abs. 2 DSG abschliessend geregelt.[44] Das ist zwar unbestritten, wird aber dennoch zuweilen übersehen. Das liegt nicht zuletzt an der kleinteiligen Regelung des Datenschutzgesetzes, das aus so vielen Bäumen besteht, dass man oft den Wald nicht mehr sieht. Das gilt insbesondere für die Datenbearbeitungsgrundsätze (Art. 12 Abs. 2 lit. a DSG). Sie konkretisieren den Tatbestand der Persönlichkeitsverletzung (Art. 12 Abs. 1 DSG) im Hinblick auf gewisse Datenbearbeitungsszenarien. Darüberhinaus bleibt aber bei jeder Datenbearbeitung die Grundnorm in Art. 12 Abs. 1 DSG (und damit letztlich Art. 28 Abs. 1 ZGB) für die Frage eines Verletzungstatbestands massgeblich.[45]

2. Die Stimme als Teil der rechtlich geschützten Persönlichkeit

Es existieren verschiedene Definitionen der Persönlichkeit. Prägend sind die Definitionen von TERCIER und JÄGGI. TERCIER definiert die Persönlichkeit als «l'ensemble des biens inhérents à chaque personne, biens qui lui appartiennent de sa naissance à sa mort de par sa seule qualité de personne physique ou morale».[46] Nach JÄGGI ist die Persönlichkeit «der Einzelne als Geistwesen und in seiner Einmaligkeit, mit der Gesamtheit seiner Anlagen und Tätigkeiten in der ihm eigenen Ausprägung.»[47] Die verschiedenen Teilgehalte der Persönlichkeit lassen sich nicht abschliessend festlegen, sondern können und müssen – auch mit Rücksicht auf neue Eingriffsszenarien – laufend weiterentwickelt werden.[48]

Ein Gut, welches jeder (gesunden) natürlichen Person inhärent ist und von der Geburt bis zum Tode zu ihr gehört, ist ihre Stimme. Sie ist «der vitalste

43 HK DSG-ROSENTHAL, Art. 13 N 33.

44 HK DSG-ROSENTHAL, Art. 12 N 14 und Art. 13 N 33.

45 Herrschende Lehre. Statt vieler BSK-DSG-RAMPINI, Art. 12 N 7; HK DSG-ROSENTHAL, Art. 12 N 3.

46 TERCIER, personnalité, N 103.

47 JÄGGI, ZSR 79 II (1960), 146a.

48 BSK-ZBG-MEILI, Art. 28 N 5, m.w.H; AEBI-MÜLLER, Persönlichkeitsschutz, § 2 N 33.

Ausdruck zwischenmenschlicher Beziehungen.»[49] Sie ist bei jedem Menschen einzigartig und daher Teil seiner Persönlichkeit.[50] Lehre und Rechtsprechung zählen sie daher zum Schutzbereich von 28 ZGB (teilweise wird von einem Recht an der eigenen Stimme gesprochen).[51] Konkret handelt es sich dabei um einen Schutz vor Eingriffen Dritter, der verbietet, dass die Stimme einer Person ohne Rechtfertigungsgrund beschafft, weiterverbreitet oder verfälscht wird.[52] Vorausgesetzt ist, dass die betroffene Person individualisierbar ist, man also weiss, zu wem die Stimme gehört.[53]

3. Der Stimmabdruck als Persönlichkeitsverletzung

Fällt bereits die blosse Aufnahme einer individualisierbaren Stimme in den Schutzbereich der Persönlichkeit,[54] muss dies erst recht für die Analyse der individuellen Stimme der Kundin zwecks biometrischer Erkennung gelten.[55] Die Stimme ist dermassen eng und dauerhaft mit der betroffenen Person verbunden, dass eine Analyse derselben zwangsläufig in ihren höchstpersönlichen Bereich eingreift. Überdies wird mit dem Stimmabdruck ein neuer Identifikator für die betroffene Person geschaffen. Es steht weder Bundesorganen noch (viel weniger) Privaten zu, beliebig biometrische Merkmale von Personen zu vermessen und daraus Identifikatoren anzufertigen. Bereits aus diesen Gründen stellt der Stimmabdruck eine Persönlichkeitsverletzung dar.

---

49 LOBE, NZZ vom 27. April 2018 («Unsere Stimme sagt alles über uns – auch das, was wir gar nicht sagen wollen»), abrufbar unter: <https://www.nzz.ch/feuilleton/unsere-stimme-sagt-alles-ueber-uns-auch-das-was-wir-gar-nicht-sagen-wollen-ld.1380929>.

50 GEISER, Persönlichkeitsverletzung, 43; AEBI-MÜLLER, Persönlichkeitsschutz, § 2 N 44.

51 BGE 110 II 411 E. 3b S. 418 f.; BARRELET/WERLY, Communication, N 1513; BSK-ZGB-MEILI, Art. 28 N 22; BRÜCKNER, Personenrecht, N 632 f.; GEISER, Persönlichkeitsverletzung, 43 ff.; PEDRAZZINI/OBERHOLZER, Personenrecht, 136; TERCIER, personnalité, N 452 ff.; WEBER/UNTERNÄHRER/ZULAUF, Filmrecht, 159 f.

52 WEBER/UNTERNÄHRER/ZULAUF, Filmrecht, 159 f.; BSK-ZGB-MEILI, Art. 28 N 22, m.w.H; TERCIER, personnalité, N 457; restriktiver hingegen GEISER, Persönlichkeitsverletzung, 45.

53 BARRELET/WERLY, Communication, N 151.; BSK-ZGB-MEILI, Art. 28 N 22, m.w.H.; PEDRAZZINI/OBERHOLZER, Personenrecht, 136; TERCIER, personnalité, N 452 ff.; WEBER/UNTERNÄHRER/ZULAUF, Filmrecht, 159 f.

54 Siehe die Ausführungen im vorangehenden Absatz. Ausdrücklich für die Aufnahme eines Bildes einer Person BGE 138 II 346 E. 8.3 S. 360 (Google Street View).

55 Beim Stimmabdruck ist die Individualisierbarkeit der Stimme ohne Weiteres gegeben. Die Kundin ist der Bank bekannt, der Stimmabdruck ist ihr mit exakt dem Zweck zugeordnet, sie anlässlich eines nächsten Anrufs zu identifizieren. Diese Voraussetzung für eine Persönlichkeitsverletzung ist also mit dem Stimmabdruck ohne Weiteres erfüllt.

Die Verletzung ist zudem schwerwiegend. Denn mit der Stimmerkennung wird ein dauerhafter Identifikator für eine Person geschaffen – für das gesamte Leben, und genau genommen darüber hinaus. Die betroffene Person kann diesen Identitifikator nicht verändern und der Identifikator kann bei einem Abhandenkommen auch nicht einfach neu eingestellt werden, wie dies etwa bei einem Passwort der Fall ist. Selbst im Vergleich zu anderen biometrischen Erkennungsverfahren ist die Stimmbiometrie einzigartig: Wer über sie verfügt, kann die betroffene Person identifizieren, ohne dass der Identifikationsprozess für diese erkennbar ist. Bei einem Irisscan oder bei einem Fingerabdruck muss demgegenüber die betroffene Person im Rahmen eines Authentifizierungsverfahrens für den Abgleich noch einmal ihre Biometrie zur Verfügung stellen – sie muss sich vor einen Irisscanner stellen oder ihren Finger auf eine Scanstelle legen. Sie ist sich also bewusst, dass ein biometrisches Kontrollverfahren stattfindet und dass ihr Gegenüber über ihre diesbezüglichen Daten verfügt.[56]

Aus dem Gesagten folgt, dass die Erstellung des Stimmabdrucks eine Persönlichkeitsverletzung i.S.v. Art. 28 ZGB darstellt. Dies gilt auch auf der Ebene des Datenschutzgesetzes (Art. 12 Abs. 1 DSG), nachdem dieser Vorgang gleichzeitig eine Bearbeitung personenbezogener Daten der Kundin beinhaltet.

Ob darüberhinaus eine Persönlichkeitsverletzung vorliegt, weil mit der Stimmerkennung die Datenbearbeitungsgrundsätze in Art. 12 Abs. 2 lit. a DSG verletzt sind, muss nicht zusätzlich geprüft werden – Fragen würden hier insbesondere der Grundsatz der Verhältnismässigkeit und der Grundsatz von Treu und Glauben aufwerfen. Denn Art. 12 Abs. 2 lit. a DSG gilt nur in eine Richtung: Der Gesetzgeber hat mit dieser Norm in Konkretisierung

[56] Vorbehalten sind Überlistungsszenarien, die allerdings auf einer anderen Ebene liegen. Dort geht es darum, dass man das Sicherheitsdispositiv, das auf einen biometrischen Identifikator beruht, austrickst: Man überlistet den Irisscanner oder man überlistet das Fingerabdruck-Kontrollsystem oder man überlistet das Stimmabdruck-System, indem man den entsprechenden Identifikator ohne Zustimmung und Wissen der betroffenen Person nachkonstruiert und sich dann als die betreffende Person ausgibt. Dies ist ein weiteres Risikoszenario bei biometrischen Daten, die alle diese Daten aber gleichermassen betrifft.

von Art. 28 ZGB und Art. 12 Abs. 1 DSG die Fiktion einer Persönlichkeitsverletzung geschaffen.[57] Wer einzelne Datenbearbeitungsgrundsätze nicht einhält, verletzt *per se* das Persönlichkeitsrecht der betroffenen Person.[58] Mit dieser Fiktion wird die Anwendung des allgemeinen Persönlichkeitsschutzes im Kontext der Datenverarbeitung im Hinblick auf einzelne Konstellationen vereinfacht. Das Umgekehrte gilt aber nicht: Die Einhaltung sämtlicher Datenbearbeitungsgrundsätze bedeutet nicht, dass *keine* Persönlichkeitsverletzung vorliegt.[59] Wie bereits erwähnt, kann eine Persönlichkeitsverletzung sogar dann vorliegen, wenn gar keiner der Tatbestände in Art. 12 Abs. 2 Bst. a-c DSG erfüllt ist.

4. Die Weitergabe des Stimmabdrucks als Persönlichkeitsverletzung

Art. 12 Abs. 2 lit. c DSG enthält eine Konkretisierung der persönlichkeitsverletzenden Datenbearbeitung: Die Weitergabe von besonders schützenswerten Personendaten erfüllt ohne Weiteres den Verletzungstatbestand gemäss Art. 12 DSG. Im Fall der Banken steht diese Konstellation allerdings nicht im Vordergrund, weil es zunächst einmal nur um die Frage geht, ob Banken und andere Dienstleister den Stimmabdruck selbst erstellen und nutzen dürfen.

V. Rechtfertigungsgründe nach DSG im Überblick

Gemäss Art. 13 Abs. 1 DSG ist eine Persönlichkeitsverletzung widerrechtlich, wenn sie nicht durch die Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist (vgl. Art. 13 Abs. 1 DSG).

Eine gesetzliche Grundlage ist für die Erstellung des Stimmabdrucks nicht ersichtlich. Gemäss Art. 179quinquies StGB ist zwar die Stimmaufnahme nicht strafbar, wenn die aufgenommenen Gespräche «Bestellungen, Aufträge, Reservationen und ähnliche Geschäftsvorfälle zum Inhalt haben». In solchen Fällen besteht auch ein zivilrechtlicher Rechtfertigungsgrund.[60] Erstens ist zweifelhaft, ob die Hotline eines Finanzdienstleisters überhaupt unter diesen

---

57 Botschaft DSG, BBl 1988, 458; BSK-DSG-RAMPINI, Art. 12 N 1, 6; HK DSG-ROSENTHAL, Art. 12 N 14.

58 Vgl. BSK-DSG-RAMPINI, Art. 12 N 6; HK DSG-ROSENTHAL, Art. 12 N 14.

59 Vgl. BSK-DSG-RAMPINI, Art. 12 N 7.

60 Vgl. EDÖB, Aufzeichnung von Telefongesprächen.

Tatbestand fällt.[61] Zweitens erstreckt sich der Rechtfertigungsgrund mit Sicherheit nicht auf die Erstellung eines Stimmabdrucks.

Öffentliche Interessen spielen bei privaten Datenbearbeitern als Rechtfertigungsgrund eine untergeordnete Rolle.[62] Sie lassen sich aufgrund ihrer zeitlichen und örtlichen Wandelbarkeit nicht abschliessend definieren.[63] Die wichtigsten Gruppen sind die polizeilichen Interessen wie z.B. die öffentliche Ordnung und Sicherheit oder Treu und Glauben im Geschäftsverkehr, planerische Interessen (z.B. Raumplanung), soziale und sozialpolitische Interessen (z.B. Arbeitnehmerschutz), und rechtsstaatliche Interessen.[64] Im Bereich des Persönlichkeitsschutzes ist insbesondere das Informationsinteresse der Öffentlichkeit an Personen des öffentlichen Lebens von Bedeutung.[65] Vorliegend ist kein öffentliches Interesse der Banken an der Verwendung von Stimmabdrücken zwecks Authentifikation ihrer Kundinnen und Kunden ersichtlich.

Näher zu prüfen ist hingegen der Rechtfertigungsgrund der Einwilligung, denn immerhin kann die Kundin anlässlich des ersten Anrufs bei der Hotline erklären, dass sie die Anfertigung eines Stimmabdrucks nicht wünscht.[66] Auch der Rechtfertigungsgrund eines überwiegenden privaten Interesses seitens der Banken bedarf einer genaueren Betrachtung, ist doch das Vorliegen eines Interesses offenkundig, was allerdings noch nicht bedeutet, dass dieses Interesse überwiegt.

VI. Rechtfertigung durch Einwilligung?

Die Anforderungen an die Einwilligung sind in Art. 4 Abs. 5 DSG festgehalten. Danach ist die Einwilligung nur gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung besonders schützenswerter Personendaten muss die Einwilligung zudem ausdrücklich erfolgen.

---

61 Wie der EDÖB unter Hinweis auf die parlamentarischen Beratungen richtig festhält, geht es um Bestell- bzw. Reservationsanrufe (z.B. in der Tourismusbranche) und nicht um Gespräche, die Reklamationen oder Vertragsverhandlungen zum Inhalt haben.

62 HK DSG-ROSENTHAL, Art. 13 N 20.

63 HÄFELIN/MÜLLER/UHLMANN, Verwaltungsrecht, § 7 N 465.

64 HÄFELIN/MÜLLER/UHLMANN, Verwaltungsrecht, § 7 N 471 ff.; BVerG A-7040/2009 vom 30. März 2011, E. 10.4.2 (Google Street View).

65 HK DSG-ROSENTHAL, Art. 13 N 22.

66 Siehe vorne III. (Eingangsparagraph).

1. Angemessene Information

a) Anforderungen

Angemessen informiert ist die betroffene Person dann, wenn sie über alle notwendigen Informationen verfügt, um die Tragweite der Einwilligung in die konkrete Datenbearbeitung zu erkennen,[67] oder kurz: «wenn die Eingriffe in die Persönlichkeitsrechte transparent werden».[68] Der betroffenen Person müssen mindestens die Datenbearbeiter, Art, Zweck und Umfang der Bearbeitung sowie gegebenenfalls deren Risiken bekanntgegeben werden.[69] Auch die Folgen einer Verweigerung der Einwilligung sind der betroffenen Person mitzuteilen.[70]

Diese Informationen müssen ihr in leicht verständlicher Art und Weise präsentiert werden.[71] Aus dem klaren Wortlaut («*nach* angemessener Information») ergibt sich, dass die Information *vor* der Erteilung der Einwilligung zu erfolgen hat.[72] Nicht erforderlich ist eine Information über Risiken, die allgemein bekannt sind oder die für die betroffene Person auch ohne Information erkennbar sind.[73] Sowohl der notwendige Umfang als auch die Form der Information richten sich nach den Umständen des Einzelfalls.[74]

b) Angemessene Information durch telefonische Ansage?

Orientiert man sich wiederum am medial verbreiteten Beispiel der PostFinance, so informiert diese ihre Kundinnen und Kunden einerseits mittels folgender telefonischer Ansage:

> «Dieses Gespräch wird zu Sicherheits- und Wiedererkennungszwecken aufgezeichnet. PostFinance erstellt aus der Aufnahme einen Stimmabdruck, um

---

67 BVerG A-3908/2008 vom 4. August 2009, E. 4.2; EPINEY, in: Belser/Epiney/Waldmann, § 9 N 17; HK DSG-ROSENTHAL, Art. 4 N 72.

68 SHK-BAERISWYL, Art. 4 N 59.

69 EPINEY, in: Belser/Epiney/Waldmann, § 9 N 17; ebenso BSK-DSG-MAURER-LAMBROU/STEINER, Art. 4 N 16f. BAERISWYL verlangt zusätzlich noch die Angabe der Kategorien der bearbeiteten Daten, SHK-BAERISWYL, Art. 4 N 59.

70 BSK-DSG-MAURER-LAMBROU/STEINER, Art. 4 N 16f.

71 EPINEY, in: Belser/Epiney/Waldmann, § 9 N 17; BSK-DSG-MAURER-LAMBROU/STEINER, Art. 4 N 16f.

72 So zu Recht auch HK DSG-ROSENTHAL, Art. 4 N 72; einschränkend WERMELINGER/SCHWERI, Jusletter 3.3.2008, Rz. 12.

73 HK DSG-ROSENTHAL, Art. 4 N 74.

74 EPINEY, in: Belser/Epiney/Waldmann, § 9 N 17.

> Ihre Identität bei jeden [recte: jedem] Anruf anhand Ihrer Stimme zu verifizieren. Wünschen Sie keinen Stimmabdruck, bitten wir Sie, dies dem Kundenbetreuer mitzuteilen.»

Die Ansage enthält Informationen über die Datenbearbeiterin (PostFinance), die Bearbeitungszwecke (Sicherheit, Wiedererkennung bei künftigen Anrufen), die Art der Datenbearbeitungen (Aufnahme des Gesprächs, Erstellung eines Stimmabdrucks und seine spätere Verwendung zwecks Verifikation) sowie eine Belehrung der Kundin über ihr Widerspruchsrecht.

Allerdings ist nicht davon auszugehen, dass die Durchschnittskundin aufgrund dieser Ansage die effektive Tragweite der geplanten Datenbearbeitung wirklich erfasst. Insbesondere kann nicht unterstellt werden, eine Durchschnittskundin wisse ohne Weiteres, was mit einem Stimmabdruck gemeint ist (nämlich die Festlegung eines unabänderlichen Identifkators), und dass sie Fremdwörter wie «Identität» und «verifizieren» versteht.

Die telefonische Information ist somit für sich alleine nicht als angemessen zu betrachten. Entsprechend kann gestützt darauf keine gültige Einwilligung erteilt werden.

c) Angemessene Information durch Website?

Die telefonische Ansage bei einer Hotline kann durch weiterführende Informationen auf der Website des Dienstleisters komplementiert werden.

Auf der Website der PostFinance[75] wird der Kundin beispielsweise erklärt, dass aus den verschiedenen Merkmalen ihrer Stimme wie Sprechtempo, Lautstärke und Frequenz ein Stimmabdruck erstellt werde, der in Form eines Codewerts ohne Gesprächsinhalt auf den Servern der PostFinance in der Schweiz gespeichert werde. Diesen Stimmabdruck benutze die PostFinance, um festzustellen, «ob die Person, die anruft, tatsächlich diejenige ist, als die sie sich ausgibt». Auch zu gewissen mit der Stimmerkennung verbundenen Herausforderungen (z.B. Heiserkeit der Kundin, ähnliche Stimme einer Verwandten) nimmt die PostFinance in verständlicher Art und Weise Stellung.[76]

Fraglich ist, ob diese zusätzlichen Informationen dazu führen, dass von einer gültigen Einwilligung ausgegangen werden kann. Das ist aus zwei Gründen zu verneinen. Erstens ist nicht sichergestellt – es ist sogar unwahr-

---

[75] Siehe unter <www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

[76] Zum Ganzen <www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

scheinlich –, dass die Kundin das Telefongespräch in Kenntnis der Informationen auf der Website vornimmt. Insofern fällt die zusätzliche Information für die Frage der rechtsgültigen Einwilligung ausser Betracht. Doch selbst wenn man die Webinformationen dem Telefongespräch ausnahmsweise «zurechnen» könnte, so würde sie – zweitens – nicht genügen, weil sie in ungenügendem Mass auf die Risiken hinweist, die mit einem solchen Vorgang verbunden sind. Die Verbindung zwischen einer Person und ihrer Stimme ist hochsensibel. Wird auf irgendeine Art und Weise bekannt, dass ein Stimmabdruck zu einer bestimmten Person gehört, so kann diese Person künftig überall allein durch ihre Stimme identifiziert werden.[77] Eine angemessene Information der Kundin würde daher voraussetzen, dass sie über dieses Risiko aufgeklärt wird und dass die Massnahmen geschildert werden, mit denen die PostFinance dieses Risiko zu verhindern sucht. Ansonsten kann die Kundin die Tragweite ihrer Entscheidung nicht überblicken. Entsprechend liegt auch in diesem Fall keine rechtsgenügende Einwilligung vor.

d) Fazit: Keine angemessene Information

Die telefonische Ansage stellt für sich alleine keine angemessene Information i.S.v. Art. 4 Abs. 5 DSG dar. Selbst wenn darin auf die weiterführenden Informationen auf der Website verwiesen würde, wäre die Information nicht angemessen, da keine genügende Risikoaufklärung stattfindet. Die fehlende Risikoaufklärung führt im Übrigen dazu, dass auch die Zustimmung zum Stimmabdruck, welche die Kundin im Online-Banking-Portal vornimmt, die Voraussetzungen für eine rechtsgültige Einwilligung nach DSG nicht erfüllt.

2. Freiwilligkeit

Die Freiwilligkeit der Einwilligung ist vorliegend relativ unproblematisch, da die Kundin die Möglichkeit hat, der Erstellung eines Stimmabdrucks zu widersprechen und stattdessen anhand von Sicherheitsfragen authentifiziert zu werden. Zu bedenken ist aber, dass sich die Kundinnen und Kunden, die bei einer Hotline, gerade der Hotline einer Bank, anrufen, häufig in einer Drucksituation befinden dürften – beispielsweise, weil ihnen das Portemonnaie abhandengekommen ist und sie ihre Kreditkarte so schnell wie möglich sperren lassen möchten. Ob sie in einer solchen Situation noch die Vor- und Nachteile

[77] Forbes 6. Oktober 2016 («Voice Recognition: Risks To Our Privacy»), abrufbar unter: <https://www.forbes.com/sites/realspin/2016/10/06/voice-recognition-every-single-day-every-word-you-say/>.

der Stimmerkennung abwägen und eine freiwillige Entscheidung treffen können, darf bezweifelt werden.

3. Ausdrücklichkeit (besonders schützenswerte Personendaten)

Wie erläutert,[78] werden bei der Erstellung des Stimmabdrucks besonders schützenswerte Personendaten bearbeitet, weshalb die Einwilligung nicht nur informiert und freiwillig, sondern darüberhinaus ausdrücklich erfolgen muss. Eine ausdrückliche Zustimmung bei Stimmerkennungsverfahren verlangt auch der EDÖB.[79] Der Begriff «ausdrücklich» ist dabei wie im Vertragsrecht gleichbedeutend mit «nicht konkludent».[80]

Wenn nun die Kundin nach Anhörung der elektronischen Ansage das Telefonat nicht beendet, sondern direkt ihr Anliegen an den Kundenberater heranträgt, willigt sie nicht ausdrücklich ein. Eine andere Situation bestünde, wenn der Kundenberater nochmals nachfragen und die Kundin erklären würde, dass sie mit dem Stimmabdruck einverstanden sei. Dann wäre die Einwilligung ausdrücklich. Allerdings wäre sie trotzdem ungültig, da die Kundin nicht angemessen informiert wurde.

4. Fazit: Keine Rechtfertigung durch Einwilligung

Bei der hier untersuchten Ausgestaltung des Zustimmungsverfahrens für die Anfertigung eines Stimmabdrucks fehlt es an der rechtsgültigen Einwilligung: Weder die telefonische noch die webbasierte Information ist von ihrem Inhalt her genügend verständlich und genügend detailliert, um die Voraussetzung einer angemessenen Information zu erfüllen. Selbst wenn man also

78 Siehe oben III.2.

79 EDÖB, Erläuterungen zu Stimmerkennungsverfahren, passim. In den Erläuterungen wird das Stimmerkennungsverfahren nicht ausdrücklich als Bearbeitung besonders schützenswerter Daten qualifiziert, diese Qualifikation ergibt sich aber aus dem geforderten Zustimmungsmodus der Ausdrücklichkeit. Richtig ist allerdings, dass nicht *jede* Bearbeitung besonders schützenswerter Personendaten eine Persönlichkeitsverletzung beeinhaltet und deshalb einer Rechtfertigung bedarf (so auch VASELLA, Stimmerkennung). Das ändert allerdings nichts daran, dass – spezifisch – die Erstellung eines Stimmabdrucks eine Persönlichkeitsverletzung ist, die ohne Rechtfertigungsgrund widerrechtlich ist.

80 Zutreffend und mit Erläuterung der verschiedenen Auslegungen der Lehre VASELLA, Jusletter 16.11.2015, Rz. 21 ff.

annehmen würde, dass es – mangels Bearbeitung von besonders schützenswerten Personendaten – keiner ausdrücklichen Zustimmung bedarf, wären die Voraussetzungen für eine rechtsgültige Einwilligung nicht erfüllt.

Allerdings wird hier vertreten, dass der Stimmabdruck als Bearbeitung von besonders schützenswerten Personendaten zu qualifizieren ist, weshalb die Einwilligung ausdrücklich zu erfolgen hat. Auch dieses weitergehende Erfordernis ist nicht erfüllt, denn die Kundin muss beim aktuellen Verfahren ausdrücklich erklären, dass sie *keinen* Stimmabdruck wünscht. Eine ausdrückliche Einwilligung beinhaltet dieser Vorgang jedenfalls nicht. Im Übrigen ist fraglich, wie die Nichtausübung der Widerspruchsmöglichkeit zu qualifizieren ist: Bei Lichte betrachtet handelt es sich um eine Vertragsänderung, die für ihre Gültigkeit der Zustimmung bedarf. Schweigen gilt im Vertragsrecht nicht als Zustimmung (vgl. Art. 6 OR).

VII. Rechtfertigung durch überwiegende private Interessen?

Falls kein Gesetz, kein überwiegendes öffentliches Interesse und keine gültige Einwilligung für den Stimmabdruck besteht, so bleibt noch zu untersuchen, ob dieser durch das überwiegende private Interesse des Bearbeiters gerechtfertigt ist. Art. 13 Abs. 2 DSG enthält eine nicht abschliessende Auflistung von Situationen, in denen ein überwiegendes privates Interesse «in Betracht» fällt. Diese Formulierung verdeutlicht, dass in den aufgezählten Fällen kein Automatismus greift, sondern stets noch eine Interessenabwägung durchgeführt werden muss, den Beispielen mithin nicht der Rang gesetzlicher Vermutungen zukommt.[81] Sie bilden aber nach der Botschaft «Gewichtssteine» für die Interessenabwägung durch das Gericht.[82] Als mögliche Interessen fallen nicht nur Interessen des Datenbearbeiters, sondern auch Interessen Dritter, insbesondere der betroffenen Person selbst, in Betracht.[83]

1. Mögliche Interessen

Vorliegend ist von den genannten Beispielen nur die Abwicklung eines Vertrages i.S.v. Art. 13 Abs. 2 Bst. a DSG einschlägig, wonach ein überwiegendes

81 HK DSG-ROSENTHAL, Art. 13 N 33; BSK-DSG-RAMPINI, Art. 13 N 26.

82 Botschaft DSG, BBl. 1988, 460.

83 BGE 138 II 346 E. 10.3 S. 364 f. (Google Street View).

Interesse namentlich dann in Betracht fällt, wenn in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten des Vertragspartners bearbeitet werden. Die Norm adressiert den Datenbearbeitungsbedarf, der mit einer Vertragsbeziehung einhergeht, und schafft den notwendigen Spielraum für deren Errichtung und sachgerechte Durchführung. Die Stimmauthentifizierung steht im Zusammenhang mit der Nebenpflicht der Banken, eine Kunden-Hotline zu betreiben und die Kundinnen und Kunden im Falle eines Anrufs zuverlässig zu authentifizieren. Diese Nebenpflicht ist vorliegend zu berücksichtigen.

Aber: Ein Spielraum ist kein Freipass. Auch innerhalb eines Vertragsverhältnisses ist die Persönlichkeit der Gegenpartei zu wahren. Art. 13 Abs. 2 Bst. a DSG vermag mit anderen Worten nicht unbesehen jede Persönlichkeitsverletzung zu rechtfertigen, sondern erfordert eine Interessenabwägung im Einzelfall.[84] Da hier mildere Mittel für die Authentifizierung der Kundinnen und Kunden möglich sind (Stichwort: Sicherheitsfragen), dürfte das Interesse der Bank an der Erfüllung ihrer Nebenpflicht für sich alleine nicht ausschlaggebend sein.

Zu prüfen ist daher, welche Interessen die Banken daran haben, diese Nebenpflicht *spezifisch mittels Stimmerkennung* zu erfüllen. Medienberichten zufolge sind dies einerseits das Interesse an einer schnelleren Authentifikation der Kundinnen und Kunden und andererseits das Interesse an einer sichereren Verifizierung und insbesondere der Verhinderung von Identitätsdiebstahl.[85]

2. Effiziente Kundenauthentifizierung

Als berechtigte Interessen i.S.v. Art. 13 DSG kommen auch rein wirtschaftliche Interessen infrage, wie z.B. das Interesse an einer effizienten Gestaltung der Datenbearbeitung.[86] Das Interesse, die Kundenauthentifizierung möglichst zeit- und ressourcensparend zu gestalten ist daher ein berechtigtes Interesse.

Das Stimmerkennungsverfahren hat gegenüber den Sicherheitsfragen den Vorteil der Zeitersparnis. Textgebundene Stimmerkennungsverfahren ver-

---

84 Allgemein zur Notwendigkeit einer Interessenabwägung bei den Rechtfertigungsgründen nach Art. 13 Abs. 2 DSG siehe HK DSG-ROSENTHAL, Art. 13 N 6.

85 Inside-IT vom 18. Dezember 2018 («PostFinance setzt auf Stimmerkennung zur Authentifizierung»), abrufbar unter: <www.inside-it.ch/articles/53194>.

86 BGE 138 II 346 E. 10.3 S. 364 f. (Google Street View).

langen nur das Sprechen eines vorgegebenen Textes und nicht die Beantwortung mehrerer Fragen, textungebundene Verfahren laufen gar im Hintergrund des Kundengesprächs ab. Sie nehmen daher weniger Zeit für die Authentifikation der Kundin in Anspruch und das Gespräch kann sich stärker auf das konkrete Anliegen der Kundin konzentrieren. Überdies dauern die Kundengespräche generell weniger lange, was einerseits die Ressourcen der Bank schont und andererseits die Nerven der übrigen Kundinnen und Kunden, die weniger lange in Warteschlaufen verbringen müssen.

Beim Interesse an einer effizienten Kundenauthentifizierung handelt es sich somit nicht nur um ein Interesse der Bank, sondern auch um ein Interesse der Kundin selbst sowie der übrigen Kundinnen und Kunden.

3. Sicherere Kundenauthentifizierung

Ein weiteres Interesse liegt in der sicheren Kundenauthentifizierung. Auch dieses erfüllt die Voraussetzung eines Interesses «von allgemein anerkanntem Wert»[87] und kann daher in der Interessenabwägung berücksichtigt werden. Die sichere Kundenauthentifizierung liegt gleichzeitig im Interesse der Kundin selbst.

4. Interessenabwägung

Dass die Banken schützenswerte (wirtschaftliche und sicherheitsrelevante) Interessen an der Erstellung von Stimmabdrucken geltend machen können, bedeutet noch nicht, dass diese Interessen die Persönlichkeitsverletzung der Kundin rechtfertigen. Eine Rechtfertigung liegt nur vor, wenn man die Interessen zugunsten der Stimmauthentifizierung höher gewichtet als die Interessen der Kundin am Schutz ihrer Persönlichkeit.

a) Effiziente Kundenauthentifizierung

Anhaltspunkte für diese Interessenabwägung liefert insbesondere die bundesgerichtliche Rechtsprechung. Zwar anerkennt das Bundesgericht die grundsätzliche Eignung des wirtschaftlichen Interesses als Rechtfertigungsgrund, sie lässt dieses Interesse im Regelfall aber nicht genügen.[88] Vor diesem

---

87 BUCHER, Natürliche Personen, N 518.

88 Siehe dazu BGE 138 II 346 E. 10.4, 10.6.1, 10.6.3, S. 365 f., 367, 369 (Google Street View). So auch BSK ZGB-MEILI, Art. 28 N 49, unter Hinweis auf den soeben erwähnten BGE 138 II 346.

Hintergrund fallen die reinen Effizienzinteressen der Banken an einer Authentifizierung mittels Stimmerkennung als Rechtfertigungsgrund ausser Betracht. Das gilt umso mehr, als der Verzicht auf diese Authentifizierungsmethode für die Banken keine schwerwiegenden oder gar existenzbedrohenden Folgen hätte; die Institute verfügten bislang über Alternativen und können diese Alternativen auch für die Zukunft beibehalten und um neue Modelle ergänzen. Im konkreten Abwägungsprozess kommt dem wirtschaftlichen Interesse der Banken also von vornherein kein massgebliches Gewicht zu. Betrachtet man auf der anderen Seite den massiven Eingriff in die Persönlichkeit, der mit einem Stimmabdruck verbunden ist, führt die Interessenabwägung eindeutig dazu, dass der Persönlichkeitsschutz höher zu gewichten ist als das wirtschaftliche Interesse der Banken.

b) Sichere Kundenauthentifizierung

Für die Gesamtabwägung bleiben damit die Sicherheitsaspekte auf der einen Seite und der Persönlichkeitsschutz auf der anderen Seite. Auch hier sind die Sicherheitsinteressen in einem ersten Schritt auf das Gewicht hin zu überprüfen, das ihnen im Abwägungsprozess überhaupt zukommen soll. Hierzu ist festzuhalten, dass Stimmerkennungsverfahren zwar als zuverlässig gelten, sie aber keine vollständige Sicherheit gewähren. Ähnlich klingende Verwandte werden nicht immer herausgefiltert,[89] Systeme wurden in der Vergangenheit mehrfach überlistet.[90] Auch hier bestehen zudem Alternativen, die einen vergleichbaren Sicherheitsstandard bieten, ohne dass eine Persönlichkeitsverletzung in Kauf genommen werden muss, etwa die Ergänzung der Sicherheitsfragen um einen weiteren Überprüfungsfaktor.[91] Mithin besteht

---

89 Siehe dazu BLONSKI, Biometrische Daten, 19. Erst 2017 gelangte das Stimmerkennungssystem der HSBC in die Schlagzeilen, weil es einen BBC-Reporter fälschlicherweise als dessen Bruder authentifizierte. Siehe BBC News 19. Mai 2017 («BBC fools HSBC voice recognition security system»), abrufbar unter: <www.bbc.com/news/technology-39965545>. Die PostFinance äussert sich zu diesem Risiko auf ihrer Website nur ausweichend: <www.postfinance.ch/de/privat/support/persoenliche-daten/authentifizierung-stimmerkennung.html>.

90 So gelang es zwei Sicherheitsforschern, durch Machine Learning synthetische Stimmen zu erzeugen und damit Apples Siri sowie Microsofts Cloud-Dienst Azure Speaker Recognition zu täuschen. Siehe dazu Heise vom 13. August 2019 («Die eigene Stimme als Passwort? Besser nicht ...») abrufbar unter: <https://www.heise.de/newsticker/meldung/Die-eigene-Stimme-als-Passwort-Besser-nicht-4134163.html?view=print>.

91 Z.B. via Mobile-App (wo allfällige biometrische Erkennungsmerkmale lediglich dezentral gespeichert sind), oder mittels Abfragen eines Zugangscodes, der vom Kartenlesegerät generiert wird.

ein schützenswertes, aber kein ausserordentlich schwerwiegendes Sicherheitsinteresse an der Verwendung eines Stimmabdrucks zu Identifizierungszwecken.

Dem Interesse an einer sicheren Authentifizierung stehen der Schutz der Persönlichkeit vor tiefgreifenden und intensiven Eingriffen gegenüber. Wie bereits ausgeführt wurde, stellt ein Stimmabdruck einen massiven Eingriff in die Persönlichkeit der betroffenen Person dar.[92] Die Stimme ist einzigartig und sie ist untrennbar mit der Person verbunden. Mit der Stimmerkennung wird (bis zu einer allfälligen Löschung) ein ewiger, unveränderbarer Identifikator für eine Person geschaffen. Dieser Identifikator hebt sich von den anderen biometrischen Erkennungsmerkmalen zusätzlich ab, indem die betroffene Person ohne weiteres Zutun (also ohne nochmalige Zurverfügungstellung ihrer biometrischen Daten) identifiziert werden kann. Das macht die Verwendung der Stimmbiometrie sehr einfach, aber gleichzeitig im Hinblick auf die eigene Datenherrschaft sehr riskant.

Im Ergebnis ist die Anfertigung eines Stimmabdrucks ein massiver Eingriff in die Persönlichkeit der betroffenen Person, der in keinem Verhältnis zu den Sicherheitsinteressen der Banken beim Authentifizierungsprozess steht. Insgesamt können sich Banken weder auf ihre wirtschaftlichen noch auf ihre sicherheitsbezogenen Interessen berufen, um die persönlichkeitsverletzenden Anfertigung eines Stimmabdrucks zu rechtfertigen.

VIII. Fazit

«Sprich nur ein Wort, und ich sage Dir, wer Du bist.» Mit der Stimmauthentifizierung greifen die PostFinance und andere Banken, die ein solches Verfahren verwenden, in die höchstpersönliche Sphäre ihrer Kundinnen und Kunden ein. Sie schaffen sich aufgrund der bei jedem Menschen einzigartigen und unveränderbaren Stimme einen privaten Identifikator der jeweiligen Kundin oder des jeweiligen Kunden. Dies stellt eine Persönlichkeitsverletzung im Sinne von Art. 12 Abs. 1 DSG dar.

Diese Persönlichkeitsverletzung ist dann nicht widerrechtlich, wenn sie durch das Gesetz, ein überwiegendes öffentliches oder privates Interesse oder durch die Einwilligung seitens der verletzten Person gerechtfertigt ist. Näher in Betracht kommen nur der Rechtfertigungsgrund der Einwilligung und der

[92] Siehe zu diesen Argumenten oben V.3.

Rechtfertigungsgrund des überwiegenden privaten Interesses. Beim hier untersuchten Modellverfahren scheitert die gültige Einwilligung bereits daran, dass an der angemessenen Information fehlt, die Kundin also nicht *informiert* einwilligt. Dass zusätzlich keine ausdrückliche Einwilligung erfolgt, bestätigt nur das bereits gefundene Ergebnis. Ob man also, wie es der EDÖB vertritt, den Stimmabdruck als Bearbeitung besonders schützenswerter Personendaten einstuft, ist für das Ergebnis der fehlenden rechtsgültigen Einwilligung nicht ausschlaggebend. Dennoch verdient die Auffassung des EDÖB Zustimmung: Die Erstellung eines Stimmabdrucks beinhaltet die Bearbeitung besonders schützenswerter Personendaten, weshalb es einer ausdrücklichen Zustimmung bedarf.

Schliesslich vermögen auch die unstreitig vorhandenen Sicherheits- und Effizienzinteressen seitens der Bank die Persönlichkeitsverletzung nicht zu rechtfertigen. In der Interessenabwägung stellen sie angesichts des massiven Eingriffs in den Schutzbereich der Persönlichkeit, den ein Stimmabdruck beinhaltet, kein überwiegendes Interesse dar.

Im Ergebnis wird also mit den bestehenden Modellen der Stimmerkennung das Persönlichkeitsrecht der Kundinnen und Kunden verletzt, womit gleichzeitig gesagt ist, dass auch eine Verletzung des Datenschutzgesetzes vorliegt.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 19. Juni 2019.

AEBI-MÜLLER REGINA E., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Abhandlungen zum schweizerischen Recht, Heft 710, Bern 2005.

BAERISWYL BRUNO/PÄRLI KURT, Datenschutzgesetz (DSG), Stämpflis Handkommentar, Bern 2015 (zit. SHK-BEARBEITER).

BARRELET DENIS/WERLY STÉPHANE, Droit de la communication, 2. Auflage, Bern 2011.

BELSER EVA MARIA/EPINEY ASTRID/WALDMANN BERNHARD, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011.

BLECHTA GABOR P. Art. 3 DSG, in: Urs Maurer-Lambrou / Gabor P. Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Basel 2014.

BLONSKI DOMINIKA, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, ASR – Abhandlungen zum Schweizerischen Recht, Band/Nr. 816, Bern 2015.

BRÜCKNER CHRISTIAN, Das Personenrecht des ZGB (ohne Beurkundung des Personenstandes), Zürich 2000.

BUCHER ANDREAS, Natürliche Personen und Persönlichkeitsschutz, 4. Auflage, Basel 2009.

GEISER THOMAS, Die Persönlichkeitsverletzung insbesondere durch Kunstwerke, Basler Studien zur Rechtswissenschaft, Reihe A: Privatrecht, Band 21, Basel und Frankfurt am Main 1990.

GEISER THOMAS/FOUNTOULAKIS CHRISTIANA (HRSG.), Basler Kommentar Zivilgesetzbuch I, Art. 1-456, 6. Auflage, Basel 2018.

HÄFELIN ULRICH/MÜLLER GEORG/UHLMANN FELIX, Allgemeines Verwaltungsrecht, 7. Auflage, Zürich/St. Gallen 2016.

JÄGGI PETER, Fragen des privatrechtlichen Schutzes der Persönlichkeit, ZSR 1960 II, S. 133a-261a.

MAURER-LAMBROU URS/BLECHTA GABOR P. (HRSG.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Basel 2014 (zit. BSK-DSG-BEARBEITER, Art. […] N. […]).

MAURER-LAMBROU URS/STEINER ANDREA, Art. 4 DSG; in: Urs Maurer-Lambrou/Gabor P. Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Basel 2014.

MEILI ANDREAS, Art. 28 ZGB, in: Thomas Geiser/Christiana Fountoulakis (Hrsg.), Basler Kommentar Zivilgesetzbuch I, Art. 1-456, 6. Auflage, Basel 2018.

PEDRAZZINI MARIO M./OBERHOLZER NIKLAUS, Grundriss des Personenrechts, 4. Auflage, Bern 1993.

RAMPINI CORRADO, Art. 13 DSG, in: Urs Maurerl-Lambrou/Gabor P. Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz Öffentlichkeitsgesetz, 3. Auflage, Basel 2014.

ROSENTHAL DAVID/JÖHRI YVONNE, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich/Basel/Genf 2008 (zit. HK-BEARBEITER, Art. […] N. […]).

SCHALLER JEAN MARC, Legitimationsmängel, in: Susan Emmenegger (Hrsg.), Bankvertragsrecht, Basel 2017, S. 45–70.

SPRECHER FRANZISKA, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, ZBJV 154/2018, 482-519.

TERCIER PIERRE, Le nouveau droit de la personnalité, Zürich 1984.

TILLENBURG GEREON, Stimmt die Stimme? Biometrielösungen im Einsatz, DuD 3/2011, S. 197-199.

VASELLA DAVID, Der EDÖB in «10vor10» zur Stimmerkennung bei PostFinance, 20. Mai 2019, abrufbar unter: < https://datenrecht.ch/der-edoeb-in-10vor10-zur-stimmerkennung-bei-postfinance/>.

– Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, in: Jusletter 16. November 2015.

WEBER ROLF H./UNTERNÄHRER ROLAND/ZULAUF RENA, Schweizerisches Filmrecht, ZIK - Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich, Band/Nr. 25, Zürich/Basel/Genf 2003.

WERMELINGER AMÉDÉO/SCHWERI DANIEL, Teilrevision des Eidgenössischen Datenschutzrechts – Es nützt nicht viel, schadet es etwas?, in: Jusletter 3. März 2008.

WOLFANGEL EVA, Unsere Stimme haben sie, digma 2019, S. 28-31.

Materialien

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988, BBl 1988 II, S. 413-534.

Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2003, S. 2101-2155.

EDÖB, Schlussbericht vom 1. Juni 2015 betreffend Abklärung im Zusammenhang mit E-Cockpit und Bicicletta.

– Leitfaden zu biometrischen Erkennungssystemen, Version 1.0, September 2009, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/do kumentation/leitfaeden/leitfaden-zu-biometrischen-erkennungssystemen.html>

– Aufzeichnung von Telefongesprächen, abrufbar unter: <www.edoeb.admin.ch/edoeb/de/home/datenschutz/telekommunikation/telefonie/aufzeichnung-von-telefongespraechen.html>

– Erläuterungen zu Stimmerkennungsverfahren (Stand: April 2017), abrufbar unter <www.edoeb.admin.ch/edoeb/de/home/datenschutz/technologien/biometrie/erlaeuterungen-zu-stimmerkennungsverfahren.html>

Entwurf zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017, S. 7193-7276).

Profiling nach der DSGVO und dem E-DSG bei Banken

David Vasella, Zürich*

* Rechtsanwalt, Dr. iur., CIPP/E, Partner bei Walder Wyss AG, Zürich.

I. Einleitende Bemerkungen

1. Worum geht es?

Der Ausdruck «Profiling» erinnert an «Racial Profiling», das Profiling von Serientätern im Fernsehen und die massenhafte Auswertung der Datenspuren unseres digitalen Lebens, also das Vordringen der Technologie in die tieferen Schichten der menschlichen Persönlichkeit und an datenbasierte Diskriminierungen. Ein Blick in die fast zwanzig Jahre alte Empfehlung des Europarats zum Profiling[1] zeigt die damaligen Befürchtungen: Durch Profiling ist es möglich, Personen unbemerkt und auf Basis grosser Datenmengen in Kategorien einzuordnen, was – je nach Anwendungsgebiet und Kontext – die Selbstbestimmung und sogar die Menschenwürde der Betroffenen gefährdet.

Gleichzeitig umfasst Profiling nach heutigen Definitionen auch harmlose Vorgänge und Vorgänge im Interesse der betroffenen Person, bspw. Datenanalysen zur Betrugsprävention. Dieser Gegensatz wird in der gesetzlichen Regelung sichtbar: Der Ausdruck «Profiling» wird in der Europäischen Datenschutz-Grundverordnung (DSGVO), aber auch im Entwurf des DSG (E-DSG) wiederholt bloss als dramaturgisches Mittel eingesetzt; eigenständiger Regelungsgegenstand ist das Profiling nur vereinzelt. Gleichzeitig beruht Art. 20 Abs. 2 lit. b E-DSG auf der Fiktion, Profiling sei prinzipiell hochriskant, weshalb jedes Profiling eine Datenschutz-Folgenabschätzung erfordert.

2. Profiling und Persönlichkeitsprofile: Revision des DSG

Das DSG wird derzeit bekanntlich revidiert, im Gefolge besonders der DSGVO und der Revision der Europaratskonvention 108. Schon der Vorentwurf des revidierten DSG vom 21. September 2016 (VE-DSG) sah dabei vor, den Begriff des Persönlichkeitsprofils fallenzulassen und stattdessen das Profiling zu regeln – ein naheliegender Vorschlag, zumal die Europäische Datenschutz-Grundverordnung nun wie erwähnt das «Profiling» regelt und der Begriff des Persönlichkeitsprofils ausländischen Datenschutzrechten soweit ersichtlich unbekannt ist.[2] Der VE-DSG stiess im Vernehmlassungsverfahren allerdings auf wenig Gegenliebe. Kritisiert wurden besonders die sogar über die Anforderungen der DSGVO hinausgehenden Eigenheiten, der sog. Swiss Finish,[3] aber auch zahlreiche weitere Punkte. Ein wesentlicher Kritikpunkt

1 Europarat, Empfehlung Profiling, S. 1 ff.

2 Botschaft rev. DSG, S. 6971.

3 Vgl. VASELLA/SIEVERS, digma 2017, S. 44 ff.

war die vorgeschlagene Regelung des Profiling. Der VE-DSG definierte das Profiling so weit, dass selbst jede Datenauswertung von Hand als Profiling in Betracht kam. Darüber hinaus galt nach dem Vorentwurf, dass jedes Profiling ohne ausdrückliche Einwilligung persönlichkeitsverletzend gewesen wäre. Selbst andere Rechtfertigungsgründe wären nicht in Frage gekommen (Art. 23 Abs. 2 lit. d VE-DSG). Faktisch wäre für viele Alltagsvorgänge ein Verbot mit sehr beschränkten Ausnahmen eingeführt worden.

Im derzeitigen Entwurf des DSG (E-DSG) schränkte der Bundesrat die Definition des Profiling ein und liess gleichzeitig das grundsätzliche Verbot fallen, was die vorgeschlagene Regelung erheblich entschärft hat. Derzeit ist davon auszugehen, dass der Nationalrat den Entwurf mit den von der SPK-N vorgeschlagenen Änderungen in der Herbstsession 2019 berät.[4] Man darf gespannt sein, was die weitere Beratung in den Räten ergibt.

II. Übersicht über die gesetzliche Regelung

Die DSGVO spricht häufig vom Profiling:

- Art. 4 Ziff. 4 (Legaldefinition);
- Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g (Informationspflicht);
- Art. 15 Abs. 1 lit. h (Auskunftspflicht);
- Art. 21 Abs. 1 und 2 (Widerspruchsrecht aufgrund einer besonderen Situation bzw. gegen Direktmarketing);
- Art. 22 Abs. 1 (automatisierte Einzelfallentscheidungen);
- Art. 35 Abs. 3 lit. a (Datenschutz-Folgenabschätzung);
- Art. 47 Abs. 2 lit. e (Binding Corporate Rules);
- Art. 70 Abs. 1 lit. f (Aufgaben des Europäischen Datenschutzausschusses); und
- in den Erwägungsgründen 60, 63, 71, 72 und 91.

Allerdings trügt diese Liste. Häufig wird das Profiling nur mitgenannt, um eine andere Aussage zu verstärken. Das trifft, zumindest nach hier vertretener Auffassung, zu auf die Informations- und Auskunftspflichten, das Widerspruchsrecht, die Beschränkung automatisierter Einzelfallentscheidungen und Datenschutz-Folgenabschätzungen. Eine eigenständige Bedeutung hat das Profiling nur in Art. 4 Nr. 4 (Legaldefinition), am Rande bei Art. 70 Abs. 1 lit. f DSGVO (Aufgaben des Ausschusses) und in den Erwägungsgründen 60

[4] Medienmitteilung der SPK-N vom 29. Mai 2019.

und 63 (eigenständige Informationspflicht bei Profiling) und 71 (Anforderungen an die Durchführung des Profiling).

Vergleichbares gilt nach dem Entwurf des DSG (E-DSG), doch ist der Regelungsgehalt hier weiter. Nur mitgenannt wird das Profiling in Art. 19 Abs. 1 (Informationspflicht). Eigenständige Bedeutung hat das Profiling dagegen in

- Art. 4 lit. f (Legaldefinition);
- Art. 5 Abs. 6 (Ausdrücklichkeit der Einwilligung);
- Art. 20 Abs. 2 lit. b (Pflicht zur Durchführung einer DSFA bei Profiling);
- Art. 27 Abs. 2 lit. c Ziff. 1 (keine Vermutung des überwiegenden Interesses an der Prüfung der Kreditwürdigkeit, wenn dabei ein Profiling erfolgt); und
- Art. 30 Abs. 2 lit. b (Erfordernis einer formellgesetzlichen Grundlage für das Profiling durch Bundesbehörden).

III. Zur Legaldefinition des Profiling

1. Art. 4 Nr. 4 DSGVO

a) Begriff und Beispiele

Die DSGVO definiert das Profiling in Art. 4 Nr. 4 als «jede Art der automatisierten Verarbeitung» von Personendaten, die darin besteht, dass diese Daten «verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten». Zu einer solchen Bewertung gehören insbesondere die «Analyse oder Vorhersage» von «Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche[n] Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel». Es geht also um

- eine Verarbeitung von Personendaten,[5]
- die automatisiert erfolgt, und zwar
- mit dem Ziel einer Bewertung persönlicher Aspekte.

Die Legaldefinition ist klärungsbedürftig. Zunächst fragt sich, wann eine Verarbeitung von Personendaten i.S.v. Art. 4 Nr. 1 und 2 DSGVO «automatisiert» erfolgt. Dieser Ausdruck findet sich in der DSGVO wiederholt, besonders in Art. 2 Abs. 1 zum sachlichen Anwendungsbereich, wird aber nicht definiert

[5] Die DSGVO verwendet den Begriff der «personenbezogenen Daten»; der Lesbarkeit zuliebe spricht dieser Beitrag dennoch von «Personendaten»; gleichzeitig aber von «Bearbeitung», wenn es um schweizerisches Datenschutzrecht, und von «Verarbeitung», wenn es um Europäisches Datenschutzrecht geht.

und auch in den Erwägungsgründen nicht geklärt. Aus Art. 4 Nr. 2 und Art. 20 Abs. 1 lit. b DSGVO ist aber zu schliessen, dass es um eine Verarbeitung «mit Hilfe automatisierter Verfahren» geht, und die Artikel-29-Datenschutzgruppe[6] stellt diese den Datensammlungen aus Papier gegenüber.[7] Eine Verarbeitung erfolgt demnach immer dann automatisiert, wenn die Daten in elektronischer Form verarbeitet werden.[8] Für das Profiling soll es dabei genügen, wenn die Verarbeitung nur teilweise automatisiert erfolgt.[9] Eine Verarbeitung kann also auch dann ein Profiling darstellen, wenn ein Teil der Verarbeitung von Hand bzw. analog erfolgt.

Im Ergebnis wird das Tatbestandselement der Automatisierung selten einschränkend wirken. Eine Einschränkung kann auch nicht sinnvoll über quantitative Elemente erfolgen. Es ist bspw. nicht notwendig, dass eine umfangreiche Datenbasis verwendet wird, sobald schon wenige Daten geeignet sind, eine Bewertung persönlicher Aspekte zu ermöglichen; ohnehin wäre es unmöglich, eine genaue Grenze festzulegen. Wenn also etwa aufgrund eines Wohnortwechsels in ein bestimmtes Quartier auf die Bonität einer Person geschlossen wird (vgl. S. 198), dürfte dieser Vorgang als Profiling gelten.[10] Ob die Verlässlichkeit der Bewertung gut oder schlecht ist, spielt für den Begriff des Profiling dabei keine Rolle; diese Frage ist bei den inhaltlichen Anforderungen an das Profiling zu prüfen.

Wichtiger, aber schwieriger zu beantworten ist die Frage, wann eine solche Verarbeitung das Ziel verfolgt, «persönliche Aspekte» zu «bewerten». Eine «Bewertung» verlangt jedenfalls eine inhaltliche Auseinandersetzung. Dies entspricht dem Wortsinn, wird aber auch durch die Beispiele der Analyse oder Prognose persönlicher Eigenschaften oder Verhaltensweisen in Art. 4 Nr. 4 DSGVO verdeutlicht. Erforderlich ist deshalb eine Auseinandersetzung mit der Datenbasis, die zu einer zusätzlichen Aussage führt, die man als «informatiellen Mehrwert» bezeichnen könnte. Es geht mit anderen Worten darum, das Erkenntnispotential von Datenbeständen zu erschliessen.[11]

---

6 Die Art.-29-Datenschutzgruppe ist der frühere Name des Ausschusses der Datenschutz-Aufsichtsbehörden der Mitgliedstaaten und des Europäischen Datenschutzbeauftragten. Mit dem Wirksamwerden der DSGVO wurde sie durch den «Europäischen Datenschutzausschuss» abgelöst (Art. 68 ff. DSGVO).

7 Art.-29-Gruppe, Leitlinien Datenportabilität, S. 7.

8 So auch ROSSNAGEL, Art. 2 DSGVO N 14.

9 Art.-29-Gruppe, Leitlinien Profiling, S. 7; so auch SCHOLZ, Art. 4 Nr. 4 DSGVO N 4.

10 Vgl. SCHOLZ, Art. 4 Nr. 4 DSGVO N 5.

11 So SCHOLZ, Art. 4 Nr. 4 DSGVO N 6.

Eine Bewertung fehlt also, wenn Personen lediglich nach feststehenden Kriterien klassifiziert werden. Wer seine Kunden lediglich in Alterskohorten einteilt, profiliert sie deshalb nicht.[12] Anders verhält es sich, wenn Kunden Affinitäten zugewiesen werden, d.h. ein statistisch bestimmtes Interesse an einer Produktkategorie: Eine solche Klassifizierung ist ein Profiling, denn hier wird ein Kunde dadurch bewertet, dass eine Verhaltensprognose erstellt wird.

Damit stellen etwa folgende Tätigkeiten ein Profiling i.S.d. DSGVO dar, soweit sie in den räumlichen Anwendungsbereich der DSGVO[13] fallen:

- Die Bestimmung der Bonität, also der Wahrscheinlichkeit eines Zahlungsausfalls;
- die Kreditfähigkeitsprüfung i.S.v. des KKG;[14]
- das Tracking des Aufenthaltsorts einer Person in einer App mit dem Ziel, ortsbasierte Aktionen anzuzeigen, z.B. in einer App zur Verwaltung von Kreditkarten;
- die Prüfung von Kreditkartentransaktionen auf auffällige Muster, die auf einen Betrugsversuch hindeuten können;
- das Screening von E-Mails zur Aufdeckung und Verhinderung von Insiderhandel oder anderen Verstössen;[15]
- die Personalisierung von Beratungsleistungen und von Angeboten auf individuelle Kunden;[16]
- im HR-Bereich die Vorauswahl von Bewerbungen,[17] Laufbahnprognosen, Potenzialanalysen,[18] Background-Prüfungen,[19] die Auswertung von Stimmprofilen.[20]

---

12 So auch Art.-29-Gruppe, Leitlinien Profiling, S. 7.

13 Dazu Art. 3 DSGVO und Art. 129 IPRG.

14 Art. 28 Abs. 2 und Art. 29 Abs. 2 KKG; vgl. auch Art. 30 Abs. 1 KKG betr. summarische Kreditfähigkeitsprüfung; vgl. auch OGer BE, ZK 16 148 vom 23. September 2016, E. 20.7.1 („prognostische Beurteilung").

15 Vgl. FINMA RS 2013/8, Rz. 53 f. (Massnahmen zur Überwachung der Mitarbeitergeschäfte); SBVg, Data Leakage Protection, S. 23.

16 Dies erwähnt bspw. die ZKB in ihrer Datenschutzerklärung, abrufbar unter <http://bit.ly/2KNyV2f>; vgl. dazu auch Art. 10 ff. FIDLEG (Inkrafttreten am 1. Januar 2020); WEBER/BAISCH, AJP 2016, S. 1071.

17 Dazu WILDHABER, AJP 2017, S. 214.

18 SCHOLZ, Art. 22 DSGVO N 24.

19 Vgl. dazu etwa SBVg, Data Leakage Protection, S. 46.

20 Dazu BETZ, *passim*.

b) Automatisierte Entscheidung im Einzelfall

Abzugrenzen ist das Profiling von der «automatisierten Entscheidung im Einzelfall» (im Folgenden «AEE»), die etwa Art. 13 Abs. 2 lit. f DSGVO in einem Atemzug nennt. Eine AEE ist nach Art. 22 Abs. 1 DSGVO

- eine «Entscheidung»,
- die der betroffenen Person gegenüber eine rechtliche Wirkung entfaltet
- oder sie «in ähnlicher Weise erheblich beeinträchtigt».

Eine AEE stellt keine Datenbearbeitung dar, sondern eine auf einer automatisiert bearbeiteten Datengrundlage beruhende Entscheidung. Die zugrundeliegende Bearbeitung kann ein Profiling sein, aber zwingend ist dies an sich nicht.[21] Ebenso lässt sich aus der Wendung «automatisierte[n] Entscheidungsfindung einschließlich Profiling» (Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h, Art. 22 Abs. 1 DSGVO) jeweils nicht schliessen, Profiling stelle stets eine AEE dar; hier geht es nur darum, die besondere Bedeutung des Profiling illustrativ hervorzuheben (darauf ist zurückzukommen). Allerdings wird eine AEE in den meisten Fällen ein Profiling umfassen. Das liegt am Begriff der «Entscheidung»: Eine Entscheidung setzt voraus, dass der Verantwortliche aus mehreren Möglichkeiten auswählt, also eine gewisse Wahlfreiheit hat. An einer Entscheidung fehlt es, wenn ein Verantwortlicher nur einer gegenseitig vereinbarten Logik folgt, bspw. eine Auszahlung am Geldautomaten verweigert, weil ein vertraglich definiertes Limit erreicht ist. Hier hat der Verantwortliche keine Wahl, weshalb er keine Entscheidung trifft.[22] Dasselbe gilt bei anderen Automatismen, bspw. der automatisierten Prüfung, ob das Kontoguthaben eine Überweisung erlaubt oder der Kreditkartensaldo den Karteneinsatz.[23] Darüber hinaus wäre der Betroffene einer Entscheidung in solchen Fällen nicht «unterworfen», wie es die DSGVO verlangt, weil er an ihr – durch den Vertragsschluss zu den entsprechenden Bedingungen – ja gerade mitgewirkt hat.[24] Infolgedessen wird eine Entscheidung in den meisten Fällen auf einer «Bewertung» des Betroffenen beruhen, also einer Form des

---

21 Art.-29-Gruppe, Leitlinien Profiling, S. 8.

22 Man mag einwenden, der Verantwortliche könne auch hier entscheiden, nämlich aus Kulanz; tut er dies nicht, fehlt es aber schon an einer rechtlichen oder vergleichbaren Wirkung auf den Betroffenen.

23 Vgl. SCHOLZ, Art. 22 DSGVO N 18; GOLA, Art. 22 DSGVO N 20 (der dasselbe Ergebnis mit einer teleologischen Reduktion begründet).

24 So auch SCHOLZ, Art. 22 DSGVO N 18; SCHULZ, Art. 22 DSGVO N 19; a.A. ARNING, S. 230.

Profiling. Im Ergebnis erscheint die AEE weitgehend als qualifizierte Form des Profiling.

Eine AEE liegt allerdings nur dann vor, wenn die Entscheidung ausschliesslich automatisiert erfolgt. Anders als beim Profiling führt echte menschliche Beteiligung an der Entscheidung aus dem Anwendungsbereich heraus, d.h. eine Beteiligung, die nicht nur formal ist.[25] Ein Beispiel ist eine inhaltliche Überprüfung der Maschinenentscheidung durch einen Menschen mit der Kompetenz und faktischen Möglichkeit, die Entscheidung umzustossen. Im Fall einer Kreditentscheidung setzt dies voraus, dass der zuständige Sachbearbeiter einen gewissen Entscheidungsspielraum hat, die Entscheidung also nicht ausschliesslich oder stark überwiegend durch einen Scorewert vorgegeben ist. Eine Ablehnung eines Kreditantrags ausschliesslich aufgrund eines zu schlechten Scorewerts («Cut-off-Score») kann daher eine AEE darstellen.[26]

Zudem ist eine Entscheidung nur erfasst, wenn sie zu einer Rechtsfolge führt, z.B. zur Beendigung einer Vertragsbeziehung, oder zu einer ähnlichen Beeinträchtigung. Eine «Beeinträchtigung» ist klarerweise negativ; positive Folgen sind daher nicht erfasst. Strittig ist aber, ob auch die Rechtsfolge negativ sein muss, um den Tatbestand zu erfüllen. Nach hier vertretener Auffassung trifft dies zu, so dass eine vollautomatisierte Gutheissung eines Kreditgesuchs keine AEE darstellt, denn hier rechtfertigen sich die besonderen Einschränkungen der AEE nicht.

2. Art. 4 lit. f E-DSG

a) Begriff

Die Revision des DSG bezweckt die Anpassung der Definition des «Profiling» an das europäische Recht.[27] Ganz geglückt ist das nicht. Unter Profiling versteht Art. 4 lit. f E-DSG «die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten […]». Der Botschaft zufolge genügt dabei nur ein doppelt automatisierter Vorgang:[28]

– Personendaten müssen automatisiert ausgewertet werden, und

[25] Art.-29-Gruppe, Leitlinien Profiling, S. 21.
[26] Näher SCHOLZ, Art. 22 N 25 ff.
[27] Botschaft E-DSG, 6978.
[28] Botschaft E-DSG, 7022.

– auf dieser Basis muss auch die Bewertung der Person automatisiert erfolgen.

Anders als nach der DSGVO lässt die Botschaft dabei nur einen vollständig automatisierten Vorgang genügen.[29] Dies lässt einige Fragen offen. Mit der «vollständigen Automatisierung» ist wohl nur gemeint, dass beide Stufen, sowohl die Auswertung der Daten als auch die Bewertung der Person, automatisiert sein müssen. Die Trennung dieser beiden Stufen ist zwar fragwürdig. Da die Botschaft diese Unterscheidung aber vornimmt, ist die Forderung nach voller Automatisierung wohl dahingehend zu deuten, dass beide Stufen automatisiert sein müssen. Das bedeutet aber nicht, dass beide Stufen für sich genommen keine relevante menschliche Tätigkeit ertragen. Ein Profiling wird deshalb auch dann vorliegen, wenn ein Mensch beteiligt ist, solange die Bewertung im Wesentlichen automatisiert erfolgt, etwa bei einem Kreditscoring, bei dem ein Mensch eingreift. Ein engeres Verständnis fände im Wortlaut des Gesetzes keine Stütze, und auch der Normzweck spricht gegen das enge Verständnis. Ferner beabsichtigt der Entwurf des DSG der Botschaft zufolge eine «inhaltliche» Anpassung an die europäische Terminologie.[30] Das ist zwar in sich widersprüchlich, deutet aber gleichwohl darauf hin, dass die Regelung der DSGVO übernommen werden sollte. Ohnehin wird die Praxis bei der DSGVO entlehnten Konzepten wie dem Profiling ohne viel Federlesens das Verständnis der DSGVO zugrunde legen, zumal die datenschutzrechtliche Diskussion noch für längere Zeit von der DSGVO geprägt bleiben dürfte.[31] Im Ergebnis ist also davon auszugehen, dass auch teilautomatisierte Bewertungen ein Profiling i.S.v. Art. 4 lit. f E-DSG darstellen können.

b) Automatisierte Einzelentscheidung (AEE)

Auch der E-DSG kennt die Figur der automatisierten Entscheidung im Einzelfall, die hier «automatisierte Einzelentscheidung» heisst (Art. 19 E-DSG). Hier lehnt sich der Wortlaut an Art. 22 Abs. 1 DSGVO an, und auch inhaltlich deckt sich der Begriff mit dem Verständnis der DSGVO.[32] Keine AEE liegt da-

---

29 Botschaft E-DSG, 7022.

30 Botschaft E-DSG, 7021.

31 Der EDÖB hat ebenfalls schon anklingen lassen, dass er eine freiwillige Anwendung der DSGVO in der Schweiz erwartet, vgl. dazu den Beitrag von VASELLA auf datenrecht.ch vom 20. Mai 2019, abrufbar unter <http://bit.ly/2KMmBiB>.

32 Nach Ansicht von ROSENTHAL stellt ein Profiling i.S.v. Art. 4 lit. f E-DSG immer auch eine AEE dar (ROSENTHAL, Jusletter 27. November 2017, Rz. 102). Nach hier vertretener

her bspw. dann vor, wenn ein Mensch auf Basis eines Scoring einen Kreditentscheid fällt. Im Übrigen soll der Bundesrat den Begriff laut Botschaft erforderlichenfalls konkretisieren.[33]

IV. Rechtmässigkeit des Profiling

1. Rechtmässigkeit nach der DSGVO

Als Form der Datenbearbeitung untersteht das Profiling den allgemeinen datenschutzrechtlichen Grundsätzen und Anforderungen (für die DSGVO vgl. Erwägungsgrund 72). Dazu gehört im Anwendungsbereich der DSGVO zunächst der Grundsatz der Rechtmässigkeit, d. h. das Erfordernis einer Verarbeitungsgrundlage (Art. 5 Abs. 1 lit. a und Art. 6 ff. DSGVO). In Frage kommen für das Profiling alle Rechtsgrundlagen in Art. 6 und 9 f. DSGVO.

Ohne hier auf Einzelheiten einzugehen, lässt sich festhalten, dass viele Profiling-Vorgänge für den Abschluss oder die Durchführung eines Vertrags erforderlich sind (Art. 6 Abs. 1 lit. b DSGVO), etwa bei Verträgen, die grundsätzlich ein kreditorisches Risiko beinhalten. Solche Verträge «rechtfertigen die Durchführung eines Profilings sowohl im vorvertraglichen Stadium als auch während ihrer Durchführung»,[34] soweit das Profiling zur Beurteilung des Kreditrisikos geeignet ist; dies gilt sowohl für die Beschaffung eines externen Scorings als auch die eigene Durchführung eines entsprechenden Profiling. Aber auch bei anderen Verträgen kann Profiling erforderlich sein, z.B. für die Prüfung von Betrugsrisiken bei Kreditkartentransaktionen[35] oder im HR-Bereich.[36] Demgegenüber werden Aufsichtsbehörden Profiling zu Werbezwecken kaum als vertragsnotwendig gelten lassen, und zwar auch dann nicht, wenn das Profiling in den AGB des Anbieters erwähnt wird.[37]

Die Skepsis der Aufsichtsbehörden gegenüber dem Profiling zu Werbezwecken ist generell hoch. Hier sollte zwar an sich das berechtigte Interesse i.S.v. Art. 6 Abs. 1 lit. f DSGVO weit tragen, berücksichtigt man die Tatsache,

---

Auffassung ist das nicht zutreffend; die Wendung «automatisierten Bearbeitung, einschliesslich Profiling» lässt diesen Schluss nicht zu; «Profiling» wird hier vielmehr, wie bei den analogen Bestimmungen der DSGVO, lediglich illustrativ verwendet.

33 Botschaft E-DSG, S. 7056.

34 45. Tätigkeitsbericht Hessen, Ziff. 4.2.1.3; so auch BUCHNER/PETRI, Art. 6 DSGVO N 47 f.

35 Zu eng Art.-29-Gruppe, Arbeitspapier Rechtsgrundlage Vertrag, S. 9, wonach Profiling für Zwecke der Betrugsbekämpfung kaum notwendig sein soll.

36 Hier ist gestützt auf die Öffnungsklausel in Art. 88 DSGVO auch das Recht der Mitgliedstaaten zu beachten, z.B. § 26 des deutschen BDSG.

37 Vgl. Art.-29-Gruppe, Arbeitspapier Rechtsgrundlage Vertrag, S. 9 und 13.

dass der Schutz der betroffenen Person durch das Widerspruchsrecht von Art. 21 Abs. 1 und 2 DSGVO gewährleistet wird; zumindest dann, wenn der Verantwortliche diesen Schutz durch geeignete Garantien flankiert.[38] Die Entwicklung in Deutschland geht aber in eine andere Richtung. Zuletzt hat die Datenschutzkonferenz in ihrer Orientierungshilfe zwar nicht ausgeschlossen, dass sich ein personenbezogenes Tracking im Internet – das unter den Begriff des Profiling fallen kann – auf ein berechtigtes Interesse stützt, dass dies aber eine aufwendige, einzelfallbezogene Interessenabwägung verlangt.[39]

Ebenfalls in Frage kommt ein Profiling im Rahmen gesetzlicher Pflichten, z.B. zur Bekämpfung der Geldwäscherei. Hier verweist die Art.-29-Datenschutzgruppe auf die Rechtsgrundlage der Rechtspflicht, nicht der Vertragsnotwendigkeit.[40] Das ist solange überzeugend, als sich die Rechtspflicht aus EU-Recht bzw. dem Recht der Mitgliedstaaten ergibt (Art. 6 Abs. 3 DSGVO). Führt eine schweizerische Bank demgegenüber mit Bezug auf einen Kunden im EWR-Gebiet, aber gestützt auf schweizerisches Recht Profiling durch,[41] stellt sich spätestens dann die Frage der Rechtsgrundlage, wenn der betreffende Kunde gegenüber der Bank nach Art. 139 IPRG die DSGVO anruft. Hier kann die Bank wahlweise auf Art. 6 Abs. 1 lit. b und/oder lit. f DSGVO verweisen, denn das Profiling ist objektiv vertragsnotwendig und entspricht gleichzeitig dem berechtigten Interesse der Bank, schweizerisches Recht einzuhalten. Dass mehrere Rechtsgrundlagen nebeneinander anwendbar sein können, ergibt sich sodann aus dem Wortlaut von Art. 6 Abs. 1 DSGVO («rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist»).[42]

Kommt eine AEE hinzu, stellt sich die Frage der Rechtmässigkeit besonders. Art. 22 DSGVO erlaubt AEE nur eingeschränkt,[43] nämlich nur dann, wenn eine AEE für einen Vertrag zwischen der betroffenen Person und dem

---

38 «Geeignete Garantien» sind sämtliche Massnahmen zum Schutz der Betroffenen, bspw. erhöhte Transparenz, interne technische und organisatorische Massnahmen, besonders leicht auszuübende oder weitreichende Widerspruchsrechte, die freiwillige Durchführung einer Datenschutz-Folgenabschätzung usw. Alle diese Faktoren sind bei der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO zu berücksichtigen.

39 DSK, Orientierungshilfe, S. 11 ff.

40 Art.-29-Gruppe, Arbeitspapier Rechtsgrundlage Vertrag, S. 12.

41 Vgl. bspw. Art. 13 GwV-FINMA.

42 So auch BUCHNER/PETRI, Art. 6 DSGVO N 22.

43 Man kann sich fragen, ob Art. 22 DSGVO ein Verbot vorsieht oder der betroffenen Person lediglich einen Abwehranspruch verleiht. Es dürfte aber wohl von einem Verbot auszugehen sein. Das ist jedenfalls das Verständnis der Art.-29-Datenschutzgruppe.

Verantwortlichen erforderlich (Art. 22 Abs. 1 lit. a DSGVO)[44] oder gesetzlich erlaubt ist, wobei wiederum nur europäisches Recht beachtlich ist (lit. b), oder mit ausdrücklicher Einwilligung der betroffenen Person (lit. c).

2. Rechtmässigkeit nach dem E-DSG

Das schweizerische Datenschutzrecht beruht bekanntlich, anders als das Europäische Datenschutzrecht, auf dem Grundsatz der Erlaubnis mit Verbotsbehalt. Die Bearbeitung von Personendaten ist grundsätzlich zulässig. Die Frage lautet hier daher nicht, auf welche Rechtsgrundlage sich eine Bearbeitung stützt, sondern ob im konkreten Fall Rechtfertigungsbedarf besteht (Art. 26 E-DSG) und, falls ja, ob ein Rechtfertigungsgrund vorliegt (Art. 27 E-DSG). Dies gilt für alle Bearbeitungen durch Private, auch die Bearbeitung besonders schützenswerter Personendaten und Profiling.[45]

In Frage kommen alle Rechtfertigungsgründe (Art. 27 Abs. 1 E-DSG), wobei die Einwilligung ggf. – sofern sie aufgrund des E-DSG konkret erforderlich ist – ausdrücklich erfolgen muss (Art. 5 Abs. 6 E-DSG). Was «ausdrücklich» heisst, ist dabei weiterhin unklar.[46]

Fragen ergeben sich auch im Zusammenhang mit den Regelbeispielen eines überwiegenden privaten Interesses in Art. 27 Abs. 2 E-DSG. Ein Kunstfehler ist dem Bundesrat bei der Formulierung von Art. 27 Abs. 2 lit. c E-DSG unterlaufen, der Bearbeitung von Personendaten für die Prüfung der Kreditwürdigkeit. Das Interesse an dieser Datenbearbeitung soll nach Art. 27 Abs. 2 lit. c Ziff. 1 E-DSG dann nicht überwiegen, wenn ein Profiling stattfindet. Aber selbstverständlich kann das Interesse des Verantwortlichen und/oder eines Dritten an Profiling die gegenläufigen Interessen des Betroffenen überwiegen, und vor allem lässt der Vorschlag des Bundesrats ausser Acht, dass die Prüfung der Kreditwürdigkeit geradezu ein Schulbeispiel für Profiling ist. Eine Berufung auf ein überwiegendes Interesse hier nicht zuzulassen, ist widersprüchlich; dann könnte Art. 27 Abs. 2 lit. c insgesamt gestrichen werden.

---

44 Dieser praktisch bedeutsame Rechtfertigungsgrund ist hier allerdings enger als bei Art. 6 Abs. 1 lit. b DSGVO. Dort genügt es, dass eine Verarbeitung für einen Vertrag erforderlich ist, dessen Partei der Betroffene ist; dass dieser Vertrag mit dem Verantwortlichen besteht, ist anders als bei Art. 22 Abs. 1 lit. b DSGVO nicht vorausgesetzt.

45 Anders im öffentlichen Bereich; hier gilt das Erfordernis einer gesetzlichen Grundlage (Art. 30 E-DSG). Der E-DSG sieht daher bspw. vor, Art. 23 FINMAG dahingehend zu ändern, dass die FINMA zum Profiling befugt ist.

46 Vgl. ROSENTHAL, Jusletter 27. November 2017, Rz. 39; VASELLA, Jusletter 16. November 2015, Rz. 22 ff.

Zwar ist die Aufzählung in Abs. 2 nicht abschliessend, so dass Profiling zur Prüfung der Kreditwürdigkeit auch ohne Anpassung des Gesetzestextes durch überwiegende Interessen gerechtfertigt werden kann. Es ist dennoch zu hoffen, dass das Parlament diesen Fehler korrigiert und das Profiling bei Art. 27 Abs. 2 lit. c E-DSG streicht (und bei dieser Gelegenheit auch die nicht sachgerechte Beschränkung auf fünf Jahre in lit. c Ziff. 3 streicht oder anpasst).

V. Informations- und Auskunftspflichten im Zusammenhang mit Profiling

1. Informations- und Auskunftspflicht bei blossem Profiling?

Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. h DSGVO verlangen, dass die betroffene Person über «das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling» zu informieren ist; und entsprechendes sieht Art. 15 Abs. 1 lit. h DSGVO für das Auskunftsrecht vor. Aus diesem Wortlaut geht hervor, dass sich die Informations- und Auskunftspflichten nur auf Profiling beziehen, das Teil einer AEE ist («einschliesslich» Profiling). Blosses Profiling, das keine AEE ist, löst keine solchen Pflichten aus. Diesem Schluss ist zunächst allerdings entgegenzuhalten, dass

– die Erwähnung des Profiling nicht notwendig wäre, wenn sich keine Rechtsfolgen daran knüpfen, und dass
– es keinen Grund gäbe, AEE in Art. 13 und 14 zu erwähnen, wenn es an diesen Stellen nur um die Information über AEE – und nicht auch für Profiling – ginge; denn für AEE ergibt sich eine Informationspflicht schon aus Art. 22 Abs. 3 DSGVO.

Grosses Gewicht haben diese Argumente allerdings nicht, zumal die DSGVO diverse Unschärfen aufweist und die Erwähnung des Profiling auch als blosses Stilmittel verstanden werden kann. Im Gegenteil drängt sich der Schluss auf, dass Art. 13-15 das Profiling ohne AEE nicht erfassen. Diese Bestimmungen verweisen ausdrücklich auf AEE «gemäss Artikel 22 Absätze 1 und 4». Art. 22 Abs. 1 DSGVO greift dann zwar die Formulierung in Art. 13, 14 und 15 DSGVO auf («einschließlich Profiling»), regelt aber klarerweise nicht das Profiling als solches. Denn wäre Profiling ohne AEE hier erfasst, hätte dies zur Folge, dass das Profiling der eingeschränkten Zulässigkeit nach Art. 22 DSGVO unterläge. Es wäre wie AEE nur zulässig, wenn es für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem

Verantwortlichen (Abs. 2 lit. a) oder aufgrund rechtlicher Vorschriften erforderlich ist (Abs. 2 lit. b) oder mit ausdrücklicher Einwilligung der betroffenen Person (Abs. 2 lit. c). Eine Rechtfertigung durch berechtigtes Interesse oder eine nicht ausdrückliche Einwilligung entfiele. Eine so weitreichende Folge müsste sich im Gesetzestext aber eindeutig wiederfinden.[47] Wenn die zitierte Formulierung bei Art. 22 Abs. 1 DSGVO das Profiling nun aber nur in symbolhafter Weise und nicht als eigenständigen Regelungsgegenstand erwähnt, kann für die entsprechende Formulierung in Art. 13 ff. nichts anderes gelten. Schon deshalb ist eine auf Art. 13 oder 14 DSGVO gestützte Informationspflicht und eine Auskunftspflicht nach Art. 15 DSGVO abzulehnen. In der Literatur ist dieser Schluss freilich umstritten.[48]

Art. 5 Abs. 1 lit. a DSGVO gibt allerdings parallel zu Art. 13 und 14 DSGVO vor, dass die Verarbeitung von Personendaten transparent erfolgen muss. Es handelt sich um eine programmatische Generalklausel, die sich aber – anders als die Vorgängernorm in der Datenschutz-Richtlinie – nicht an die Mitgliedstaaten, sondern an den Verantwortlichen[49] richtet und direkt anwendbar ist; und ihre Verletzung ist mit Busse bedroht (Art. 83 Abs. 5 lit. a DSGVO).[50] Es ist nicht auszuschliessen, dass sich daraus eine über Art. 13 f. hinausgehende Informationspflicht über Profiling ableiten lässt. So verlangt auch Erwägungsgrund 60, dass die betroffene Person darauf hingewiesen wird, dass ein Profiling stattfindet und welche Folgen dies hat.[51] Erwägungsgründe sind aber nicht Teil des «verfügenden», d.h. verbindlichen Teils der DSGVO; sie dienen nur zu dessen Begründung und dürfen «keine Bestimmungen mit normativem Gehalt» enthalten.[52] Eine Informationspflicht über

---

47 Vgl. auch SCHOLZ, Art. 22 DSGVO N 5: Art. 22 DSGVO schränkt die Zulässigkeit des Profiling nicht ein.

48 Wie hier PAAL/HENNEMANN, Art. 13 DSGVO N 26; KAMLAH, Art. 13 N 27; ARNING, S. 152; wohl auch VEIL, Art. 13 und 14 DSGVO N 114; a.A. (Informationspflicht auch bei blossem Profiling) FRANCK, Art. 13 DSGVO N 27; BÄCKER, Art. 13 DSGVO N 54; MESTER, Art. 13 DSGVO N 27.

49 Inwieweit sich aus Art. 5 DSGVO auch für den Auftragsverarbeiter Pflichten ergeben, ist nicht geklärt.

50 Rechtsstaatlich ist eine so unbestimmte Strafbestimmung falsch. Der Entwurf des DSG tut aber dasselbe, indem die Informationspflicht nach Art. 17 Abs. 2 E-DSG ebenfalls mit einer Generalklausel operiert, deren Verletzung nach Art. 54 Abs. 1 lit. a E-DSG aber mit Busse bedroht ist.

51 Das Wort «sollte» («should») in Erwägungsgrund 60 erlaubt dabei nicht den Schluss, es gehe lediglich um eine Empfehlung; das ist eine in Erwägungsgründen auch anderswo häufig verwendete Formulierung.

52 Leitfaden Rechtstexte, Ziff. 10.

Profilingmassnahmen kann sich daher nicht allein auf Erwägungsgrund 60 stützen. Erwägungsgrund 60 kann aber natürlich bei der Auslegung von Art. 5 Abs. 1 lit. a DSGVO berücksichtigt werden. Eine Informationspflicht für blosses Profiling sieht denn auch die Art.-29-Datenschutzgruppe. Der Leitfaden zum Profiling lässt sich zwar so lesen, dass es nur «good practice» ist, über Profiling zu informieren, solange keine AEE vorliegt. Dem steht aber gegenüber, dass derselbe Leitfaden an gleicher Stelle auf Erwägungsgrund 60 verweist;[53] und der Leitfaden zur Transparenz geht recht deutlich von einer Informationspflicht zu Profiling aus.[54]

Die Gerichte werden klären müssen, ob, wann und in welcher Form blosses Profiling separat informationspflichtig ist. Nach hier vertretener Auffassung verlangt die Generalklausel von Art. 5 Abs. 1 lit. DSGVO jedenfalls eine Abwägung im Einzelfall. Der Verantwortliche hat dabei Ermessensspielraum.

In der Praxis informieren Banken vielfach freiwillig über Profilingmassnahmen, so etwa die UBS,[55] die Credit Suisse[56] und die ZKB[57] und im Ausland bspw. die Deutsche Bank,[58] während z.B. die Julius Bär soweit ersichtlich darauf verzichtet. Die Informationen sind dabei jeweils knapp gehalten, was zumindest dem Anliegen der Verständlichkeit (Art. 12 Abs. 1 DSGVO) entspricht.

Im Rahmen des E-DSG besteht ebenfalls eine Informationspflicht für AEE. Art. 19 Abs. 1 E-DSG verwendet die gleiche Wendung wie die DSGVO: Die Informationspflicht bezieht sich auf AEE «einschliesslich Profiling». Insofern stellen sich ähnliche Auslegungsfragen wie soeben bei der DSGVO. Auch das Ergebnis ist dasselbe: Eine Informationspflicht entsteht nicht durch blosses Profiling. Auch die Botschaft hält dies ausdrücklich fest.[59]

---

53 Art.-29-Gruppe, Leitlinien Profiling, S. 25.

54 Art.-29-Gruppe, Leitlinien Transparenz, S. 22.

55 Data Privacy Notice, abrufbar unter <http://bit.ly/2IUoBmz>.

56 Informationspflichten im Rahmen der Erhebung von personenbezogenen Daten bei der betroffenen Person nach Artikel 13 Absätze 1, 2 und 4 sowie Artikel 21 Absatz 3 der EU-Datenschutz-Grundverordnung (DSGVO), abrufbar unter <http://bit.ly/2wUio4i>.

57 Datenschutzerklärung, abrufbar unter <http://bit.ly/2RlrmRC>.

58 Data protection information under the Swiss Federal Act on Data Protection and EU General Data Protection Regulation, abrufbar unter <http://bit.ly/2wRZkDF>.

59 Botschaft E-DSG, S. 7057.

2. Information und Auskunft bei AEE

Kommt zum Profiling eine AEE hinzu, greifen dagegen die Informationspflichten nach Art. 13 und 14 und die Auskunftspflicht nach Art. 15 DSGVO. Darüber hinaus gelten die besonderen Anforderungen bzw. Betroffenenrechte nach Art. 22 Abs. 3 DSGVO, sofern die AEE nicht auf gesetzlicher Grundlage beruht (sondern durch Vertragsnotwendigkeit oder ausdrückliche Einwilligung gerechtfertigt ist), und die eingeschränkte Zulässigkeit nach Art. 22 Abs. 1 und 2 DSGVO, die angesprochen wurde, hier aber nicht vertieft wird.

Die Informationspflicht in Art. 13, 14 und 15 DSGVO betrifft jeweils folgende Punkte:

- dass eine AEE stattfinden soll;
- ihre «Logik» und
- ihre Tragweite und die angestrebten Auswirkungen auf die Betroffenen.

Die involvierte Logik meint die Kriterien, die das Ergebnis der AEE beeinflussen, und die Art und Weise, wie sie auf die AEE einwirken. Dies verlangt weder eine detaillierte Erklärung technischer Abläufe noch eine Offenlegung der Entscheidformel, die ein Geschäftsgeheimnis darstellt,[60] aber eine verständliche Erläuterung des zugrundeliegenden Prinzips,[61] so dass der Betroffene in der Lage ist, die AEE nachzuvollziehen. Die Mitgliedstaaten können gestützt auf Art. 23 DSGVO Einschränkungen der Informations- und Auskunftspflicht vorsehen.

Art. 19 Abs. 1 E-DSG verlangt ebenfalls, dass die betroffene Person über die AEE informiert wird. Aus Art. 19 Absatz 2 E-DSG ergibt sich ferner das Recht der betroffenen Person, ihren Standpunkt darzulegen. Dies setzt voraus, dass die betroffene Person über diejenigen Informationen verfügt, die erforderlich sind, um die AEE in ihren Grundzügen zu verstehen. Offen bleibt, ob es am Verantwortlichen liegt, der betroffenen Person diese Informationen von sich aus zur Verfügung zu stellen, oder ob es genügt, erst auf Nachfrage zu informieren. Die Botschaft geht von letzterem aus. Es genügt, wenn die betroffene Person Gelegenheit hat, «ihre Ansicht zum Ergebnis der

---

60 Vgl. Erwägungsgrund 63 *(«Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen»)*; SCHOLZ, Art. 22 DSGVO N 17; vgl. auch das Urteil des deutschen Bundesgerichtshofs (BGH) vom 28. Januar 2014 i.S. Schufa, VI ZR 156/13.

61 So, Art. 13 DSGVO N 19.

Entscheidung zu äussern» und gegebenenfalls «nachzufragen, wie die Entscheidung zustande gekommen ist».[62] Aus Praktikabilitätsüberlegungen ist diese Sicht zu begrüssen, zumal der Schutz der betroffenen Person auch so sichergestellt sein dürfte. Demnach hat der Verantwortliche von sich aus nur über das Vorliegen der AEE und ihr Ergebnis zu informieren, z.B. in einem Schreiben, in der über die Ablehnung eines Online-Kreditantrags informiert wird. Aus Art. 19 E-DSG folgt weiter nur, dass die betroffene Person das Recht hat, weitere Informationen zu verlangen, sodass sie ihren Standpunkt darlegen kann (abgesehen vom Recht, eine Entscheidung durch eine natürliche Person zu verlangen; ebenfalls Art. 19 Abs. 2 E-DSG).

Anzumerken bleibt, dass weder eine Informationspflicht noch ein Anspruch auf Darlegung des Standpunkts und Überprüfung besteht, wenn eine Offerte automatisch angenommen wird (Art. 19 Abs. 3 lit. a E-DSG; wenn ein Online-Kreditantrag angenommen wird, um im Beispiel zu bleiben, muss die Bank dem Kreditnehmer also nicht mitteilen, dass die Überprüfung ihres Antrags automatisiert erfolgt ist) oder wenn die betroffene Person ausdrücklich eingewilligt hat, dass eine Einwilligung automatisiert erfolgen kann (lit. b).

VI. Zu den Anforderungen an die Durchführung des Profiling

1. Vermeidung von Diskriminierungen

Die DSGVO enthält im verfügenden Teil keine spezifischen Vorgaben an die Durchführung des Profiling. Es gelten wie erwähnt die allgemeinen Grundsätze, besonders der Grundsatz der Zweckbindung[63] und die Grundsätze des Datenschutzes durch Technikgestaltung (Privacy by design) und durch datenschutzfreundliche Voreinstellungen (Privacy by default; Art. 25 DSGVO und Art. 6 E-DSG). Erwägungsgrund 71 gibt aber vor, dass für das Profiling «geeignete mathematische oder statistische Verfahren» angewandt werden sollen und dass Fehlerquellen und Risiken unrichtiger Daten zu minimieren und Diskriminierungen zu verhindern sind. Diese Anforderungen ergeben

62 Botschaft E-DSG, S. 7058.

63 Hierzu nur soviel: Ein Profiling ist genauso wie eine AEE kein Verarbeitungszweck, sondern ein Mittel der Verarbeitung. Der Einsatz von Profilingmassnahmen und AEE stellt daher nur dann eine Zweckänderung dar, wenn das damit angestrebte Ziel nicht mehr mit den ursprünglichen Zwecken der dabei verarbeiteten Daten vereinbar ist.

sich im Anwendungsbereich der DSGVO bereits aus allgemeinen Grundsätzen (Art. 5 DSGVO) und im HR-Bereich aus arbeitsrechtlichen Vorschriften;[64] Erwägungsgrund 71 zeigt aber, dass Diskriminierungsrisiken im Zusammenhang mit Profiling als besonders gewichtig eingestuft werden. Deshalb hat der deutsche Gesetzgeber in § 31 des deutschen Bundesdatenschutzgesetzes weitere Beschränkungen vorgesehen. Dem Schutz vor Diskriminierung dient etwa § 31 Abs. 1 Ziff. 3 BDSG, wonach ein Scoring nicht nur auf Adressdaten beruhen darf. Eine Bank darf demnach die Kreditwürdigkeit nicht allein auf der Basis von Adressdaten beurteilen. Damit soll verhindert werden, dass bestimmte Gebiete durch Geoscoring pauschal schlechtergestellt werden («redlining»).

Die Bank ist nach der DSGVO infolgedessen verpflichtet, die «Logik» des Profiling (vgl. Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. g und Art. 15 Abs. 1 lit. h DSGVO) so auszugestalten, dass das Verfahren geeignet ist, die angestrebten Aussagen ausreichend abzustützen, sachgerechte Kriterien zu verwenden, Unschärfen und Fehler angemessen zu minimieren und (direkte und indirekte) Diskriminierungen zu verhindern. Auf den Einbezog besonders schützenswerter Personendaten ist nach Möglichkeit zu verzichten.[65] Die entsprechenden Überlegungen sollten mit Blick auf die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DSGVO) dokumentiert werden, ggf. im Rahmen des Verarbeitungsverzeichnisses (Art. 30 Abs. 1 DSGVO; Art. 11 E-DSG).

Für das E-DSG lassen sich diese Grundsätze nicht unbesehen übernehmen. Die Bedeutung des Diskriminierungsrisikos ist eine andere, denn die Schweiz kennt i.d.R. keine direkte Horizontalwirkung von Grundrechten.[66] Allerdings muss das Profiling selbstverständlich die Bearbeitungsgrundsätze

64 Dazu WILDHABER, AJP 2017, S. 214 ff.

65 Dieser Verzicht erlaubt es dem Verantwortlichen, sich ggf. auf ein berechtigtes Interesse i.S.v. Art. 6 Abs. 1 lit. f DSGVO zu berufen und eine ausdrückliche Einwilligung (Art. 9 Abs. 2 lit. a DSGVO) zu vermeiden. Wenn der Verantwortliche nämlich abstrakt gesehen besonders schützenswerte Personendaten bearbeitet (z.B. Angaben über Spenden an eine religiöse Vereinigung oder Ausgaben bei spezialisierten Ärzten oder in Etablissements, deren Besuch dem Intimbereich zuzurechnen ist), die besondere Aussagekraft dieser Daten in das Profiling aber nicht einbezieht (also bspw. Affinitäten bestimmt, aber keine Kategorien wie «gesundheitlich beeinträchtigt» oder «Sin Hobby» bildet), kann er vertreten, dass er für das Profiling keine besonders schützenswerten Personendaten bearbeitet und keine ausdrückliche Einwilligung erforderlich ist.

66 Vgl. SCHWEIZER, Art. 35 BV N 58 ff.

einhalten, z.B. den Grundsatz der Verhältnismässigkeit; und in diesem Rahmen können Anliegen von Erwägungsgrund 71 der DSGVO berücksichtigt werden.

2. Risikobeurteilung

Sowohl die DSGVO als auch das DSG verfolgen einen risikoorientierten (oder «risikobasierten») Ansatz. Die Pflichten des Verantwortlichen richten sich mit anderen Worten bis zu einem gewissen Grad – soweit das anwendbare Recht Pflichten nicht vollständig determiniert – nach dem Risiko, das sich aus einer Datenbearbeitung für die Betroffenen ergibt.[67] Dies verlangt generell eine Risikobeurteilung, wie sich etwa in Art. 32 Abs. 1 DSGVO oder Art. 7 Abs. 1 E-DSG zeigt.

In bestimmten Fällen schreibt das Gesetz aber eine besondere, strukturierte und dokumentierte Risikobeurteilung in Form einer Datenschutz-Folgenabschätzung vor («DSFA»; Art. 35 f. DSGVO; Art. 20 E-DSG). Das trifft dann zu, wenn eine Bearbeitung voraussichtlich ein «hohes Risiko» mit sich bringt (Art. 35 Abs. 1 DSGVO; Art. 20 Abs. 1 E-DSG). Es fragt sich daher jeweils, wann mit einem hohen Risiko zu rechnen ist; eine Risikoentscheidung, die dem Verantwortlichen überlassen ist. Die DSGVO und der E-DSG geben aber Hinweise in Form von Regelbeispielen (Art. 35 Abs. 3 DSGVO; Art. 20 Abs. 2 E-DSG). Dabei fällt auf, dass nach Art. 20 Abs. 2 lit. b E-DSG jedes Profiling als Hochrisikofall gilt. Die Botschaft begründet dies nicht. Dass Profiling als höchst suspekt empfunden wird, war aber schon im Vorentwurf überdeutlich, der Profiling generell nur mit ausdrücklicher Einwilligung zulassen wollte (Art. 23 Abs. 2 lit. d des Vorentwurfs). Für den Bundesrat ist eine Risikobeurteilung in Form einer DSFA – ggf. mit Einbezug des EDÖB nach Art. 20 21 E-DSG – offenbar der Preis dafür, das Profiling nicht zu verbieten. Abwegig ist das nicht, aber viel zu pauschal. Die These, Profiling sei stets hochriskant, ist falsch. In vielen Fällen ist Profiling harmlos und liegt noch dazu im Interesse der betroffenen Person;[68] und wenn Profiling im Einzelfall tatsächlich hochriskant sein sollte, ist eine DSFA über Art. 20 Abs. 1 E-DSG ohnehin verpflichtend.

---

67 Dazu Erwägungsgründe 74 ff.

68 Etwa durch Personalisierung von Angeboten oder durch Betrugsprävention, z.B. beim Schutz vor dem Missbrauch von Kreditkartendaten; vgl. HLADJK, Art. 22 DSGVO N 4; im HR-Prozess durch Zeitersparnis oder gerade dadurch, dass ein Bewerber lieber von einer Maschine automatisiert als von einem vorurteilsbehafteten Menschen beurteilt

Dies bestätigt ein Blick in die Leitlinien der Art.-29-Datenschutzgruppe. Im Sinne einer Faustregel ist eine DSFA dann durchzuführen, wenn bei einer Verarbeitung mindestens zwei Risikofaktoren zusammentreffen; wobei «evaluation or scoring, including profiling and predicting» (in der deutschen Sprachfassung der Leitlinien: «Bewerten oder Einstufen») einen Risikofaktor darstellt[69]. Für sich genommen führt ein Profiling demnach nicht generell zur Pflicht, eine DSFA durchzuführen, sondern nur dann, wenn einer der folgenden Risikofaktoren dazukommt:

- es wird eine AEE durchgeführt;
- es findet eine systematische Überwachung statt;
- es werden besonders schützenswerte Personendaten oder sonst besonders heikle Personendaten verarbeitet, bspw. Kontoangaben, die betrugsanfällig sind;
- Personendaten werden in grossem Umfang verarbeitet;
- Datensätze werden abgeglichen oder zusammengeführt;
- es werden Personendaten schutzbedürftiger Personen verarbeitet;
- es werden neue Technologien verwendet, oder bekannte Technologien in neuartiger Weise;
- betroffenen Personen kann ein Recht, eine Dienstleistung oder ein Vertrag verweigert werden.

Aufschlussreich ist in diesem Zusammenhang ein Blick auf die schwarzen und weissen Listen der Aufsichtsbehörden, die nach Art. 35 Abs. 4 und 5 DSGVO zu erstellen sind. Die deutsche Datenschutzkonferenz etwa verlangt eine DSFA u.a. in den folgenden Fällen:[70]

- Betrieb eines Fraud-Prevention-Systems;
- Scoring durch Wirtschaftsauskunfteien, Banken oder Versicherungen;
- Einsatz eines Data-Loss-Prevention-Systems, das systematische Profile der Mitarbeiter erzeugt;
- Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden.

---

wird; dazu BETZ, S. 149; generell durch ggf. an den Kunden weitergegebene Kosteneinsparungen und Effizienzgewinne, z.B. bei niedrigeren Gebühren in algorithmengestützter Anlageberatung, und durch Qualitätssicherung; vgl. WEBER/BAISCH, AJP 2016, S. 1069 f.

69 Art.-29-Gruppe, Leitlinien DSFA, S. 9.

70 DSK, DSFA-Liste.

Diese Liste zeigt, dass für Profiling auch nach der Art.-29-Datenschutzgruppe häufig eine DSFA durchzuführen ist. Der Schutz der Betroffenen verlangt dagegen nicht, bei Profiling immer eine DSFA durchzuführen.

Literaturverzeichnis

Stand sämtlicher Internet-Referenzen in diesem Beitrag ist der 14. Juni 2019.

ARNING MARIAN, in: Flemming Moos/Jens Schefzig/Marian Arning (Hrsg.), Die neue Datenschutz-Grundverordnung, Berlin 2018.

BÄCKER MATTHIAS, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), DS-GVO/BDSG, 2. Aufl. München 2018.

BETZ CHRISTOPH, Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern, ZD 2019, S. 148-152.

BUCHNER BENEDIKT/PETRI THOMAS, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), DS-GVO/BDSG, 2. Aufl. München 2018.

EHMANN EUGEN, in: Eugen Ehmann/Martin Selmayr (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. München 2018.

FRANCK LORENZ, in: Boris P. Paal/Daniel A. Pauly (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Aufl. München 2018.

GOLA PETER, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. München 2018.

HLADJK JÖRG, in: Eugen Ehmann/Martin Selmayr (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. München 2018.

KAMLAH WULF, in: Kai-Uwe Plath (Hrsg.), DSGVO/BDSG, 3. Aufl. Köln 2018.

MESTER ALEXANDRA, in: Jürgen Taeger/Detlev Gabel (Hrsg.), DSGVO – BDSG, 3. Aufl. Frankfurt a.M. 2019.

PAAL BORIS P./HENNEMANN, in: Boris P. Paal/Daniel A. Pauly (Hrsg.), Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 2. Aufl. München 2018.

ROSENTHAL DAVID, Der Entwurf für ein neues Datenschutzgesetz, Jusletter 27. November 2017.

ROSSNAGEL ALEXANDER, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), DS-GVO/BDSG, 2. Aufl. München 2018.

SCHOLZ PHILIP, in: Spiros Simitis/Gerrit Hornung/Indra Spieker genannt Döhmann (Hrsg.), Datenschutzrecht – DSGVO mit BDSG, Baden-Baden 2019.

SCHULZ SEBASTIAN, in: Peter Gola (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl. München 2018.

SCHWEIZER RAINER J., in: Bernhard Ehrenzeller/Benjamin Schindler/Rainer J. Schweizer/Klaus A. Vallender (Hrsg.), Die schweizerische Bundesverfassung – St. Galler Kommentar, 3. Aufl., St. Gallen 2014.

VASELLA DAVID, Zur Freiwilligkeit und zur Ausdrücklichkeit der Einwilligung im Datenschutzrecht, Jusletter 16. November 2015.

VASELLA DAVID/SIEVERS JACQUELINE, Der «Swiss Finish» im Vorentwurf des DSG, digma 2017, S. 44-48.

VEIL WINFRIED, in: Sibylle Gierschmann/Katharina Schlender/Rainer Stentzel/Winfried Veil (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln 2018.

WEBER ROLF H./BAISCH RAINER, Regulierung von Robo-Advice, AJP 2016, S. 1065-1078.

WILDHABER ISABELLE, Robotik am Arbeitsplatz: Robo-Kollegen und Robo-Bosse, AJP 2017, S. 213-224.

Materialien

Europäische Union, Gemeinsamer Leitfaden des Europäischen Parlaments, des Rates und der Kommission für Personen, die an der Abfassung von Rechtstexten der Europäischen Union mitwirken, Luxemburg 2015, abrufbar unter <http://bit.ly/2MMbp8d> (zit. Leitfaden Rechtstexte).

Artikel-29-Datenschutzgruppe, Guidelines on the right to data portability, Arbeitspapier 242rev.01 vom 5. April 2017, abrufbar unter <http://bit.ly/31nNork> (zit. Art.-29-Gruppe, Leitlinien Datenportabilität).

Artikel-29-Datenschutzgruppe, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679 vom 4. Oktober 2017, abrufbar unter <http://bit.ly/2XDPpOf> (zit. Art.-29-Gruppe, Leitlinien DSFA).

Artikel-29-Datenschutzgruppe, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Arbeitspapier 251rev.01 vom 6. Februar 2018, abrufbar unter <http://bit.ly/2XDOYn5> (zit. Art.-29-Gruppe, Leitlinien Profiling).

Artikel-29-Datenschutzgruppe, Guidelines on transparency under Regulation 2016/679, Arbeitspapier 260rev.01 vom 11. April 2018, abrufbar unter <http://bit.ly/2AZ9Aff> (zit. Art.-29-Gruppe, Leitlinien Transparenz).

Artikel-29-Datenschutzgruppe, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects vom 9. April 2019, abrufbar unter <http://bit.ly/2ZpcUuv> (zit. Art.-29-Gruppe, Leitlinien Rechtsgrundlage Vertrag).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September, BBl 2017 6971 ff. (zit. Botschaft rev. DSG).

Der hessische Beauftragte für Datenschutz und Informationsfreiheit, 45. Tätigkeitsbericht 2016, abrufbar unter <http://bit.ly/2KUDXdn> (zit. 45. Tätigkeitsbericht Hessen).

Entwurf des Bundesgesetzes über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017, S. 7193 ff., abrufbar unter <http://bit.ly/2MPJa8M> (zit. E-DSG).

Europarat, The protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2010)13 and explanatory memorandum, 23. November 2010, abrufbar unter <http://bit.ly/31ADBOF> (zit. Europarat, Empfehlung Profiling).

FINMA, Rundschreiben 2013/8 Marktverhaltensregeln – Aufsichtsregeln zum Marktverhalten im Effektenhandel vom 29. August 2013 (zit. RS 2013/8).

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK), Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Stand 17. Oktober 2018, abrufbar unter <http://bit.ly/2MQghZW> (zit. DSK, DSFA-Liste).

Schweizerische Bankiervereinigung, Data Leakage Protection – Information on Best Practice by the Working Group Information Security of the Swiss Bankers Association, Oktober 2012 (zit. SBVg, Data Leakage Protection).

Vorentwurf des Bundesgesetzes über den Datenschutz vom 21. Dezember 2016, abrufbar unter <http://bit.ly/2RiKzmU> (zit. VE DSG).